- **Expediente N.º: EXP202101565**

IMI Reference: A56ID 318964 - A60DD 432357 - Case Register 321773

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) interpuso reclamación, con fecha 5 de agosto de 2021, ante la autoridad de protección de datos de Baviera (Bavarian Lander Office for Data Protection Supervision). La reclamación se dirige contra OPEN BANK, S.A. con NIF A-28021079 (en adelante, OPENBANK). Los motivos en que basa la reclamación son los siguientes:

La entidad bancaria OPENBANK ha pedido a la parte reclamante que pruebe el origen de varias cantidades recibidas en su cuenta bancaria, en cumplimiento de la normativa contra el blanqueo de capitales. Sin embargo, no se le ha ofrecido ningún mecanismo para facilitar esta información cifrada o mediante carga directa en el portal web. La única opción válida ha sido el envío por e-mail.

Junto a la notificación se aporta:

- Copia de correo remitido desde la dirección ******EMAIL.1*** a ******EMAIL.2*** (en adelante, email de la parte reclamante) de fecha 7 de julio de 2021. En este correo, se requiere a la parte reclamante para que aporte la documentación necesaria para probar cuál es el origen los fondos de tres depósitos realizados por la parte reclamante, en cumplimiento de la legislación de prevención de blanqueo de capitales y contra la financiación del terrorismo; y se indica que, en el caso de no recibir esta documentación en el plazo de 15 días, OPENBANK deberá bloquear la realización de nuevos pagos en su cuenta de acuerdo con la normativa vigente.

- Copia de correo remitido desde el email de la parte reclamante a ******EMAIL.1*** de fecha 10 de julio de 2021. En este correo la parte reclamante indica que aporta bajo protesta la documentación correspondiente al año 2019 a través de un correo electrónico no encriptado porque, como indicó en una conversación telefónica, no existe la posibilidad de hacer llegar esa documentación electrónicamente de otra manera.

- Contestación automática al anterior correo de 10 de julio de 2021 enviada por ******EMAIL.3*** hacia la parte reclamante en la que se indica que se ha recibido su correo electrónico y le responderán pronto.

SEGUNDO: A través del "Sistema de Información del Mercado Interior" (en lo sucesivo IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la

cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, se transmitió la citada reclamación el día 24 de agosto de 2021 y se le dio fecha de registro de entrada en la Agencia Española de Protección de Datos (AEPD) el día 30 de agosto de 2021. El traslado de esta reclamación a la AEPD se realiza de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en lo sucesivo, RGPD), teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal, dado que OPENBANK tiene su sede social y establecimiento principal en España.

Los tratamientos de datos que se llevan a cabo afectan a interesados en varios Estados miembros. Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúa en calidad de "autoridad de control interesada", además de la autoridad alemana de protección de datos de Baviera, las autoridades de Países Bajos, Portugal y las autoridades alemanas de Renania del Norte-Westfalia, Hesse, Berlín y Baden-Wurtemberg. Todas ellas en virtud del artículo 4.22.b) del RGPD, dado que los interesados que residen en el territorio de estas autoridades de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

TERCERO: Con fecha 9 de septiembre de 2021, de conformidad con el entonces vigente artículo 64.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

En contestación a un requerimiento de información formulado por esta Agencia, OPENBANK aporta el 19 de mayo de 2022, entre otra, la siguiente información:

1. Indicación de que OPENBANK tiene delegado el servicio de solicitud de información a clientes a la entidad Santander Global Operations, S.A. (en adelante, SGO), que pertenece al grupo Santander, y que actúa en este caso como encargada del tratamiento.

2. Indicación de que tienen definido un procedimiento interno denominado "*Protocolo de comunicaciones a clientes por alertas de PBC/FT: Apertura y gestión de GAPS*" para establecer la forma de actuación de SGO cuando sea necesario solicitar información o documentación justificativa de un ingreso no habitual. Este procedimiento se aplicaría en todos los países en los que OPENBANK presta servicio en régimen de libre prestación de servicios, entre los que se incluyen

España y Alemania. Según lo indicado en el escrito, este procedimiento consiste en que "*el centro de atención telefónica de Openbank (en adelante, "call center"), contactará con el cliente para solicitar dicha información al número de teléfono móvil registrado en la base de datos de Openbank. Adicionalmente, se envía un correo electrónico a la dirección registrada en nuestra base de datos desde el buzón de* ******EMAIL.4*** *a clientes españoles o desde* ******EMAIL.1*** *a clientes alemanes. En aquellos casos en los que el cliente solicite información sobre otros canales a través de los cuales puede remitir la documentación requerida, se informa que tiene a su disposición los siguientes: (i) por correo postal y (ii) presencialmente en cualquiera de las dos sucursales que Openbank tiene en Madrid.*". Y manifiesta que se aporta el modelo de comunicación para ambos canales de contacto, que sería el siguiente:

> *Estimado cliente:*
> *El motivo de nuestra comunicación es informarle que Openbank está obligado, en cumplimiento de la legislación vigente, a conocer la actividad económica y origen de los fondos de sus clientes.*
> *A. Para una operación especifica: En esta comunicación le solicitamos documentación que acredite el origen de los fondos que con fecha […] ha ingresado en Openbank por un importe total de [...] €. Puede enviarnos cualquier documento que justifique el origen de los mencionados fondos.*
> *B. Para operaciones regulares: En esta comunicación le solicitamos documentación que acredite el origen de los fondos que de forma regular ha venido ingresando desde [...] y hasta la fecha por un importe total de [...] €. Puede enviarnos cualquier documento que justifique el origen de los mencionados fondos.*
> *Esta documentación la puede enviar a la siguiente dirección de correo electrónico: [*******EMAIL.5*** *para clientes españoles o* ******EMAIL.1*** *para clientes alemanes] indicando en el correo su nombre completo.*
> *Le informamos que Openbank, actuando en calidad de responsable del tratamiento de sus datos personales, tratará los mismos para el cumplimiento de las obligaciones legales a las que Openbank está sujeta adoptando medidas técnicas y organizativas suficientes para garantizar la seguridad de la información. Más información sobre sus derechos y protección de datos en [*******URL.1*** *para clientes españoles o* ******URL.2*** *para clientes alemanes]*
> *Quedando a su disposición para cuantas aclaraciones precise, reciba un cordial saludo*

3. Respecto a las medidas que se toman para garantizar la confidencialidad de la documentación que envía el cliente para justificar un ingreso no habitual, se indica, entre otras medidas, la siguiente:

> *Por último, teniendo en cuenta la seguridad que ofrecemos en nuestras páginas web y aplicaciones móviles, y que Openbank es un banco 100% digital les informamos que existen diferentes procesos en la entidad, como la contratación de préstamo hipotecario, préstamo personal o cuenta corriente, que permiten que los clientes nos remitan documentación a través del área privada de cliente donde estarán identificados con su documento de identidad y clave de acceso. En este sentido, nos gustaría indicar que esta*

funcionalidad se encuentra implantada y en funcionamiento para dar cumplimiento a la obligación de PBC/FT de aplicar medidas para garantizar el conocimiento que tiene Openbank de sus clientes y garantizar que los documentos, datos e información de que se disponga estén actualizados. Les adjuntamos a modo de ejemplo como Anexo V: Flujo de actualización de KYC y documentación de clientes.

Y se aportan impresiones de pantalla del formulario de conocimiento del cliente en el que se observa que, al finalizar la cumplimentación del formulario, se ofrece la opción de actualizar los documentos de "Documento de actividad económica" y de "Verificación de domicilio" cargándolos en ese momento.

4. Como "*Anexo IV: Soporte contractual del servicio prestado por SGO*", se aporta copia de un documento denominado "ANEXO 12 SERVICIO PREVENCIÓN DE BLANQUEO DE CAPITALES", en el que se indica que es anexo al contrato marco de arrendamiento de servicios entre OPENBANK (como cliente) y SGO (como proveedor) suscrito el 1 de enero de 2020 por un año prorrogable por periodos anuales. Este anexo está fechado el 16 de octubre de 2020 y su objeto es "*la prestación por el Proveedor al Cliente de un servicio de Back Office para las actividades relacionadas a la prevención del blanqueo de capitales y financiación del terrorismo*", con el siguiente contenido relevante:

   - En la cláusula primera:

(…).

   - En la cláusula quinta, respecto a la protección de datos de carácter personal, se indica que ***(…).***

     Además, en esta cláusula quinta se indica que ***(…)***.
     Y, en la cláusula quinta.d) se indica lo siguiente:

(…).

   - En la cláusula sexta, sobre requisitos de ciberseguridad, se incluye el siguiente apartado sobre las transferencias de datos:

(…).

   - En la cláusula undécima, sobre la subcontratación, se indica lo siguiente respecto a las actividades que no se pueden subcontratar:

(…).

CONCLUSIONES DE LAS ACTUACIONES PREVIAS DE INVESTIGACIÓN

1. Las comunicaciones con los clientes por alertas de prevención de blanqueo de capitales y financiación del terrorismo están subcontratadas a CGO tanto en España

como en Alemania. Informan de que existe un protocolo para realizar estas comunicaciones en el que se indica que, en estos casos, se contacta con el cliente utilizando el teléfono que tiene previamente registrado y, adicionalmente, se le envía un correo electrónico a la dirección de email que tiene previamente registrada.

2. De acuerdo con este protocolo, en la comunicación que se envía por correo electrónico para solicitar información al cliente por alertas de blanqueo de capitales, los canales que se le ofrecerían al cliente para enviar documentación serían los siguientes: correo electrónico, correo postal o presencialmente en las oficinas de OPENBANK en Madrid.

3. OPENBANK dispone de una manera para cargar documentos de forma segura (a través de su sitio web) para algunos procedimientos (por ejemplo, para actualizar los documentos “Documento de actividad económica” y “Verificación de domicilio” en el formulario de conocimiento del cliente). Esta manera de cargar documentos no se le ofrece al cliente dentro del protocolo por alertas de blanqueo de capitales, de acuerdo con lo indicado en la reclamación.

QUINTO: Con fecha 26 de agosto de 2022, la Directora de la AEPD adoptó un proyecto de decisión de inicio de procedimiento sancionador. Siguiendo el proceso establecido en el artículo 60 del RGPD, el 30 de agosto de 2022 se transmitió a través del sistema IMI este proyecto de decisión y se les hizo saber a las autoridades interesadas que tenían cuatro semanas desde ese momento para formular objeciones pertinentes y motivadas. Dentro del plazo a tal efecto, las autoridades de control interesadas no presentaron objeciones pertinentes y motivadas al respecto, por lo que se consideró que todas las autoridades estaban de acuerdo con dicho proyecto de decisión y estaban vinculadas por éste, de conformidad con lo dispuesto en el apartado 6 del artículo 60 del RGPD.

Este proyecto de decisión se notificó a OPENBANK conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el día 29 de agosto de 2022, como consta en el acuse de recibo que obra en el expediente.

SEXTO: Con fecha 3 de octubre de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a OPENBANK, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del Artículo 25 del RGPD, tipificada en el Artículo 83.4 del RGPD, así como por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD. En dicho Acuerdo de Inicio se le indicaba a OPENBANK que tenía un plazo de diez días para presentar alegaciones.

Este Acuerdo de Inicio, que se notificó a OPENBANK conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en fecha 3 de octubre de 2022, como consta en el acuse de recibo que obra en el expediente.

SÉPTIMO: Con fecha 6 de octubre de 2022, OPENBANK presentó un escrito a través del cual solicitaba la ampliación del plazo para aducir alegaciones y que se le facilitara copia del expediente.

OCTAVO: Con fecha 14 de octubre de 2022, el órgano instructor del procedimiento acordó la ampliación de plazo instada hasta un máximo de cinco días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP, y que se le remitiera a OPENBANK copia del expediente.

El citado acuerdo se notificó a OPENBANK en fecha 14 de octubre de 2022, como consta en el acuse de recibo que obra en el expediente.

NOVENO: Con fecha 26 de octubre de 2022, se recibió en esta Agencia, en tiempo y forma, escrito de OPENBANK en el que aducía alegaciones al Acuerdo de Inicio, acompañado de la siguiente documentación:

1.- Documento "Protocolo de comunicaciones a clientes por alertas de PBC/FT: APERTURA Y GESTIÓN DE GAPS (Versión de marzo de 2021)".
2.- Documento "Protocolo de comunicaciones a clientes por alertas de vigilancia transaccional de prevención de blanqueo de capitales y financiación del terrorismo (PBC/FT) (Versión de octubre de 2022)".
3.- Documento "Certificado sobre los apartados 3.10 y 3.11 del Manual de carácter interno de OPENBANK en materia de PBC/FT".
4.- Documento "Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles (versión agosto 2021)".
5.- Documento "Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles (versión octubre 2022)".
6.- Documento "Informe de homologación referido a Santander Global Operations, S.A."
7.- Documento "Certificado interno de seguridad emitido por Santander Global Technology and Operations, S.L."
8.- Documento "EVALUACIÓN ***(…)"***.
9.- Documento "VENDOR RISK ASSESSMENT - DP REPORT".
10.- Subida documentación área privada de cliente.
11.- Imágenes de "Sección: Preguntas Frecuentes en la página web de Openbank".
12.- Documento "Certificado de disponibilidad de carga de documentos, emitido el 21 de octubre de 2022".
13.- Documento "Certificado de número de análisis de operativa y de clientes impactados".

DÉCIMO: Con fecha 01 de diciembre de 2022, el órgano instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporados la reclamación interpuesta por la parte reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento E/09448/2021, dándose por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por OPENBANK, y la documentación que a ellas acompañaba.

Ese mismo día esta Agencia requirió a OPENBANK para que en el plazo de diez días hábiles presentara la siguiente información:

Aportar prueba documental respecto a la protección de datos desde el diseño y por defecto, por la que se requiere a OPEN BANK, S.A. la evaluación de impacto de protección de datos vigente el 07/07/2021, fecha en la que OPEN BANK, S.A. solicitó el envío de documentación a la parte reclamante, ya que en la documentación adjunta a las alegaciones de OPEN BANK, S.A. se aportan versiones posteriores, concretamente, las versiones modificadas de agosto de 2021 y octubre de 2022.

La apertura del período de prueba se notificó a OPENBANK conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el día 01 de diciembre de 2022, como consta en el acuse de recibo que obra en el expediente.

Con fecha 19 y 28 de diciembre de 2022, OPENBANK ha presentado su respuesta al citado requerimiento.

DÉCIMO PRIMERO: Con fecha 11 de abril de 2023 se formula diligencia por el instructor del procedimiento por la que se incorpora al expediente el documento “Informe anual 2021” del Grupo Santander, en el que consta estructura societaria del Grupo Santander y su volumen de negocio. En este informe consta que el volumen de negocio total anual global del Banco Santander, S.A. y sociedades dependientes (Grupo Santander) en el ejercicio financiero anterior a la comisión de la infracción, ejercicio 2020, fue de 44.279 millones de euros (ver páginas 555 y 843 del citado “Informe anual 2021”).

DÉCIMO SEGUNDO: Con fecha 23 de mayo de 2023**,** el órgano instructor del procedimiento dictó propuesta de resolución en la que se proponía, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, imponer una multa de 1.500.000 de euros a OPENBANK por la infracción del artículo 25 del RGPD, y una multa de 1.000.000 de euros por la infracción del artículo 32 del RGPD, tipificadas ambas en el artículo 83.4 del RGPD. Asimismo, se le indicaba que tenía un plazo de diez días para presentar alegaciones.

Esta propuesta de resolución, que se notificó a OPENBANK conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en fecha 1 de junio de 2023, como consta en el acuse de recibo que obra en el expediente.

DÉCIMO TERCERO: Con fecha 1 de junio de 2023, OPENBANK presenta un escrito a través del cual solicita la ampliación del plazo para aducir alegaciones y que se le facilite copia del expediente.

DÉCIMO CUARTO: Con fecha 2 de junio de 2023, el órgano instructor del procedimiento acuerda la remisión a OPENBANK de la copia del expediente, que se recibe mediante mensajería el 8 de junio de 2023, como consta en el acuse de recibo que obra en el expediente

DÉCIMO QUINTO: Con fecha 5 de junio de 2023, el órgano instructor del procedimiento deniega la ampliación de plazo solicitada para presentar alegaciones.

El citado acuerdo se notifica a OPENBANK ese mismo día, como consta en el acuse de recibo que obra en el expediente.

DÉCIMO SEXTO: Con fecha 14 de junio de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de OPENBANK en el que aduce alegaciones a la propuesta de resolución. En estas alegaciones, en síntesis, manifestaba que:

- El contenido de la propuesta de resolución es el mismo que el acuerdo de inicio del presente procedimiento sancionador, por lo que reproducirá las alegaciones ya presentadas.
- No resulta de aplicación la normativa de prevención de blanqueo de capitales.
- No existen datos financieros.
- No resultan exigibles las denominadas “medidas de nivel alto”.
- Se está vulnerando el principio *non bis in idem*, o subisidiariamente existiría un concurso medial de infracciones.
- OPENBANK cumple con el principio de protección de datos desde el diseño.
- OPENBANK no ha vulnerado el artículo 32 del RGPD.
- Se está vulnerando el principio de proporcionalidad.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: En el documento, sin firmar, que acompaña a las alegaciones al acuerdo de inicio del presente procedimiento, denominado “PROTOCOLO DE COMUNICACIONES A CLIENTES POR ALERTAS DE PBC/FT: APERTURA Y GESTIÓN DE GAPS”, se indica que la primera versión aprobada es del 03/04/2018 y que el 10/03/2021 se ha procedido a la “Revisión actualización y modificación de algunos plazos (reducción de los mismos)”. En el punto 4 del citado documento se detalla:

“4. SEGUIMIENTO DE LA PETICIÓN GAP Y BLOQUEO DE CUENTAS
Se establece el siguiente proceso y plazos para poder realizar el seguimiento de la solicitud de información relativa a alertas de PBC/FT y establecer los avisos en cuenta, cuando proceda:
***D**: SGO abre GAP solicitando al Contact Center que contacte al Cliente solicitando información/documentación. En caso de que la petición sea urgente o que el tamaño de la petición no quepa en GAP, SGO también la enviará por correo electrónico al Contact Center dejando constancia de este punto en GAP.*
***D+1**: Contact Center contacta con el cliente y solicita la información/documentación siguiendo el modelo Primera Comunicación del Anexo I. En primera instancia el contacto será por vía telefónica y además se le enviará un correo electrónico al cliente (Ver Primera Comunicación del Anexo I) detallando la documentación requerida. De no existir una dirección de correo válida se procederá a enviar la solicitud por Correo Postal.*
El Contact Center registrará en el GAP tanto el envío de esta comunicación como cualquier contacto con el cliente, o la imposibilidad de realizar dicho contacto, y reasignará el GAP a SGO.

SGO revisa GAP y registra en el comentario del GAP la fecha de la siguiente revisión (D+15).
***D+15**: De no haberse recibido la documentación requerida en dicha fecha SGO indicará al Contact Center que debe de reiterar la solicitud de información al cliente a través de un comentario y la reasignación del GAP.*
D+16**: Contact Center vuelve a contactar con el cliente, siguiendo el mismo proceso empleado en D+1 pero en este caso empleando la Segunda Comunicación del Anexo I en la cual se le advierte al cliente de la posibilidad de bloqueo.**"(…)"

En el Anexo I del citado documento, se indica:

"(…)"

SEGUNDO: El 7 de julio de 2021 se envió un correo electrónico desde la dirección ******EMAIL.1*** hacia ******EMAIL.2***. El contenido del correo electrónico es el siguiente (traducción no oficial del original en alemán):

"*Estimado Sr**. A.A.A.***
el motivo de nuestra comunicación es informarle de que Openbank está obligado, de acuerdo con la legislación vigente, a conocer la actividad económica y el origen de los fondos de sus clientes. En esta comunicación, le solicitamos los documentos que acrediten el origen de los fondos.
*Importes depositados en Openbank (cuenta finalizada en **XXXX**).*
*- a **(…)***
*- el **(…)***
*- el **(…)***
Por favor, envíenos documentos que prueben el origen de estos fondos.
Puede enviarnos cualquier documento que justifique el origen de dichos fondos (por ejemplo, impuesto sobre la renta, nómina, contrato de trabajo, contrato de compraventa si se trata de una operación inmobiliaria).
Garantizamos la absoluta confidencialidad de la documentación que nos envíe.
En caso de no recibir la documentación solicitada en el plazo de 15 días desde la fecha del presente aviso, Openbank podrá, en cumplimiento de la normativa aplicable, impedir que se realicen nuevos ingresos en sus cuentas.
*Si tiene alguna pregunta al respecto, no dude en ponerse en contacto con nosotros todos los días de 08:00 a 22:00 en el *****TELÉFONO.1**.*
Atentamente
Su equipo Openbank"

TERCERO**:** El 10 de julio de 2021 se envió un correo desde el email de la parte reclamante hacia ******EMAIL.1***. El contenido del correo electrónico es el siguiente (traducción no oficial del original en alemán):

"*Estimado Sr. o Sra,*
*Tengo una cuenta de dinero a la vista en Openbank S.A./Madrid desde el año pasado. Ahora me han pedido que aporte pruebas de depósitos a la vista de más de **XXXXX** euros, pero también de más de **XXXX** euros. Puedo entender esto como parte de la lucha contra el "blanqueo de dinero". Sin embargo, el banco no ofrece la posibilidad de cargar los datos de forma segura, por ejemplo, a través del portal del cliente. En su*

lugar, me veo obligado a transmitir mis datos personales a través de un simple correo electrónico no cifrado. A pesar de preguntar, sólo me ofrecieron esta opción, que me vi obligado a utilizar.
Les ruego que comprueben el proceso desde el punto de vista de la protección de datos y, en su caso, tomen las medidas oportunas.
Si no es usted la autoridad competente, le ruego que me remita el asunto y me envíe una notificación de presentación.
Le saluda atentamente
A.A.A."

CUARTO: El 13 de julio de 2021 la parte reclamante recibe en su correo una contestación automática enviada por ******EMAIL.3***. El contenido del correo electrónico es el siguiente (traducción no oficial del original en alemán):

"*Gracias por su solicitud. Le confirmamos que ha sido debidamente recibida y le enviaremos nuestra respuesta en breve.*
Le recordamos que nuestro horario de correo electrónico es de lunes a domingo de 08:00 a 22:00.

Se trata de una respuesta automatizada. Si tiene alguna pregunta, póngase en contacto con ******EMAIL.4****.*

Reciba un cordial saludo,
OPENBANK"

QUINTO: El documento 4 aportado por OPENBANK junto a las alegaciones al acuerdo de inicio del presente procedimiento sancionador lleva por título "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles*", no está firmado e indica que es de agosto 2021. En su página 41 incluye lo siguiente:

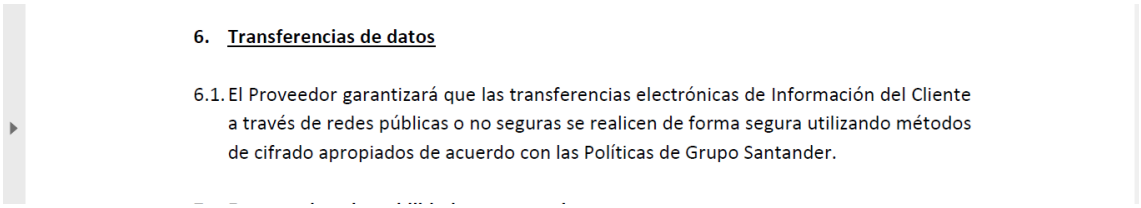
5. ANÁLISIS DE RIESGOS

	ANÁLISIS DEL RIESGO INHERENTE		CONTROL Y RIESGO RESIDUAL	
	DESCRIPCIÓN DE RIESGO INHERENTE	IMPACTO	CONTROLES Y PLAN DE MITIGACIÓN DE RIESGOS	IMPACTO
13. Seguridad	Fallos y eventos imprevistos desde el punto de vista de seguridad: - Errores de los usuarios, de configuración, - Secuencia, indisponibilidad de los datos, vulnerabilidades, - Errores de mantenimiento o actualización, - Posibles fugas de información - Errores en los accesos de los usuarios - Deficiencias técnicas y/u organizativas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.		- **"Data Loss Prevention ("DLP"),** que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa. El DLP, entre otras capacidades, permite comprobar qué información se envía a través de correo, además de los adjuntos, y podrá o bien bloquear el envío del correo electrónico o permitir el envío. Estos envíos serán revisados por el equipo de ciberseguridad y si detectan algo sospechoso, seguirán lo establecido en el procedimiento definido a estos efectos. En este aspecto, el interesado puede responder al correo electrónico con un mensaje cifrado remitiendo la contraseña mediante otro canal. El envío de un correo electrónico cifrado, supone que se implanten las medidas de seguridad adecuadas para la remisión de la información. Dicho esto, es importante destacar que las herramientas de correo electrónico de los clientes, la mayoría so Gmail, Microsfot 365, Yahoo, por defecto usan medidas de seguridad de cifrado TLS, tal y como se puede comprobar en sus propias plataformas: Medidas de seguridad implican el cifrado de la información: Gmail, Outlook/MSN, Yahoo. **Como mejora en este aspecto, Openbank ha solicitado una demanda interna para que los interesados puedan subir documentos directamente a través del apartado de la web, una vez que se hayan logado en la misma. No obstante, en tanto que no todos lo usuarios pueden llegar a estar digitalizados, también existen alternativas como envío por correo postal o entrega de documentación en Oficina.**	

SEXTO**:** Con fecha 19 de mayo de 2022, en respuesta al requerimiento de información formulado por esta Agencia, OPENBANK manifestó:

1.- Que tenía delegado el servicio de solicitud de información a clientes a la entidad Santander Global Operations, S.A. (SGO), que pertenece al grupo Santander, y que actúa en este caso como encargada del tratamiento, según contrato de fecha 16 de octubre de 2020.

En el documento "*Anexo IV: Soporte contractual del servicio prestado por SGO*" de la respuesta al requerimiento de información de esta Agencia, en el punto 6.1 de la cláusula sexta del "ANEXO 12 SERVICIO PREVENCIÓN DE BLANQUEO DE CAPITALES AL CONTRATO MARCO DE ARRENDAMIENTO MARCO DE SERVICIOS Y/O EJECUCION Y/O DESARROLLO DE PROYECTOS SUSCRITO ENTRE SANTANDER GLOBAL OPERATIONS S.A. Y OPEN BANK, S.A. SUSCRITO ENTRE OPENBANK, S.A. Y SANTANDER GLOBAL OPERATIONS, S.A. EL 1 DE ENERO DE 2020" se puede observar:



6. **Transferencias de datos**

6.1. El Proveedor garantizará que las transferencias electrónicas de Información del Cliente a través de redes públicas o no seguras se realicen de forma segura utilizando métodos de cifrado apropiados de acuerdo con las Políticas de Grupo Santander.

2.- Que tenía definido un procedimiento interno denominado "*Protocolo de comunicaciones a clientes por alertas de PBC/FT: Apertura y gestión de GAPS*" cuya finalidad era establecer el protocolo de actualización para la gestión de solicitudes de información a clientes por parte de Santander Global Technology and Operations (en adelante, "SGTO"), entidad perteneciente al Grupo Santander en la que Openbank tiene delegado este servicio como encargado de tratamiento.

3.- Que este procedimiento de gestión de solicitudes de información a clientes se aplicaba en todos los países en los que OPENBANK presta servicio en régimen de libre prestación de servicios, entre los que se incluyen España y Alemania.

4.- Que este procedimiento consistía en que "*el centro de atención telefónica de Openbank (en adelante, "call center"), contactará con el cliente para solicitar dicha información al número de teléfono móvil registrado en la base de datos de Openbank. Adicionalmente, se envía un correo electrónico a la dirección registrada en nuestra base de datos desde el buzón de* ******EMAIL.4*** *a clientes españoles o desde* ******EMAIL.1*** *a clientes alemanes. En aquellos casos en los que el cliente solicite información sobre otros canales a través de los cuales puede remitir la documentación requerida, se informa que tiene a su disposición los siguientes: (i) por correo postal y (ii) presencialmente en cualquiera de las dos sucursales que Openbank tiene en Madrid.*".

5.- Que el modelo de comunicación para ambos canales de contacto era el siguiente:

> ***(…).***
>
> *1.Los clientes podrán enviar por correo electrónico adjuntando la documentación encriptada y la contraseña mediante llamada telefónica*

SÉPTIMO: El documento 5 aportado por OPENBANK junto a las alegaciones al acuerdo de inicio del presente procedimiento sancionador lleva por título "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles"*, no está firmado e indica que es de octubre de 2022.

En su página 4, en el punto "1. RESUMEN EJECUTIVO", en el apartado "*Nombre y descripción del tratamiento*", describe el tratamiento de datos aplicable a este caso de la siguiente forma: "*Seguimiento de clientes y operaciones en cumplimiento de la normativa de PBC/FT específicamente lo establecido en el artículo 17 las entidades financieras a examinar con especial atención cualquier hecho u operación, con independencia de su cuantía, que, por su naturaleza, pueda estar relacionado con el blanqueo de capitales o la financiación del terrorismo, en particular toda operación o pauta de comportamiento compleja, inusual o sin un propósito económico o lícito aparente, o que presente indicios de simulación o fraude*."

En la página 15 del citado documento se clasifica el riesgo de la siguiente forma:

5. ANÁLISIS DE RIESGOS

Detalle de clasificación de Riesgo

Definición:
Riesgo: es un escenario que describe un acontecimiento y sus consecuencias estimado en términos de gravedad y probabilidad.
Riesgo Inherente: riesgo inherente o inicial implícito en cualquier tratamiento, teniendo en cuenta el impacto y probabilidad.
Riesgo residual: es el resultante de evaluar el nivel de riesgo resultante **después** de tomar las medidas y garantías orientadas a reducir el riesgo derivado de cada una de las fuentes de riesgo.

- Riesgo Bajo: no entrañe riesgo para los derechos y libertades de las personas físicas y por tanto de incumplimiento de la normativa.
- Riesgo Medio: si bien puede entrañar un riesgo para los derechos y libertades de las personas físicas y por tanto de incumplimiento de la normativa, este no es muy elevado y, puede mitigarse.
- Riesgo Alto: entrañe un alto riesgo para los derechos y libertades de las personas físicas y por tanto de incumplimiento de la normativa.
- No aplica

Y en la página 43 del citado documento se incluye lo siguiente:

5. ANÁLISIS DE RIESGOS

	Análisis del Riesgo Inherente		Control y Riesgo Residual	
	Descripción de Riesgo Inherente	Impacto	Controles y Plan de Mitigación de Riesgos	Impacto
13. **Seguridad**	Medidas relacionadas con las herramientas de comunicación: - Errores de los usuarios, de configuración, - Secuencia, indisponibilidad de los datos, vulnerabilidades, - Errores de mantenimiento o actualización, - Posibles fugas de información - Errores en los accesos de los usuarios - Deficiencias técnicas y/u organizativas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.		Se ha asegurado que los canales de comunicación con clientes como consecuencia asuntos relacionados con la prevención del blanqueo y financiación del terrorismo cuentas con medidas técnicas necesarias para garantizar la protección de sus datos personales. Los clientes se identificarás mediante su DNI y clave de acceso al área privada de cliente. Se adjunta procedimiento detallado: Flujo web	

OCTAVO: En el documento, sin firmar, que acompaña a las alegaciones al acuerdo de inicio del presente procedimiento, denominado "PROTOCOLO DE

COMUNICACIONES A CLIENTES POR ALERTAS DE VIGILANCIA TRANSACCIONAL DE PREVENCIÓN DE BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO (PBC/FT)", se indica que la primera versión aprobada es del 03/04/2018 y que el 10/03/2021 se ha procedido a la "Revisión actualización y modificación de algunos plazos (reducción de los mismos)". La revisión 3 del documento se indica se realizó el 06/05/2022 y consistió en la "Revisión actualización y modificación de las comunicaciones del Anexo I", mientras que la revisión 4 indica se realizó el 17/10/2022 y consistió en la "Revisión y actualización del protocolo con el objetivo de adecuarlo al nuevo proceso de subida de documentación por web privada, eliminando que el cliente tenga que remitir la misma a una dirección de correo electrónico. Documento revisado junto con el contact center y Operaciones Cumplimiento". En el punto 4 del citado documento se detalla:

"4. ENVÍO Y RECEPCION DE LA DOCUMENTACION POR PARTE DE LOS CLIENTES

En todos los casos (clientes de España y países de pasaporte -Alemania, Países Bajos y Portugal) se informará a los clientes de que suban la documentación requerida al espacio habilitado para ello en el área privada de la web de Openbank indicando, dentro del campo de texto, la información que permita justificar la operativa realizada.

El gestor del contact center prestará asistencia a los clientes cuando éstos tengan dificultades para subir la documentación. En caso de que el cliente haya olvidado su usuario y/o clave de acceso a la web de Openbank, se le informará de los pasos a seguir para reestablecer la misma. Además, se ha elaborado una guía de ayuda para los gestores e incorporado información para los clientes dentro del apartado de FAQ de la web."

Y en el *"Anexo I- Comunicaciones a clientes para solicitar información y/o documentación por una alerta de vigilancia transaccional de PBC/FT*" se explica:

"(…)"

NOVENO**:** A fecha 13 de octubre de 2022 OPENBANK tenía habilitado dentro del área privada de la página web del banco (que requiere usuario y contraseña de acceso) un espacio para que los clientes pudieran facilitar la documentación requerida en cumplimiento de lo dispuesto en el artículo 6 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

DÉCIMO**:** Durante el período de prueba, OPENBANK aportó un fichero de tipo Excel "*DOCUMENTO_NUM._1.XLSX*" sin firma ni fecha, en el que en la pestaña "*0.Hoja de Control*" se puede observar al inicio y en rojo "*Data Privacy Impact Assessment (DPIA)*". Y en la pestaña "*2. Ciclo de vida*" de este fichero, bajo el título "*Captura de Datos*", se contempla en el apartado "Actividades u operaciones de tratamiento" la "*Extracción de la operativa de transaccionalidad del cliente de los sistemas core del Banco*". ***(…):***

2. Ciclo de vida del tratamiento

Información General

El siguiente formulario debe recoger toda aquella información adicional que permita una adecuada identificación de amenazas y valoración de los riesgos a los que están expuestos los datos de carácter personal afectados. Es necesariindicar, a grandes rasgos, cómo sería el ciclo de vida del tratamiento, desde que los datos son capturados, de qué forma son almacenados o clasificados, con qué finalidad son utilizados, la existencia de cesiones o transferencias (ya sea a otras empresas nacionales o internacionales) y finalmente una descripción de cómo se procede a su destrucción.

Ciclo de vida del tratamiento	Captura de datos	Almacenamiento / clasificación	Uso / tratamiento	Cesión de los datos o transferencias a un tercero	Destrucción/ pseudonimización
Actividades u operaciones de tratamiento	Extracción de la operativa de transaccionalidad del cliente de los sistemas core del Banco	Almacenamiento de datos en listas internas de fraude.	Seguimiento y monitorización del perfil transaccional del cliente, por medio del análisis de sus posiciones y operativa en los distintos productos contratados con Openbank y ponderación	Cesión de datos del cliente a través de la herramienta Editran	Los datos no se destruyen, se almacenan de forma indefinida. No obstante se limita la profundidad histórica de la información que se consulta de un mismo cliente
Flujo y datos tratados	Datos de carácter identificativo Datos económicos, financieros y de seguros	Datos de carácter identificativo Datos económicos, financieros y de seguros	Datos de carácter identificativo Datos económicos, financieros y de seguros	Datos de carácter identificativo Datos económicos, financieros y de seguros	N/A
Intervinientes en las actividades u operaciones del tratamiento (incluyen encargados de tratamiento)	N/A	N/A	GEOBAN (encargado del seguimiento de alertas) BANCO SANTANDER SA (Análisis de operativa de segundo nivel)	Sepblac	N/A
Tecnología involucrada en las actividades del tratamiento	Partenon	Herramientas ofimáticas (Excel).	Herramienta Norkom Aplicativo FIOC	Editran	N/A

DÉCIMO PRIMERO: El Banco Santander, S.A. tiene la participación directa del 100% de Open Bank, S.A. (ver página 816 del "Informe anual 2021" del Grupo Santander).

El volumen de negocio total anual global del Banco Santander, S.A. y sociedades dependientes (Grupo Santander) en el ejercicio financiero anterior a la comisión de la infracción, ejercicio 2020, fue de 44.279 millones de euros (ver páginas 555 y 843 del "Informe anual 2021").

DÉCIMO SEGUNDO: El número de clientes total de OPENBANK es superior a 1,7 millones de clientes (Fuente: ******URL.3***)

DÉCIMO TERCERO: El número de peticiones, realizado por OPENBANK, de análisis de operativa en cumplimiento del art. 6 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y el número de clientes por ello impactados durante los años 2020, 2021 y 2022 ha sido el siguiente, de acuerdo a lo expuesto en el Documento 13 que acompaña a sus alegaciones al acuerdo de inicio del presente procedimiento sancionador:

AÑO	Nº de peticiones de análisis de operativa	Nº de clientes impactados
2020	3.806	3.584
2021	13.978	12.957
2022	14.056	12.879

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2

de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II
Cuestiones Previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que OPENBANK, a través de la entidad Santander Global Operations, S.A. como encargada del tratamiento, realiza la recogida, conservación y comunicación de, entre otros, los siguientes datos personales de personas físicas: nombre, apellidos, número de identidad fiscal, correo electrónico y el origen de los ingresos de los clientes, entre otros tratamientos.

OPENBANK realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60. En el caso examinado, como se ha expuesto, OPENBANK tiene su establecimiento principal en España, por lo que la Agencia Española de Protección de Datos es la competente para actuar como autoridad de control principal.

Por su parte, el artículo 25 del RGPD regula la protección de datos desde el diseño y por defecto, que el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento y, por otra, en el artículo 32 del RGPD se regulan las medidas de seguridad que deben adoptarse para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos personales.

III
Alegaciones aducidas

Con relación a las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por OPENBANK.

PRIMERA.- CONSIDERACIONES GENERALES ACERCA DEL CONTENIDO DE LA PROPUESTA DE RESOLUCIÓN

Alega OPENBANK que la estructura y contenido de la propuesta de resolución no solo resulta extremadamente compleja y difícil de seguir, sino que, como consecuencia de todo ello, la AEPD incurre en numerosas contradicciones.

En este sentido, alega que la propuesta de resolución dedica el fundamento de derecho III a la contestación a las alegaciones aducidas por OPENBANK al acuerdo de inicio del presente procedimiento sancionador, a cuyo objeto reproduce casi literalmente las alegaciones efectuadas por OPENBANK tratando de contraargumentar, una por una, lo señalado en cada una de ellas, pero que, posteriormente, la propuesta de resolución reproduce en los fundamentos de derecho IV y siguientes, de forma prácticamente literal y con mínimas alteraciones, el contenido del citado acuerdo de inicio, sin efectuar razonamiento o adición alguna a lo que ya se invocó por la Agencia en el momento de iniciarse el procedimiento.

Y alega que lo señalado en el fundamento de derecho III de la propuesta de resolución entra en abierta contradicción con lo mencionado a partir de su fundamento de derecho IV, dado que en el primero de estos fundamentos la AEPD niega sostener la argumentación o razonamiento que, posteriormente, reproduce y utiliza para ratificarse en su postura en los siguientes fundamentos de derecho.

Indica que esto conduce en primer lugar a una conclusión, obvia: si el razonamiento de la AEPD es exactamente el mismo que se mantuvo en el acuerdo de inicio, OPENBANK no puede sino ratificarse en todas y cada una de las alegaciones previamente efectuadas al citado acuerdo.

Al respecto, esta Agencia reconoce que es posible que la redacción de los fundamentos de derecho posteriores al que da respuesta a las alegaciones presentadas por OPENBANK fuera mejorable, razón por la cual se dará una nueva redacción que simplifique la lectura de la resolución, a la vez que se mejore la motivación en relación con la comisión de la infracción, así como la sanción a imponer y evite posibles confusiones.

SEGUNDA.- ACERCA DE LAS PREMISAS SOSTENIDAS POR LA AEPD A LO LARGO DEL PROCEDIMIENTO

OPENBANK, en sus alegaciones al Acuerdo de Inicio puso de manifiesto cómo aquél (y la Propuesta) se fundaba en tres argumentos esenciales: (i) que OPENBANK estaba sujeta en lo que respecta al cumplimiento de las obligaciones de diligencia debida, a lo establecido en el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante, la “LPBCFT”) y 60.2 de su Reglamento de desarrollo, aprobado por Real Decreto 304/2014, de 5 de mayo (en adelante, el “RPBCFT”); (ii) que la AEPD consideraba que la información solicitada por OPENBANK a la parte reclamante tenía la consideración

de “dato financiero”, que exigía la adopción de medidas reforzadas y no valoradas por OPENBANK; y (iii) que debían implementarse medidas de seguridad “de nivel alto”.

Se alega que la propuesta de resolución no contradice lo argumentado por OPENBANK, sino que niega la aplicación por el Acuerdo de Inicio de las citadas premisas, algo que, a su juicio, directamente se contradice del hecho mismo de la lectura de la propia propuesta, dado que los párrafos transcritos por OPENBANK siguen apareciendo, literalmente, en los fundamentos de derecho IV y siguientes de misma.

Al respecto, esta Agencia se reitera en que:

(i) el objeto del presente procedimiento no es la vulneración de lo dispuesto en la normativa de prevención de blanqueo de capitales sino la vulneración de lo previsto en los artículos 25 y 32 del RGPD, normativa aplicable a la protección de datos personales de las personas físicas, que es la competencia de esta Agencia;

(ii) la información solicitada por OPENBANK a la parte reclamante sí que tiene la consideración de “dato financiero”, lo cual exigía la aplicación de una serie de medidas reforzadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados (a tenor de lo dispuesto en el artículo 25 del RGPD), así como la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (a tenor de lo dispuesto en el artículo 32 del RGPD);

(iii) que en el presente caso no se trata de que debieran implantarse medidas de seguridad “de nivel alto”, sino que se trata de que debían implantarse medidas que garantizaran un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas.

No obstante, esta Agencia reconoce que es posible que la redacción de los fundamentos de derecho posteriores al que da respuesta a las alegaciones presentadas por OPENBANK fuera mejorable, razón por la cual se dará una nueva redacción que simplifique la lectura de la resolución, a la vez que se mejore la motivación en relación con la comisión de la infracción y la sanción a imponer y evite posibles confusiones.

1. Sobre la aplicabilidad de la normativa de prevención del blanqueo de capitales

Alega OPENBANK que, en relación con la supuesta aplicabilidad a las obligaciones de diligencia debida de lo establecido en el artículo 32 de la LPBCFT, la propuesta de resolución establece una premisa: que lo dispuesto en la normativa de prevención del blanqueo de capitales y la financiación del terrorismo resulta irrelevante en el presente caso, dado que (i) “la tipificación de los hechos no está motivada por una infracción de los artículos 32 y 32 bis de la Ley 10/2010, como dice OPENBANK en sus alegaciones, sino por los artículos 25 y 32 del RGPD”; (ii) “no es objeto del presente procedimiento si se ha vulnerado o no lo dispuesto en el artículo 32 o 32 bis de la LPBCFT, toda vez que no es la autoridad competente para ello y el bien jurídico protegido por la citada normativa es distinto al bien jurídico protegido por la normativa

de protección de datos"; y (iii) en relación con la invocación por OPENBANK de los informes de la propia AEPD "*lo que no puede hacerse es, tal y como pretende OPENBANK, utilizarlos para interpretar el contenido de un artículo, el 32.bis, en contraposición al artículo 32, cuando el artículo 32.bis no existía a la fecha de la emisión de tales informes, siendo añadido con posterioridad por el art. 3.15 del Real Decreto-ley 7/2021, de 27 de abril, en vigor a partir del 29/04/2021*".

Respecto de la primera de las cuestiones mencionadas, OPENBANK considera que basta una mera lectura del fundamento de derecho IV de la Propuesta de Resolución para poner de manifiesto cómo la AEPD sigue fundamentando toda la imputabilidad de OPENBANK en el supuesto incumplimiento por la misma del artículo 32 de la LPBCFT y cómo dicho precepto se refiere única y exclusivamente al cumplimiento por las entidades obligadas en materia de prevención del blanqueo de capitales a las previsiones relativas a las obligaciones de examen especial de operaciones y comunicación por inicio al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (en adelante, el "SEPBLAC").

Al respecto, esta Agencia reconoce que es posible que la redacción de los fundamentos de derecho posteriores al que da respuesta a las alegaciones presentadas por OPENBANK fuera mejorable, razón por la cual se dará una nueva redacción que simplifique la lectura de la resolución, a la vez que se mejore la motivación en relación con la comisión de la infracción y la sanción a imponer y evite posibles confusiones.

Del mismo modo, alega OPENBANK que la propuesta de resolución yerra al indicar que lo dispuesto en los artículos 32 y 32 bis de la LPBCFT se encuentra al margen de las competencias de la AEPD, toda vez que se trata de dos normas que regulan las obligaciones de los sujetos obligados en materia de protección de datos personales y no los aspectos sustantivos de la propia normativa de prevención del blanqueo de capitales. Y que estos preceptos se conforman como una norma especial referida a protección de datos personales en el entorno de la normativa de prevención del blanqueo de capitales, del mismo modo que numerosas normas sectoriales incluyen previsiones de protección de datos respecto de las cuales esa AEPD jamás ha negado su competencia, por cuanto no son sino la particularización para un supuesto o sector concreto de las propias normas contenidas en el RGPD y la LOPDGDD.

Indica OPENBANK que los preceptos mencionados son los que particularizan las obligaciones que habrán de cumplirse por los sujetos obligados para dar cumplimiento a los deberes de responsabilidad proactiva establecidos en la normativa de protección de datos personales en relación con los tratamientos de datos de esta naturaleza que deban llevar a cabo en cumplimiento de las obligaciones establecidas en la Ley, y, en lo que respecta a este caso, en lo que atañe al cumplimiento del deber de conocimiento del origen de los fondos establecido en la propia normativa de prevención del blanqueo de capitales.

Es decir, el cumplimiento del principio de responsabilidad proactiva, y en particular del de privacidad desde el diseño, se materializa en la adopción de las medidas que establece la propia LPBCFT, sin que sea admisible disgregar esta ley del propio RGPD, como si se tratase de normas legales independientes y referidas a realidades distintas. La LPBCFT indica cuáles son esas obligaciones, diferenciando de forma

evidente (y vigente al tiempo de producirse los hechos que han dado lugar al presente expediente) entre las obligaciones relacionadas con los tratamientos llevados a cabo en cumplimiento de la diligencia debida y aquéllas relacionadas con los tratamientos efectuados para el cumplimiento del examen especial de operaciones, de modo que en el presente caso es innegable la aplicación de lo previsto en el artículo 32 bis de la LPBCFT.

Al respecto, esta Agencia desea señalar que no puede menos que coincidir con todo lo afirmado por OPENBANK en este sentido. Si bien matizando que la gestión del cumplimiento normativo prevista en el artículo 25 del RGPD no se limita a la aplicación de los preceptos de la LPBCFT que particularizan algunas de las obligaciones en materia de protección de datos reforzando, a mayores, algunas de las obligaciones en relación con determinados tratamientos.

De este modo, alega OPENBANK, el cumplimiento del principio de privacidad desde el diseño en los tratamientos llevados a cabo en cumplimiento del Capítulo II de la LPBCFT se traduce en el artículo 32 bis.4 de la ley que dispone que "*los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos*".

Y es innegable, a su juicio, que OPENBANK llevó a cabo la mencionada evaluación de impacto en la protección de datos en relación con los citados tratamientos, como lo es que no concibió y aplicó esta obligación como un proceso estático, sino como un proceso dinámico, constando en el expediente las diversas evaluaciones efectuadas por OPENBANK, así como las medidas sucesivamente implementadas por aquélla, entre las cuales se encuentra actualmente la de que la información para el cumplimiento de las obligaciones de diligencia debida se facilitará en el área privada del cliente puesta a disposición del mismo por OPENBANK.

Al respecto esta Agencia desea señalar que el cumplimiento del principio de privacidad desde el diseño en los tratamientos llevados a cabo en cumplimiento del Capítulo II de la LPBCFT se traduce en mucho más que lo indicado en el artículo 32 bis.4 de la ley. A estos tratamientos les es de aplicación todo lo indicado en el artículo 25 del RGPD, tal y como le es de aplicación a todos los sujetos incluidos en su ámbito de aplicación. No obstante, en el caso concreto de las entidades sujetas al régimen de la LPBCFT, la obligación de realizar una evaluación de impacto a fin de adoptar medidas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales (y como mínimo, garantizar la trazabilidad de los accesos y comunicaciones de los datos), es una obligación a mayores, por la naturaleza misma de los tratamientos llevados a cabo en cumplimiento del Capítulo II de la LPBCFT, los cuales requieren de una mayor protección dado el mayor riesgo para los derechos y libertades de las personas físicas.

Cabe significar, asimismo, que la privacidad desde el diseño tampoco se limita a realizar las evaluaciones de impacto de protección de datos referidas en la LPBCFT.

En el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de OPENBANK, toda vez que no se ha incluido la actividad de recogida de datos de los clientes en el denominado "ciclo de vida del tratamiento" de su fichero Excel de documento de evaluación de impacto de protección de datos (aportado durante el período de prueba del presente procedimiento); por ello, al no preverse siquiera esta actividad, no se han aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados.

En cuanto a los análisis realizados por OPENBANK en los documentos denominados "Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles", en su versión de agosto de 2021, la cual ni siquiera estaba vigente al momento de los hechos objeto de la reclamación, los cuales tuvieron lugar en el mes de julio de 2021, sólo se había previsto como una posibilidad que los clientes remitieran la información mediante mensaje cifrado remitiendo la contraseña mediante otro canal. E incluso en el citado documento se menciona que se "ha solicitado una demanda interna para que los interesados puedan subir documentos directamente a través del apartado de la web, una vez que se hayan logado en la misma". No obstante, se ha podido comprobar que a la parte reclamante nunca se le dio esa posibilidad, ni en la comunicación inicial remitida por OPENBANK ni posteriormente cuando solicitó una vía alternativa segura para el envío de esa comunicación. También se comprobó que en el modelo de comunicación que se enviaba a los clientes no se daba ninguna de estas opciones, sólo se hacía mención a la posibilidad de responder el correo electrónico que se enviaba sin dar más indicaciones sobre cómo podía protegerse dicha información.

Resulta curioso que, pese a no facilitar ningún medio lo suficientemente seguro a sus clientes para proporcionar la información a que estaban obligados, ambos documentos en sus versiones de 2021 y 2022 reconocen que el riesgo inherente a tal tratamiento era de alto impacto para los derechos y libertades de los interesados.

Y, no obstante, recién es en la versión de octubre de 2022 cuando OPENBANK indica que "los clientes se identificarán mediante DNI y clave de acceso al área privada de cliente".

Lo que sí es cierto es que la comunicación dirigida al cliente cumplía lo previsto en el documento aportado por OPENBANK como protocolo para solicitar la documentación a los clientes en virtud de la LPBCFT y la comunicación dirigida a los clientes no indicaba medio alguno para proporcionar esa información, más allá de la posibilidad de responder el citado correo electrónico.

En cualquier caso, para cumplir con la protección de datos desde el diseño y por defecto no es suficiente con simplemente contar con un documento de protocolo o de modelo de comunicación, si luego al revisar dichos documentos se comprueba que no se realizó una previsión en condiciones sobre las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados, tal y como dispone el artículo 25.1 del RGPD.

Tampoco es suficiente con contar con documentos que establezcan protocolos o modelos a seguir, si luego en la práctica al realizar el tratamiento no se proporcionan tampoco medidas apropiadas para aplicar los principios de protección de datos ni se integran las garantías necesarias para cumplir con los requisitos del RGPD.

En el presente caso, ha quedado acreditado que en julio de 2021 se le solicitó a la parte reclamante que enviara determinada información, que podía tener un alto impacto para sus derechos y libertades, mediante correo electrónico, sin darle más indicaciones sobre cómo podía enviar dicha información a través de un canal seguro.

También ha quedado acreditado que la parte reclamante había manifestado al banco su preocupación en este sentido y había solicitado se le facilitara un medio seguro para compartir tal información. Pero, ante la negativa del banco, no le quedó otra opción que enviar la información solicitada a través de un simple correo electrónico, para su disgusto y pese a haber expresado sus reticencias. E incluso la parte reclamante pidió expresamente que se tuviera en cuenta su preocupación y se habilitara un medio seguro a futuro para compartir este tipo de información.

No obstante, en los documentos de agosto de 2021 que aportó OPENBANK junto con sus alegaciones al acuerdo de inicio, tampoco se prevé otro medio.

Del contenido de la documentación que figura en el expediente, ha quedado acreditado:

- Que en el “Anexo I - Comunicaciones a clientes para solicitar información y/o documentación por PBC” del documento ““PROTOCOLO DE COMUNICACIONES A CLIENTES POR ALERTAS DE PBC/FT: APERTURA Y GESTIÓN DE GAPS”, de fecha marzo 2021, en la primera comunicación que se dirige al cliente, en la que se le solicite que acredite el origen de los fondos, no se prevé indicar un medio específico por el cual deba facilitar tal información a OPENBANK. Y que en la segunda comunicación que se dirige al cliente no se prevé indicar tampoco un medio por el cual facilitar tal documentación al banco, pero se incluye en el texto la amenaza de que en caso de no recibir la documentación solicitada en los próximos 15 días OPENBANK puede impedir la realización de nuevos ingresos en sus cuentas.

- Que el 7 de julio de 2021 OPENBANK solicitó a la parte reclamante que enviara la documentación que acreditaba el origen de determinados fondos, bajo la amenaza de que en 15 días podían impedir nuevos ingresos en su cuenta, sin indicarle medio alguno por el cual debía facilitar tal información.

- Que el 10 de julio de 2021 la parte reclamante aportó la documentación solicitada manifestando su disconformidad porque cuando preguntó por la forma de remitir tal información, le indicaron que lo hiciera por correo electrónico, sin más. Y en este correo electrónico que envía, la parte reclamante indica que no lo considera un medio seguro, que lo realiza a través de este medio porque se vio obligado a ello, e incluso él mismo proporciona como ejemplo de medio seguro la posibilidad de remitirlo “a través del portal del cliente”, posibilidad que no se le proporcionó desde OPENBANK. También ruega que comprueben el

proceso desde el punto de vista de la protección de datos y tomen las medidas oportunas. No obstante, este correo electrónico sólo recibió un acuse de recibo automático por parte del banco, el 13 de julio de 2021.

- En el documento "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles*", de agosto 2021, se prevé que el interesado puede responder al correo electrónico con un mensaje cifrado remitiendo la contraseña mediante otro canal. Y que se ha solicitado que se pudiera realizar directamente a través del apartado de la web, una vez logados.

- En el documento "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles"*, octubre de 2022, se prevé que los clientes se autenticarán mediante su DNI y clave de acceso al área privada de cliente.

- En el documento "PROTOCOLO DE COMUNICACIONES A CLIENTES POR ALERTAS DE VIGILANCIA TRANSACCIONAL DE PREVENCIÓN DE BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO (PBC/FT)", de octubre 2022, se indica que se informará a los clientes de que suban la documentación a través del área privada de la web de OPENBANK. Y en el *"Anexo I- Comunicaciones a clientes para solicitar información y/o documentación por una alerta de vigilancia transaccional de PBC/FT*" se indica al cliente que envíe la documentación a través del "Área Clientes" de la web de OPENBANK.

Es decir, el protocolo vigente al momento de los hechos (de marzo de 2021) no preveía proporcionar información sobre el método de envío de la documentación solicitada, no obstante los riesgos en los derechos y libertades presentes en tal tratamiento de datos.

En julio de 2021 la parte reclamante llama la atención sobre esta cuestión en el correo que envía el 10 de julio de 2021 a OPENBANK. Pero el banco hace caso omiso y ni siquiera se le dio una respuesta a su inquietud, que versaba claramente sobre una cuestión de protección de datos personales, lo cual evidencia también la falta de un procedimiento interno de OPENBANK para canalizar estas cuestiones.

En agosto de 2021, OPENBANK prevé la posibilidad de que los clientes envíen la referida documentación a través de un correo electrónico cifrado y facilitando la contraseña mediante otro correo (sin especificar cuál). Y se indica que se solicitó la posibilidad de que se pudiera proporcionar esta documentación a través del área del cliente de la web de OPENBANK.

Y no es hasta octubre de 2022 que los protocolos de comunicación y los documentos de supuesta evaluación de impacto de esta cuestión incorporan de forma específica que los clientes puedan aportar la documentación solicitada a través de la página web de OPENBANK, logándose en su área de cliente.

Es decir, se adoptó la solución de poder proporcionar esta información a través del área de cliente un año y medio más tarde de que se adoptara el protocolo de actuación de marzo 2021 y más de un año más tarde de que la parte reclamante hubiera llamado la atención sobre esta cuestión en concreto y que el documento de supuesta evaluación de impacto de esta cuestión ya lo hubiera previsto como una posibilidad a

la que había que realizar seguimiento.

Todo ello evidencia que OPENBANK no aplicó un enfoque de protección de datos desde el diseño ni antes ni durante la realización del tratamiento, por lo que se desestima la presente alegación.

Alega OPENBANK que es perfectamente consciente de que el principio de privacidad desde el diseño exige que las medidas reforzadas para garantizar los derechos de los interesados se lleven a cabo con anterioridad a la práctica del tratamiento, pero que la obligación de que recabe del interesado información acerca del origen de los fondos viene prevista en la LPBCFT, cuya vigencia es anterior en más de ocho años a la del RGPD. Y que OPENBANK venía obligada a llevar a cabo el tratamiento de los datos al que se refiere el presente expediente mucho tiempo antes de que se adoptasen o cobrasen plena aplicación las normas contenidas en el RGPD y la LOPDGDD. Por ello, difícilmente puede exigirse a la misma la aplicación estricta del principio (en el sentido de que las medidas debían ser previas al tratamiento), so pena de incumplir sus obligaciones en materia de prevención del blanqueo de capitales y la financiación del terrorismo.

Al respecto, esta Agencia desea señalar que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal fue aprobada más de 10 años antes que la LPBCFT y que la propia LPBCFT contenía en su redacción original una referencia a la normativa de protección de datos personales en su artículo 32. Y que no cabe ninguna duda de que los sujetos a los que resultaba de aplicación la LPBCFT estaban plenamente sujetos a lo previsto en la normativa entonces vigente sobre protección de datos personales. Con independencia de que hubiera un artículo 32 de la LPBCFT específico para los tratamientos del Capítulo III de la citada Ley (que imponía una serie de mayores obligaciones para los responsables de tratamiento), ello no era óbice para que en el resto de tratamientos fuera de aplicación la normativa de protección de datos personales vigente en cada momento: en un principio, la LOPD de 1999, hasta que resultó de aplicación el RGPD y la LOPDGDD que desplazaron a aquella.

Si bien es cierto que el enfoque del RGPD y la LOPDGDD resultó completamente novedoso respecto la normativa de protección de datos anterior, no es menos cierto que OPENBANK contó con tiempo más que suficiente a lo largo de los tres años (seis años si se cuenta desde la adopción del texto RGPD) que transcurrieron entre que se aprobó el RGPD (abril de 2016), hasta que resultó de aplicación el RGPD (mayo 2018, lo que concedía dos años largos para la preparación y adaptación al RGPD) y los hechos objeto de la reclamación a que dio lugar el presente procedimiento sancionador (julio de 2021) para adecuar sus tratamientos a lo dispuesto en los artículo 25 y 32 del RGPD (cuatro años si se tiene en cuenta que recién se adoptaron las medidas para que los clientes pudieran compartir la información solicitada a través de su área privada en octubre de 2022).

Por supuesto que hubiera sido imposible que se tuviera un enfoque de protección de datos desde el diseño antes de realizar el tratamiento, cuando éste tuvo lugar muchos años antes de que el RGPD existiera, pero resulta innegable que el principio de protección de datos desde el diseño no implica únicamente que las medidas debían ser previas al tratamiento, sino que el propio artículo 25 del RGPD indica “*tanto en el*

momento de determinar los medios de tratamiento como en el momento del propio tratamiento", esto es, no solo de forma previa sino a lo largo de que ese tratamiento tenga lugar y siempre que se determinen los medios de tratamiento, lo cual es una decisión que se va tomando también a lo largo del tiempo, conforme van cambiando las circunstancias y las posibilidades de cada momento.

A mayor abundamiento, cabe significar que, sin denostar las obligaciones legales impuestas mediante la LPBCFT, las obligaciones legales previstas en el RGPD están como mínimo al mismo nivel, máxime cuando con estas últimas se protege un derecho fundamental. Obligaciones que tienen que ser cumplidas por OPENBANK, independientemente del cumplimiento de las que devengan de la LPBCFT; y ello sin que el cumplimiento de las previstas en esta última norma imposibilite el cumplimiento de las del RGPD.

OPENBANK está focalizando en sus riesgos, en los riesgos para la organización si no cumple con la LPBCFT, y no en los riesgos en los derechos y libertades de sus clientes en materia de protección de datos.

Por último, alega OPENBANK que el artículo 32 de la LPBCFT únicamente resulta aplicable a las obligaciones contenidas en su Capítulo III. Y ello hasta el punto de instar al legislador a la adopción de una norma que estableciera específicamente el alcance de dichas obligaciones en materia de protección de datos personales en relación con lo establecido en su Capítulo II de aquella Ley, como finalmente se materializó en el artículo 32 bis de la LPBCFT, añadido por el art. 3.15 del Real Decreto-ley 7/2021, de 27 de abril. Y que sólo de este modo puede interpretarse la conclusión alcanzada por el Informe 195/2013 del Gabinete Jurídico de esta AEPD cuando indica que "la interpretación de que el nivel de seguridad alto es al que se refiere el artículo 32.5 de la Ley 10/2010 es únicamente exigible en relación con los ficheros creados para el cumplimiento de las obligaciones establecidas en el Capítulo III de la citada Ley ha de considerarse congruente con el hecho de que la propia Ley establece determinadas limitaciones al afectado en relación únicamente con dichos ficheros, siendo ese nivel exigible una garantía adicional establecida como contrapeso de las citadas limitaciones" y el hecho de que en el Informe 41/2018 la AEPD instase al legislador la necesidad de regular las obligaciones de protección de datos en el marco del cumplimiento de los deberes de diligencia debida y de examen especial de operaciones, recomendando la redacción de normas diferenciadas para uno y otro tipo de tratamientos.

En resumen, alega OPENBANK que la argumentación sostenida por la AEPD debe decaer, dado que fundamenta el supuesto incumplimiento por OPENBANK del principio de privacidad desde el diseño y de la implementación de medidas de seguridad en una norma, el artículo 32 de la LPBCFT, que no resulta aplicable al caso, por haberlo incluso indicado así la propia Agencia.

Al respecto, esta Agencia coincide en que no es de aplicación a las obligaciones del Capítulo II de la LPBCFT el artículo 32 de la LPBCFT, sino el artículo 32 bis de la misma, razón por la que se dará una nueva redacción a los fundamentos de derecho posteriores al que da respuesta a las alegaciones presentadas por OPENBANK.

EN CONCLUSIÓN:

1.- La gestión del cumplimiento normativo del artículo 25 del RGPD, la privacidad desde el diseño, no se agota con el cumplimiento de las obligaciones en materia de protección de datos previstas en la LPBCFT.

2.- La gestión del cumplimiento normativo del artículo 25 del RGPD no se agota con la realización de evaluaciones de impacto de protección de datos.

3.- OPENBANK no había previsto la actividad de tratamiento consistente en la recogida de datos financieros de los clientes para la prevención del blanqueo de capitales.

4.- Las evaluaciones de impacto de protección de datos efectuadas por la parte reclamante en el momento en el que se produjeron los hechos no recogían la actividad de tratamiento consistente en la recogida de datos financieros de los clientes para la prevención del blanqueo de capitales.

5.- Al no preverse esta actividad por OPENBANK, no se habían identificado y evaluado los riesgos en los derechos y libertades de los clientes presentes en tal tratamiento.

5.- Al no identificarse y evaluarse los riesgos no se han establecido y aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados (de todos sus clientes).

6.- Todo lo anterior pone de manifiesto, de manera indubitada que OPENBANK no cumplió con su obligación de aplicar el artículo 25 del RGPD, la privacidad desde el diseño ni antes ni durante la realización del tratamiento.

2. Sobre la referencia efectuada por la AEPD a los datos financieros

Alega OPENBANK que la propuesta de resolución entra en una clara contradicción, dado que introduce en dos párrafos consecutivos del fundamento de derecho III dos consideraciones diametralmente opuestas y que parecen fundar su reproche sancionador.

Así, se indica que "*no corresponde determinar el nivel de riesgo y la necesidad de adoptar medidas de seguridad apropiadas en función de los datos financieros de forma aislada, sino según lo que prevé la normativa de protección de datos aplicable al caso, esto es, dependiendo del tipo de tratamiento, así como de manera específica, en materia de prevención de blanqueo de capitales*", lo que parece reforzar la idea, ya rebatida anteriormente, de que es la naturaleza del tratamiento, y no la de la tipología de los datos, la que justifica su reproche.

Pero inmediatamente añade que "*las circunstancias de hecho del presente caso determinan que deben ser adoptadas medidas de seguridad reforzadas dado que el tratamiento de los datos personales financieros de la parte reclamante presenta un*

elevado nivel de riesgo". Es decir, es la naturaleza de los datos, considerados financieros, y no la finalidad del tratamiento, la que justifica la adopción de unas medidas que la AEPD considera no cumplidas.

Al respecto, esta Agencia desea señalar que el análisis y adopción de medidas técnicas y organizativas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias para cumplir los requisitos del RGPD y proteger los derechos de los interesados (artículo 25 del RGPD) y para aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas (artículo 32 del RGPD), no debe realizarse únicamente en virtud de la naturaleza o finalidad del tratamiento que se realice ni únicamente en virtud de la tipología de los datos que se trate, como si fueran aspectos excluyentes, sino que debe realizarse teniendo en cuenta todos los aspectos que el tratamiento en cuestión pudiera entrañar.

El análisis efectuado por OPENBANK sobre el concepto de "dato financiero" para determinar si el tratamiento ante el que nos encontramos entraña un mayor riesgo y si esta categoría de datos merecen una especial protección no es correcto, toda vez que pretende valorar de forma separada el concepto "dato financiero" de la normativa de LPBCFT, cuando la necesidad de una evaluación de impacto de protección de datos y la consecuente adopción de medidas reforzadas que garanticen la integridad y confidencialidad de los datos personales, así como la garantizar la trazabilidad de los accesos y comunicaciones de los datos, ya se encuentran establecidas por el ordenamiento jurídico.

En cumplimiento de la LPBCFT, las entidades obligadas pueden tratar datos financieros, pero no sólo datos de esta categoría también son tratados datos personales de diversa naturaleza: de identificación, de contacto o económicos (empresariales, profesionales, de inversiones…). La protección de datos en cumplimiento de la LPBCFT no puede verse limitada por los criterios aplicables tan sólo a uno de estos datos, como pretende razonar OPENBANK, cuando lo que trata de proteger es el acceso a la información que suponen todos estos datos personales, no sólo de forma individual, sino a su tratamiento de forma conjunta.

Indica OPENBANK que lo anteriormente alegado se refuerza por el hecho de que el fundamento de derecho IV de la propuesta de resolución vuelve a considerar la referencia a los datos financieros efectuada por el considerando 28 del RGPD como esencial para determinar la necesidad de que OPENBANK hubiera establecido una medida adicional en la recogida de los datos relacionados con el origen de los fondos.

Al respecto, esta Agencia desea señalar que no entiende la referencia que se realiza al considerando 28 del RGPD, toda vez que éste trata de la seudonimización de los datos. En cualquier caso, la referencia a los datos financieros sí que es determinante, dado que son datos que merecen una especial protección al suponer su tratamiento un mayor riesgo para los derechos y libertades de las personas físicas.

Alega OPENBANK que, en cuanto a la referencia efectuada por la AEPD a las Directrices del Grupo de Trabajo del artículo 29 (en adelante, el "GT29"), baste señalar que el tratamiento controvertido ni supone ningún tipo de "evaluación o puntuación" de los interesados ni su contraste con "una base de datos de referencia de crédito o una

base de datos contra el blanqueo de capitales y la financiación del terrorismo", sino sólo la obtención de información sobre el origen de los fondos correspondientes a determinadas operaciones.

Al respecto, esta Agencia desea recordar el contenido de las "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679", en lo que aquí interesa: "*Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo (…) se deben considerar los nueve criterios siguientes: 1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes…"* (el subrayado es nuestro).

Esta Agencia considera que la actividad realizada por OPENBANK en virtud de lo dispuesto en el Capítulo II de la LPBCFT, por la que se le solicita a los clientes que aporten los "soportes que justifican un determinado ingreso, por cuanto permitirán de clarificar el origen de los fondos que han sido ingresados en la cuenta del cliente en OPENBANK" sí que se enmarca dentro de una institución financiera que investigue a sus clientes en una posible base de datos contra el blanqueo de capitales y la financiación del terrorismo, razón por la que son operaciones que entrañan probablemente un mayor riesgo.

Y tanto ello es así, que son operaciones que entrañan probablemente un mayor riesgo, que la misma LPBCFT consideró conveniente incorporar la necesidad de realizar una evaluación de impacto de la protección de datos de los tratamientos a los que se refiere dicho artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

Asimismo, alega OPENBANK que la propuesta de resolución parece indicar que OPENBANK no ha llevado a cabo evaluación alguna del impacto del tratamiento en la protección de datos, lo que entra en directa contradicción con el expediente administrativo, en que consta la misma, así como las medidas adoptadas para paliar los riesgos sobre la protección de datos derivados del tratamiento.

Al respecto, esta Agencia desea recordar que el objeto del presente procedimiento no es si OPENBANK realizó o no una evaluación de impacto tal y como le obliga el artículo 32 de la LPBCFT, sino si la organización había incorporado los principios de protección de datos desde el diseño y por defecto (artículo 25 del RGPD) y si había adoptado las medidas de seguridad apropiadas en relación al riesgo para los derechos y libertades de los interesados (artículo 32 del RGPD).

En el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de OPENBANK, toda vez que no se ha incluido la actividad de recogida de datos de los clientes en el denominado "ciclo de vida del tratamiento" de su fichero Excel de documento de evaluación de impacto de protección de datos (aportado durante el

período de prueba del presente procedimiento); por ello, al no preverse siquiera esta actividad, no se han aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados.

Por lo demás, esta Agencia se reitera en lo ya contestado en la alegación sobre la aplicabilidad de la normativa de prevención del blanqueo de capitales respecto al análisis del contenido de las comunicaciones enviadas a la parte reclamante así como de la documentación aportada al expediente, todo lo cual evidencia que OPENBANK no aplicó un enfoque de protección de datos desde el diseño ni antes ni durante la realización del tratamiento.

Alega OPENBANK que, tanto el Manual de legislación europea sobre protección de datos como la Guía sobre gestión del riesgo de la AEPD se refieren, al mencionar los datos financieros, a los relacionados con los medios de pago, aun cuando la propuesta de resolución parezca negar, de forma terminante y no fundada, dicha afirmación.

Al respecto, esta Agencia desea recordar el contenido del Capítulo 9.2 del Manual de legislación europea en materia de protección de datos, elaborado por la Agencia de la Unión Europea para los Derechos Fundamentales, el Consejo de Europa, el Tribunal Europeo de Derechos Humanos y el Supervisor Europeo de Protección de Datos donde se refiere a los "datos financieros": "*A pesar de que los datos financieros no se consideran datos sensibles en virtud del Convenio 108 o del Reglamento general de protección de datos, su tratamiento requiere garantías especiales que garanticen la exactitud y la seguridad de los datos. En particular, los sistemas de pago electrónico necesitan incorporar medidas de protección de datos, es decir, protección de la privacidad o de los datos desde el diseño y por defecto".* La mención a la protección de la privacidad respecto a los sistemas de pago electrónico viene a resaltar la importancia de éstos, pero no excluye que, de igual manera, otros datos financieros puedan requerir garantías especiales, tal y como ocurre en el presente caso con los datos recogidos en virtud de lo dispuesto en el Capítulo II de la LPBCFT.

En cuanto a la Guía sobre la gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD, se diferencia entre tres tipologías de datos económicos que deben valorarse a la hora de determinar el nivel de riesgo de un determinado tratamiento para la realización de la DPIA, diferenciando entre estas tres categorías de datos:

- Datos relacionados con la "[s]*ituación económica, (P.ej., sin ser exhaustivos, renta personal, Ingresos mensuales, Patrimonio (bienes muebles/inmuebles), Situación laboral)*". A estos datos se les asigna un "riesgo medio".
- Datos relacionados con el "[e]*stado financiero (P. ej,. sin ser exhaustivos, solvencia financiera, capacidad de endeudamiento, nivel de deuda (Préstamos personales, hipotecas), listas de solvencia, impagos, activos (fondos de inversión, rendimientos generados, acciones, cuentas a cobrar, rentas percibidas, etc.), pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; o deudas u obligaciones)*". A estos datos también se les asigna un "riesgo medio".

• "*Datos de medios de pago (P. ej., sin ser exhaustivos, tarjetas de crédito e información de acceso a servicios de monedas virtuales)*". En el caso de estos datos sí se asigna un "riesgo alto".

OPENBANK añadió en sus alegaciones al acuerdo de inicio del presente procedimiento sancionador que, en los criterios establecidos por la AEPD para la realización de una DPIA se recogen en el número 4 los "[t]*ratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos*".

Y que el elevado riesgo que debería justificar la implementación de lo que dicho Acuerdo denomina "*medidas de seguridad de nivel alto*" únicamente sería predicable, a juicio de OPENBANK, de la información que:

• Se refiriese a medios de pago, es decir, la referida a los datos relacionados con aquellos instrumentos que permiten al interesado la adquisición de bienes y servicios o le habilitan para la cancelación de deudas que pudiera mantener con terceros, al margen de la enumeración no exhaustiva del documento.

• La que permitiera determinar la situación financiera o la solvencia de una persona.

Al respecto, esta Agencia considera que la documentación solicitada por OPENBANK en virtud de lo dispuesto en el Capítulo II de la LPBCFT, es decir, "el soporte documental relacionado con el origen de un fondo de su cuenta bancaria (P.ej., su nómina, contrato laboral, contrato de compraventa si se trata de una operación inmobiliaria, donación o herencia, la factura por los servicios prestados que le son satisfechos por el beneficiario de aquéllos, la resolución por la que se declare la percepción de una determinada ayuda, etc.)" contiene datos relacionados con la situación económica y el estado financiero de los clientes, de los que permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que requieren de una mayor protección.

Por último, alega OPENBANK que la conclusión de esta Agencia según la cual "los datos con relación a tres ingresos en cuentas bancarias deben ser considerados como "datos financieros", y la información relativa al origen de estos ingresos, sin tener estrictamente naturaleza financiera, está íntimamente relacionada con estos movimientos bancarios, por lo que, al suministrarse información sobre el origen de los ingresos, a su vez se pone de manifiesto los movimientos en la cuenta bancaria de la parte reclamante que las actividades origen de esos ingresos producen", carece de soporte alguno que la acredite. Y que, en cualquier caso, es evidente que no serían lo mismo -y no puede pretenderse que lo sea- los datos catalogados como "financieros" (ingresos en cuenta bancaria) que los restantes datos (la información relativa al origen de estos ingresos), que la propuesta de resolución considera "íntimamente relacionada" con los movimientos bancarios.

Al respecto, esta Agencia insiste en que considera que la información relativa al origen de los ingresos en cuentas bancarias de los clientes es información que está íntimamente relacionada con tales movimientos bancarios y que contiene datos relacionados con la situación económica y el estado financiero de los clientes, de los

que permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que requieren de una mayor protección en atención a los riesgos en los derechos y libertades de los interesados.

En este sentido, no podemos dejar de indicar que los datos personales financieros conjuntamente considerados (los remitidos por el cliente por sí mismos, a los que se puede sumar los que ya tiene la entidad bancaria) pueden revelar múltiples aspectos sobre el cliente, como la situación financiera o la solvencia patrimonial tal y como hemos indicado.

Así, el Dictamen 1/15 del Tribunal de Justicia (Gran Sala) de 26 de julio de 2017 establece que, "128 Por otra parte, aun cuando algunos de los datos del PNR, aisladamente considerados, no parezcan poder revelar información importante sobre la vida privada de las personas afectadas, no deja de ser cierto que, conjuntamente considerados, dichos datos pueden revelar, entre otros extremos, un itinerario de viaje completo, hábitos de viaje, relaciones existentes entre dos o varias personas así como información sobre la situación económica de los pasajeros aéreos, sus hábitos alimentarios o su estado de salud, y podrían incluso proporcionar datos sensibles sobre dichos pasajeros, tal como se define en el artículo 2, letra e), del Acuerdo previsto", riesgo que asimismo recoge la STJUE de 1 de agosto de 2022.

En cualquier caso, la propia LPBCFT reconoce que son operaciones que entrañan probablemente un mayor riesgo, por lo que consideró conveniente incorporar la necesidad de realizar una evaluación de impacto de la protección de datos de los tratamientos a los que se refiere dicho artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

EN CONCLUSIÓN, la documentación solicitada por OPENBANK en virtud de lo dispuesto en el Capítulo II de la LPBCFT, es decir, "el soporte documental relacionado con el origen de un fondo de su cuenta bancaria (P.ej., su nómina, contrato laboral, contrato de compraventa si se trata de una operación inmobiliaria, donación o herencia, la factura por los servicios prestados que le son satisfechos por el beneficiario de aquéllos, la resolución por la que se declare la percepción de una determinada ayuda, etc.)" contiene datos financieros relacionados con la situación económica y el estado financiero de los clientes, de los que permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que su tratamiento requieren de una mayor protección en atención a los riesgos en los derechos y libertades de los interesados.

Por lo que se desestima la presente alegación.

3. Sobre la exigibilidad de las denominadas "medidas de nivel alto"

Alega OPENBANK que en el acuerdo de inicio del presente procedimiento sancionador se había invocado la exigibilidad de un nivel de seguridad "alto", que no era exigible desde la entrada en vigor del RGPD, y la propuesta de resolución se limita a indicar que reproducía el texto del artículo 32 de la LPBCFT en su redacción vigente al tiempo de producirse los hechos (lo que no hace sino reforzar lo ya indicado en relación con su indebida aplicación). Pero debe añadirse asimismo que, por más que

se indique lo contrario, el Acuerdo de Inicio, y la Propuesta de Resolución sí pretendían aplicar miméticamente a OPENBANK el régimen anterior a la plena aplicación del RGPD, dado que se refieren a una medida, el cifrado de datos, que expresamente se asociaba en dicha regulación a las denominadas “medidas de seguridad de nivel alto”.

Y que en este punto, la propuesta vuelve a negar, aunque, a su juicio, exista una evidencia que lo contradiga en el expediente, que OPENBANK efectuase una evaluación del impacto del tratamiento en los derechos de los interesados, para determinar el alcance de las medidas a adoptar, haciendo recaer todo el reproche a OPENBANK en el hecho de que uno solo de todos sus clientes “llamó la atención [a OPENBANK] sobre este extremo”, no siendo satisfactoria, a juicio de la Agencia, la respuesta dada por OPENBANK a aquél.

Y ello conduce a OPENBANK a cuestionarse si lo que la AEPD considera vulnerado en este caso es su deber de adopción de medidas técnicas y organizativas encaminadas a paliar los riesgos del tratamiento, previo análisis de dichos riesgos a través de una evaluación de impacto en la protección de datos, algo que (a su juicio) la AEPD no podrá negar que OPENBANK ha llevado a cabo, o el objeto del reproche de la AEPD es que no ha dado a la “inquietud” del interesado la respuesta que esa Autoridad considera adecuada, aun cuando no es posible negar (a su juicio) que OPENBANK sí respondió a lo solicitado.

Al respecto, esta Agencia desea señalar que el presente procedimiento sancionador refiere única y exclusivamente a que OPENBANK no aplicó, antes y durante la realización del tratamiento en cuestión, la protección de datos desde el diseño y por defecto, para asegurar el cumplimiento de los principios consagrados por el RGPD (artículo 25 del RGPD), y no adoptó las medidas de seguridad apropiadas en función del riesgo para proteger los derechos y libertades de los interesados (artículo 32 del RGPD), en lo relativo al tratamiento de datos objeto del presente procedimiento. Ya se ha indicado, además y a mayor abundamiento, que la protección de datos desde el diseño no se agota con la realización de una evaluación de impacto.

Las referencias que realizó esta Agencia a la LPBCFT han de entenderse únicamente para reforzar las infracciones de la normativa de protección de datos que esta Agencia habría constatado.

No obstante, esta Agencia dará una nueva redacción a los fundamentos de derecho posteriores, tal y como se indicó anteriormente.

Asimismo, esta Agencia desea señalar que ha revisado las medidas adoptadas por OPENBANK en lo que refiere a la información compartida por los usuarios para dar cumplimiento a las obligaciones previstas por la LPBCFT y la realidad es que no se les proporcionaba un medio seguro a los clientes para facilitar la información solicitada, información que, en relación con los riesgos, podía tener un alto impacto en los derechos y libertades de sus clientes si se materializaba, tal y como se desprende del propio análisis realizado por OPENBANK en sus documentos denominados “Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles”, tanto en su versión de agosto 2021 como la de octubre 2022. El hecho de que aun cuando la parte reclamante llamó la atención sobre este extremo, enviando un correo electrónico

a la dirección que le indicaron para remitir la documentación financiera, sin obtener respuesta alguna por parte de OPENBANK, evidencia aún más la falta de conciencia sobre esta cuestión, dado que tampoco se le proporcionó un medio alternativo para ello ni siquiera cuando lo solicitó. Es decir, que lo que esta Agencia considera vulnerado en este caso es no sólo que OPENBANK, al momento de producirse los hechos, no había llevado a cabo antes de realizar el tratamiento en cuestión ni durante su realización un análisis que permitiera asegurar el cumplimiento de los principios de protección de datos ni tampoco adoptó unas medidas apropiadas al riesgo para las libertades y derechos de los interesados, sino también que OPENBANK no ha dado a la "inquietud" del interesado una respuesta adecuada, todo lo cual no hace más que evidenciar la no adopción de los principios de protección de datos desde el diseño y por defecto.

En cuanto a los análisis realizados por OPENBANK en los documentos denominados "Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles", en su versión de agosto de 2021, la cual ni siquiera estaba vigente al momento de los hechos objeto de la reclamación, los cuales tuvieron lugar en el mes de julio de 2021, sólo se había previsto como una posibilidad que los clientes remitieran la información mediante mensaje cifrado remitiendo la contraseña mediante otro canal. E incluso en el citado documento se menciona que se "ha solicitado una demanda interna para que los interesados puedan subir documentos directamente a través del apartado de la web, una vez que se hayan logado en la misma". No obstante, se ha podido comprobar que a la parte reclamante nunca se le dio esa posibilidad, ni en la comunicación inicial remitida por OPENBANK ni posteriormente cuando solicitó una vía alternativa segura para el envío de esa comunicación. También se comprobó que en el modelo de comunicación que se enviaba a los clientes no se daba ninguna de estas opciones, sólo se hacía mención a la posibilidad de responder el correo electrónico que se enviaba sin dar más indicaciones sobre cómo podía protegerse dicha información.

Resulta curioso que, pese a no facilitar ningún medio lo suficientemente seguro a sus clientes para proporcionar la información a que estaban obligados, ambos documentos en sus versiones de 2021 y 2022 reconocen que el riesgo inherente a tal tratamiento era de alto impacto para los derechos y libertades de los interesados.

Y, no obstante, recién es en la versión de octubre de 2022 cuando OPENBANK indica que "los clientes se identificarán mediante DNI y clave de acceso al área privada de cliente".

Por último, OPENBANK alega que en ningún caso ha dejado de responder a las inquietudes de la parte reclamante ni cabe considerar que exista en dicha respuesta amenaza alguna de ningún tipo, como se indica la Propuesta de Resolución. OPENBANK se ha limitado a poner de manifiesto que la ausencia de información a la misma en relación con el origen de los fondos en los ingresos controvertidos exigirá que por parte de OPENBANK se proceda al bloqueo de la cuenta, al poder existir indicios, por incumplimiento de la normativa de prevención del blanqueo de capitales, de la existencia de una conducta ilícita en su cliente.

Al respecto, esta Agencia desea señalar que no se le ha proporcionado a la parte reclamante una respuesta satisfactoria a su inquietud, toda vez que no se le

proporcionó un medio adecuado para facilitar la información solicitada por OPENBANK en virtud del Capítulo II de la LPBCFT.

En todo caso, cabe aclarar en este momento que, lo que OPENBANK denomina como "inquietud" por parte del cliente, no es más que una persona, su cliente, que pretende se haga efectivo su Derecho Fundamental a la Protección de Datos de Carácter Personal.

En cuanto a si existió algún tipo de amenaza a la parte reclamante, se desea recordar el contenido del modelo de comunicación a los clientes, vigente en julio de 2021:

"□ **Segunda comunicación: D+16**
(…)
En el caso de no recibir la documentación solicitada en los próximos 15 días a contar desde la fecha de la presente comunicación, le informamos que Openbank puede impedir la realización de nuevos ingresos en sus cuentas en cumplimiento de la normativa en vigor. (…)" (el subrayado es nuestro)

Y el correo enviado a la parte reclamante el 7 de julio de 2021 por parte de OPENBANK decía lo siguiente:

"*Estimado Sr.* ***A.A.A.***
(…)
En caso de no recibir la documentación solicitada en el plazo de 15 días desde la fecha del presente aviso, Openbank podrá, en cumplimiento de la normativa aplicable, impedir que se realicen nuevos ingresos en sus cuentas. (…)" (el subrayado es nuestro)

El contenido de las comunicaciones enviadas por OPENBANK a los clientes (entre ellos, la parte reclamante), por las que se solicita el envío de la documentación en virtud del Capítulo II de la LPBCFT, contienen un aviso de que si no se remite la citada documentación en el plazo de 15 días, OPENBANK puede impedir que se realicen nuevos ingresos en sus cuentas.

El diccionario de la Real Academia Española explica que "amenaza" es un "dicho o hecho con que se amenaza". Mientras que "amenazar" es aquello "dicho de algo malo o dañino: Presentarse como inminente para alguien o algo" y también "dar indicios de ir a sufrir algo malo o dañino".

Bloquear los nuevos ingresos de las cuentas de los clientes, por supuesto que es algo malo o dañino para quien lo sufre, por más que ello sea, al decir de OPENBANK, "al poder existir indicios, por incumplimiento de la normativa de prevención del blanqueo de capitales, de la existencia de una conducta ilícita en su cliente".

Incluir esa información en las comunicaciones dirigidas a los clientes, hace que estos últimos remitan la documentación solicitada aunque no se le proporcionen medios apropiados para ello (como ha debido hacer la parte reclamante), por miedo a las posibles consecuencias desfavorables para ellos, en este caso, el bloqueo de sus cuentas.

Por todo lo expuesto, se desestima la presente alegación.

TERCERA.- ACERCA DE LA VULNERACIÓN DEL PRINCIPIO NON BIS IN IDEM O SUBSIDIARIAMENTE DE LA EXISTENCIA DE CONCURSO MEDIAL EN EL PRESENTE CASO

OPENBANK alega que se le pretende sancionar doblemente como consecuencia de un mismo hecho y por la vulneración de un mismo bien jurídico, al considerarse que no había establecido medidas de seguridad adecuadas para la transmisión (y consiguiente recepción por aquélla) de lo que erróneamente se consideraban "datos financieros" y, al propio tiempo, no haber adoptado dichas medidas desde el diseño del tratamiento.

Del mismo modo, alega que, en el negado supuesto de que no se considerase que nos encontrábamos ante una doble sanción por un mismo hecho, resultando vulnerado un mismo bien jurídico protegido, de lo que no cabía duda es de que la supuesta ausencia de medidas de seguridad adecuadas en la remisión de la documentación traía su causa, necesariamente, del, a juicio de la AEPD, inadecuado análisis de riesgos efectuado por OPENBANK, de forma que no habría previsto la implementación de tales medidas. De este modo, si se negaba la vulneración del principio non bis in idem, de lo que no cabía duda alguna era de la existencia de un concurso medial entre ambas infracciones.

Cita OPENBANK la propuesta de resolución del presente procedimiento sancionador en la que se dice expresamente lo siguiente en relación con la supuesta vulneración del artículo 25 del RGPD:

> *"En este protocolo, OPENBANK no tenía previsto ofrece a sus clientes ningún canal de comunicación con un nivel alto de seguridad, a pesar de que en la cláusula sexta del contrato con su encargado de tratamiento indica que "las transferencias electrónicas de Información del Cliente a través de redes públicas o no seguras se realicen de forma segura utilizando métodos de cifrado apropiados de acuerdo con las Políticas de Grupo Santander".*
>
> *Al aplicar el citado protocolo, OPENBANK hace recaer en el cliente la responsabilidad de una comunicación segura, siendo este quien debe procurar la confidencialidad e integridad de sus datos personales. En este punto, recordemos que, en virtud del principio de responsabilidad proactiva consagrado en el artículo 5.2 del RGPD, el responsable del tratamiento, en este caso OPENBANK, es quien debe asegurar la efectiva privacidad e integridad de los datos personales objeto de tratamiento."*

Indica OPENBANK que el peso de la imputación de la supuesta vulneración del artículo 25 del RGPD se hace recaer en el hecho de que no había establecido, a juicio de la AEPD "ningún canal de comunicación con un nivel alto de seguridad" trasladando al interesado la responsabilidad de velar por "la confidencialidad e integridad de sus datos personales".

Es decir, es la propia Propuesta de Resolución la que indica claramente que la supuesta falta de diseño de medidas técnicas y organizativas adecuadas se refiere,

específicamente, a la supuesta falta de medidas de seguridad en el envío de la documentación, haciendo posteriormente una valoración acerca de la supuesta ineficacia del cifrado de correos electrónicos para garantizar la integridad y confidencialidad de los datos.

De este modo, resulta a OPENBANK ciertamente sorprendente que la propia Propuesta de resolución afirme en un lugar distinto que en el presente caso no se está haciendo referencia, al hablarse de las medidas técnicas y organizativas adecuadas al riesgo, a las medidas relacionadas con el envío de la documentación, cuya supuesta ausencia ha sido la que ha dado lugar a la comunicación dirigida por la parte reclamante a OPENBANK.

Al respecto, esta Agencia se reitera en que se dará una nueva redacción a los fundamentos de derecho posteriores, tal y como se indicó anteriormente.

Alega OPENBANK que para apoyar la supuesta diferenciación y, en su defecto, desconexión entre ambas infracciones, la AEPD señala en el fundamento de derecho III de la Propuesta de resolución, que la supuesta vulneración del artículo 25 del RGPD no se refiere a la falta de adopción de medidas específicas en la remisión de los documentos, sino al hecho de que dichas medidas no han sido comunicadas a la parte reclamante cuando puso de manifiesto su preocupación sobre el modo de remisión de aquéllos.

Sin embargo, entiende OPENBANK que tal argumento no puede sostenerse, dado que esa supuesta falta de comunicación traería su causa del hecho de que las medidas de seguridad cuya vulneración se achaca a OPENBANK, y que además fueron posteriormente implementadas, no existían al tiempo de producirse la remisión de tal preocupación a OPENBANK.

Es decir, nos encontraríamos simplemente ante la adición de un nuevo elemento que no altera la relación causal entre las infracciones imputadas a OPENBANK, dado que la ahora argumentada por la AEPD como base de la imputación del artículo 25 del RGPD (falta de atención a la inquietud manifestada por interesado, al que, aun cuando pudiera parecer lo contrario de la lectura de la Propuesta, sí se dio respuesta) traería su causa del hecho de que no se habían, a juicio de la AEPD, adoptado medidas de seguridad adecuadas porque, supuestamente, OPENBANK no había llevado a cabo un adecuado análisis de los riesgos del tratamiento para los derechos de los interesados y adoptado tales medidas técnicas y organizativas.

Y todo ello nos devolvería a la conclusión inicial ya manifestada por OPENBANK: se está imponiendo una doble sanción por unos mismos hechos y la supuesta vulneración de un mismo bien jurídico o, cuando menos, una de las supuestas infracciones trae causa directa y subsume a la otra, hasta el punto de que si no se hubiera cometido ésta no se habría cometido la segunda.

Y a tal efecto indica OPENBANK que resulta paradigmático observar cómo, pese a su ímprobo esfuerzo, la Propuesta de Resolución no hace más que ratificar lo alegado al Acuerdo de Inicio, cuando se indica en la página 64 de la Propuesta lo siguiente:

"Del examen de los hechos probados y de la documentación obrante en el expediente, puede diferenciarse claramente dos infracciones basadas en hechos y fundamentos distintos. La comisión de la infracción del artículo 32 del RGPD deviene del requerimiento de documentación de OPENBANK a los clientes (y en concreto, a la parte reclamante) siguiendo el protocolo de comunicación previsto a tal efecto, en el que no se le indica al cliente ningún medio seguro para facilitar la información solicitada. Ni tan siquiera cuando el cliente solicita al banco un medio alternativo, como ocurrió en el caso concreto de la parte reclamante, que no tuvo más opción que remitir la citada documentación por correo electrónico ya que al dirigirse a OPENBANK para que se le facilitara otra opción, ello no ocurrió.

Por lo tanto, no se aplicaron medidas técnicas y organizativas de seguridad apropiadas por parte de OPENBANK para la realización del tratamiento en cuestión en general ni aun ante la petición formulada por la parte reclamante, efectuándose un tratamiento de datos (recordemos que la recogida de datos es una operación de tratamiento según el artículo 4.2) del RGPD), sin las medidas de seguridad adecuadas para garantizar la confidencialidad del tratamiento.

Por otra parte, la comisión de la infracción del artículo 25 del RGPD se fundamenta en que el protocolo de OPENBANK vigente al momento de los hechos (de marzo de 2021) no preveía proporcionar información sobre el método de envío de la documentación solicitada. Se sanciona la falta de diseño de un sistema adecuado para cumplir con los principios del tratamiento, los requisitos del RGDP y garantizar los derechos de los interesados."

Es decir, se considera infringido el artículo 32 del RGPD porque "no se le indica al cliente ningún medio seguro para facilitar la información solicitada" y por el artículo 25 del RGPD porque el protocolo de OPENBANK "no preveía proporcionar información sobre el método de envío de la documentación solicitada", lo que es exactamente lo mismo que se acaba de invocar como motivo de la imputación del artículo 32 del RGPD.

En primer lugar, esta Agencia desea señalar que la infracción del artículo 25 del RGPD y la infracción del artículo 32 del RGPD, son infracciones que están tipificadas de manera diferenciada al vulnerar preceptos distintos que protegen bienes jurídicos diferentes, como a continuación se expondrá. Por lo tanto es algo previsto por el legislador, sin que la vulneración de uno de los preceptos impida la del otro, lo que además no supone per se conculcar el principio de non bis in idem.

Asimismo, si bien están calificadas ambas infracciones como graves a efectos de la prescripción en la LOPDGDD, se reseñan en distintos apartados del artículo 73 de la LOPDGDD:

"(…)
d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.
f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.
g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679. (…)".

Por tanto, se trata de infracciones perfectamente diferenciadas.

En segundo lugar, el artículo 31 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) establece: "*No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento*".

En el presente caso, la infracción por vulnerar lo dispuesto en el artículo 25 del RGPD se determina ante la inadecuada protección de datos desde el diseño y por defecto, en virtud del cual "*el responsable del tratamiento aplicará tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas*". Estas medidas no tienen por qué tratarse estrictamente de medidas de seguridad, cuestión que se recoge específicamente en el artículo 32 del RGPD en cuando al tratamiento en concreto, por el que *"el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".*

El artículo 25 del RGPD se vulnera cuando no se han adoptado *aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679,* lo que puede producirse o no por ausencia o deficiencia de las medidas de seguridad. Las medidas técnicas y organizativas a que hace referencia el artículo 25 del RGPD para aplicar los principios de protección de datos desde el diseño no están limitadas a medidas estrictamente de seguridad.

Esto sería simplificar la esencia y el espíritu que inspira el RGPD, así como la voluntad del legislador, ya que el cumplimiento del RGPD no se limita a la implantación de medidas técnicas y organizativas de seguridad; lo cual significaría, en el presente caso, reducir la garantía exigida por el artículo 25 del RGPD a su logro únicamente con medidas de seguridad dejando sin efecto y de facto las garantías establecidas por le RGPD.

En este sentido, el artículo 25 del RGPD establece:

"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y

> *libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados"* (el subrayado es nuestro)

Esta Agencia se reitera en que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el artículo 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. De seguridad. Sólo de seguridad.

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo mientras que en el caso del artículo 25 del RGPD se debe garantizar la gestión del cumplimiento normativo de todo el RGPD. Por tanto, como se puede observar, los dos artículos persiguen fines distintos y protegen bienes jurídicos diferentes, aunque puedan estar relacionados.

En cuanto al examen del non bis in idem, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que:

> *"(…) Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.*
>
> *Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):*
>
> *a) La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.*
>
> *b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.*

c) La identidad de fundamento o causal, implica que las medidas sancionadoras no pueden concurrir si responden a una misma naturaleza, es decir, si participan de una misma fundamentación teleológica, lo que ocurre entre las penales y las administrativas sancionadoras, pero no entre las punitivas y las meramente coercitivas."

Tomando como referencia lo anteriormente explicitado en el presente procedimiento sancionador no se ha vulnerado el principio non bis in idem, puesto que la infracción del artículo 25 del RGPD se concreta en no haber realizado una adecuada gestión del cumplimiento normativo, mientras que la infracción del art. 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes con independencia de la petición realizada por la parte reclamante. Aunque la parte reclamante no hubiera realizado petición alguna (otros muchísimos clientes se habrán limitado a remitir la documentación requerida sin plantearse nada) las medidas de seguridad serían, en sí mismas, inadecuadas.

Y todo ello frente a las alegaciones formuladas por OPENBANK que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el artículo 25 del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la adopción de las medidas que garanticen la aplicación de forma efectiva los principios de protección de datos y el cumplimiento de los requisitos del RGPD y proteger los derechos de los interesados. Y ello no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Por lo demás, esta Agencia se reitera en lo afirmado en la citada propuesta de resolución.

Respecto a la infracción de lo dispuesto en el artículo 25 del RGPD, cabe recordar que la Protección de Datos desde el Diseño y por Defecto (PDDD) es una obligación legal, cuya vulneración constituye una infracción según lo dispuesto en el artículo 83 del RGPD.

La protección de datos desde el diseño forma parte del sistema de gestión del cumplimiento normativo, que implica concebir y planificar el tratamiento, verificar su cumplimiento y poder demostrarlo, todo ello enmarcado en un proceso de revisión y mejora continua, donde la privacidad desde el diseño juega un papel fundamental.

Las organizaciones deben preocuparse por instaurar una verdadera cultura de protección de datos en la organización, donde la protección de datos esté integrada en las políticas de cumplimiento normativo de aquellas, desde el inicio mismo del diseño de los tratamientos de datos de carácter personal.

Por su parte, en la "Guía de Privacidad desde el Diseño" de la AEPD lo define de la siguiente forma: "*La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por*

las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada".

Y en la resolución del procedimiento sancionador PS/00001/2021 esta Agencia ha considerado que *"La responsabilidad proactiva implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento generalizado de las obligaciones en materia de protección de datos. Comprende el establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización, especialmente si es una gran empresa, -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que le permita demostrar su cumplimiento."*

En el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de OPENBANK, toda vez que no se ha incluido la actividad de recogida de datos de los clientes en el denominado "ciclo de vida del tratamiento" de su fichero Excel de documento de evaluación de impacto de protección de datos (aportado durante el período de prueba del presente procedimiento); por ello, al no preverse siquiera esta actividad, no identificarse ni evaluarse los riesgos presentes en el tratamiento, no se han aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros de los previstos en el artículo 5 del RGPD, el relativo a la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados.

También ha quedado de manifiesto que la organización no contaba con un procedimiento adecuado para dar debida respuesta a una preocupación de un cliente sobre una cuestión de protección de datos, toda vez que en el presente caso la parte reclamante en su correo de 10 de julio de 2021 manifestó su disconformidad respecto a enviar los datos a través de un correo electrónico no cifrado. Incluso indica que preguntó a OPENBANK pero no se le ofreció otra opción. Es más, la parte reclamante aporta la solución que más tarde es la adoptada por OPENBANK, en tanto dijo "…*el banco no ofrece la posibilidad de cargar los datos de forma segura, por ejemplo, a través del portal del cliente (…)".* Y solicitó que *"comprueben el proceso desde el punto de vista de la protección de datos y, en su caso, tomen las medidas oportunas".* Sin embargo, no es hasta el inicio del presente procedimiento sancionador que OPENBANK ha revisado esta cuestión y ha adoptado una nueva solución en aras de cumplir con la normativa de protección de datos.

Por lo que respecta a la vulneración del artículo 32 del RGPD, ésta se fundamenta en que el único canal de comunicación para el envío de documentos ofrecido a los clientes (entre ellos, la parte reclamante), tal y como consta en los hechos probados, era contestar al propio correo electrónico, y que dicho medio de envío no era un medio adecuado en función del riesgo que podía existir para los derechos y libertades de los interesados. En el caso concreto, OPENBANK no facilitó a su cliente un medio apropiado para aportar la documentación ni siquiera pese a las advertencias de la parte reclamante en este sentido, por lo que el envío se hizo sin las medidas de seguridad adecuadas.

Y ello pese a que los documentos 4 y 5 presentado por OPENBANK junto con sus alegaciones, denominados “Evaluación de impacto- Seguimiento de clientes y operaciones sensibles”, versión agosto 2021 y octubre de 2022, respectivamente, en el apartado “13. Seguridad” se ha calificado el riesgo como de impacto alto. Además, en la versión de octubre de 2022, en la página 43 se ha incluido la siguiente indicación sobre “*Control y riesgo residual*”: “*Se ha asegurado que los canales de comunicación con clientes como consecuencia asuntos relacionados con la prevención del blanqueo y financiación del terrorismo cuentas con medidas técnicas necesarias para garantizar la protección de sus datos personales. Los clientes se identificarán mediante su DNI y clave de acceso al área privada de cliente*”.

De forma subsidiaria, en cuanto a la aplicación de las medidas técnicas y organizativas reforzadas al tratamiento en cuestión, cabe afirmar que el hecho de que un tratamiento en su conjunto no sea considerado de alto riesgo y que no tenga que realizarse una evaluación de impacto de protección de datos, no significa que no deban aplicarse medidas de seguridad apropiadas al mayor riesgo que presente alguna de las actividades o etapas del tratamiento en cuestión, conforme a lo dispuesto en el artículo 32 del RGPD. Según el planteamiento de OPENBANK, sólo deberían aplicarse determinadas medidas de seguridad reforzadas, a tratamientos de alto riesgo, pero esta idea no se corresponde con lo establecido en el RGPD donde las medidas deben ser apropiadas al riesgo presente en cada una de las fases del tratamiento.

En el ciclo del tratamiento, que comprende diversas y distintas actividades, no todo el riesgo tiene porqué ser uniforme, pueden existir diversos niveles de riesgos en las distintas etapas del tratamiento, dependiendo de las actividades que lo constituyen. Y si en una fase hay un mayor riesgo, aunque no todo el tratamiento sea de un mayor riesgo, deberían aplicarse medidas adecuadas.

En consecuencia, se trata de dos hechos distintos con distinto fundamento jurídico. En el artículo 25 del RGPD el bien jurídico que se protege es el cumplimiento del RGPD, en cuanto a la obligación de diseño del tratamiento en toda su extensión, identificando y valorando los riesgos en los derechos y libertades de los interesados a los efectos de implementar medidas técnicas y organizativas apropiadas para aplicación efectiva de los principios de protección de datos, para cumplir con la gestión del cumplimiento del RGPD; lo que no ha ocurrido en este caso, al no haberse siquiera evaluado (ni antes ni durante la realización del tratamiento) la posibilidad de que los clientes enviaran la información requerida en virtud del Capítulo II de la LPBCFT y cómo garantizar el cumplimiento de lo dispuesto en el RGPD. Y ni tan siquiera se le dio respuesta a la inquietud, al problema planteado por la parte reclamante respecto a la protección de sus datos personales en esta cuestión. El sistema ni tan siquiera tenía prevista una alarma ante cualquier cuestión que pudiera afectar los derechos y libertades de los clientes en materia de protección de datos, esto es un procedimiento implantado por el responsable del tratamiento que se pusiera en marcha ante cualquier fallo del propio sistema, ya fuera alertado por un cliente, por un empleado o detectado por la propia empresa. En este caso era remisión de documentación con datos financieros, pero podría haber sido cualquier cuestión planteada en protección de datos que afectara los derechos y libertades de los interesados. Al contrario, el sistema se limitó a contestar con una respuesta automática, sin analizar el fondo de lo planteado por la parte reclamante y sin proporcionarle una respuesta satisfactoria (esto es, sin brindarle un medio apropiado para compartir tal información). Y el responsable del tratamiento,

OPENBANK, tampoco se puso a trabajar tras el requerimiento efectuado por el cliente, implantando un sistema que impidiese dejar desamparados a sus clientes cuando les formularan cualquier cuestión, cualquier problemática en materia de protección de datos. Cabe recordar que se trata de un derecho fundamental. De riesgos en los derechos y libertades de los interesados. De evitar su materialización. Si nada se prevé, en los términos del sistema preventivo de enfoque de riesgos dispuesto por el RGPD, tarde o temprano el riesgo se va a materializar.

Por su parte, el artículo 32 RGPD se refiere a la seguridad del tratamiento, esto es, a la protección de los datos personales objeto de tratamiento en cuanto a la aplicación de medidas que garanticen un nivel de seguridad adecuado al riesgo, establecidas por el responsable del tratamiento, precepto infringido en el presente caso, donde se realizó un tratamiento por parte de OPENBANK, en el que no se proporcionaba al interesado un medio seguro para facilitar la información requerida por OPENBANK, lo cual ocasionó que en el caso concreto de la parte reclamante tuviera que enviar la documentación solicitada a través de un simple correo electrónico, pese a haber solicitado al banco un medio alternativo para ello, sin que éste se le hubiera facilitado. Todo ello pese a que OPENBANK en sus documentos reconoce que se trataba de un riesgo de impacto “alto” para los derechos y libertades de los interesados.

Por todo lo expuesto, se desestima la presente alegación.

En cuanto a la existencia de un concurso medial de infracciones, además de lo ya expuesto, esta Agencia desea señalar que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD, dado que el RGPD tiene su propio principio de proporcionalidad.

Y ello porque el RGPD es un sistema cerrado y completo.

El RGPD es una norma europea directamente aplicable en los Estados miembros, que contiene un sistema nuevo, cerrado, completo y global destinado a garantizar la protección de datos de carácter personal de manera uniforme en toda la Unión Europea.

En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne su finalidad última que es la garantía efectiva y real del derecho fundamental a la Protección de Datos de Carácter Personal. Lo contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

De hecho, una muestra específica de la inexistencia de lagunas en el sistema del RGPD es el artículo 83 del RGPD que determina las circunstancias que pueden operar como agravantes o atenuantes respecto de una infracción (art. 83.2 del RGDP) o que especifica la regla existente relativa a un posible concurso medial (art. 83.3 del RGPD).

A lo anterior hemos de sumar que el RGPD no permite el desarrollo o la concreción de sus previsiones por los legisladores de los Estados miembros, a salvo de aquello que

el propio legislador europeo ha previsto específicamente, delimitándolo de forma muy concreta (por ejemplo, la previsión del art. 83.7 del RGPD). La LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que éste le permite y con el alcance que éste le permite.

Ello es así porque la finalidad pretendida por el legislador europeo es implantar un sistema uniforme en toda la Unión Europea que garantice los derechos y libertades de las personas físicas, que corrija comportamientos contrarios al RGPD, que fomente el cumplimiento, que posibilite la libre circulación de estos datos.

En este sentido, el considerando 2 del RGPD determina que:

> *"(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".* (el subrayado es nuestro)

E indica el considerando 13 del RGPD que:

> *"(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".* (el subrayado es nuestro)

En este sistema, lo determinante del RGPD no son las multas. Los poderes correctivos de las autoridades de control previstos en el art. 58.2 del RGPD conjugado con las disposiciones del art. 83 del RGPD muestran la prevalencia de medidas correctivas frente a las multas.

Así, el art. 83.2 del RGPD dice que "*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j).".*

De esta forma las medidas correctivas, que son todas las previstas en el art. 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.

Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

Por ello, el art. 83.1 del RGPD previene que "*Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasoria".*

Las multas han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

Para que dicho sistema funcione con todas sus garantías en necesario que varios elementos se desplieguen de forma íntegra y completa. La aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español al permitirlo el propio RGPD-, ya sea por la aplicación de un concurso medial distinto del dispuesto en el RGPD, restaría efectividad al sistema que perdería su sentido, su finalidad teleológica, la voluntad del legislador, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

El RGPD está dotado de su propio principio de proporcionalidad que ha de ser aplicado en sus estrictos términos.

Y ello porque no hay laguna legal, no hay aplicación supletoria del art. 29 del RGPD.

Amén de lo expuesto, cabe significar que no hay laguna legal respecto de la aplicación del concurso medial. Ni el RGPD permite ni la LOPDGDD dispone la aplicación supletoria de las previsiones del art. 29 de la LRJSP.

En el Título VIII de la LOPDGDD relativo a "Procedimientos en caso de posible vulneración de la normativa de protección de datos", el artículo 63 que abre el Título se dispone que *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.".* Si bien existe una remisión clara a la LPACAP, no se establece en absoluto una aplicación subsidiaria respecto de la LRJSP que no

contiene en su articulado disposición alguna relativa a procedimiento administrativo alguno.

De igual forma que la AEPD no está aplicando los agravantes y atenuantes dispuestos en el art. 29 de la LRJSP, puesto que el RGPD establece los suyos propios, por ende, no hay laguna legal ni aplicación subsidiaria del mismo, tampoco cabe la aplicación de apartado relativo al concurso medial y por idénticas razones.

Por su parte, en cuanto al análisis del caso concreto objeto del presente procedimiento sancionador, cabe destacar que sin que resulte de aplicación el art. 29 de la LRJSP por los motivos expuestos, tampoco habría concurso medial.

El artículo 29.5 de la LRJSP establece que *"Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*".

Pues bien, el concurso medial tiene lugar cuando en un caso concreto la comisión de una infracción es un medio necesario para cometer otra distinta.

Los hechos constados determinan la comisión de dos infracciones distintas, sin que la conculcación del artículo 25 del RGPD, tal y como asevera OPENBANK, sea el medio necesario por el que se produce la infracción del artículo 32 del RGPD.

Es posible que en la aplicación por parte del responsable del tratamiento de la privacidad desde el diseño y por defecto, a fin de cumplir los requisitos del RGPD y proteger los derechos y libertades de los interesados, incorporando un enfoque de protección de datos desde el diseño y por defecto, se adopten unas medidas técnicas y organizativas de seguridad que no garanticen un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas.

Y viceversa, es posible que un responsable de tratamiento no realice un análisis en condiciones de las medidas que garanticen el cumplimiento normativo de la organización, pero que tenga adoptadas unas medidas de seguridad que sí que resulten apropiadas, porque sirvan a dicha finalidad y ya estuvieran implantadas.

Como ya se ha indicado anteriormente, en el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de OPENBANK, toda vez que no se ha incluido la actividad de recogida de datos de los clientes en el denominado "ciclo de vida del tratamiento" de su fichero Excel de documento de evaluación de impacto de protección de datos (aportado durante el período de prueba del presente procedimiento); por ello, al no preverse siquiera esta actividad, no se han aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados.

También ha quedado de manifiesto que la organización no contaba con un procedimiento adecuado para dar debida respuesta a una preocupación de un cliente sobre una cuestión de protección de datos, toda vez que en el presente caso la parte reclamante en su correo de 10 de julio de 2021 manifestó su disconformidad respecto a enviar los datos a través de un correo electrónico no cifrado. Incluso indica que

preguntó a OPENBANK pero no se le ofreció otra opción. Es más, la parte reclamante aporta la solución que más tarde es la adoptada por OPENBANK, en tanto dijo "…*el banco no ofrece la posibilidad de cargar los datos de forma segura, por ejemplo, a través del portal del cliente (…)".* Y solicitó que *"comprueben el proceso desde el punto de vista de la protección de datos y, en su caso, tomen las medidas oportunas".* Sin embargo, no es hasta el inicio del presente procedimiento sancionador que OPENBANK ha revisado esta cuestión y ha adoptado una nueva solución en aras de cumplir con la normativa de protección de datos.

Por lo que respecta a la vulneración del artículo 32 del RGPD, ésta se fundamenta en que el único canal de comunicación para el envío de documentos ofrecido a los clientes (entre ellos, la parte reclamante), tal y como consta en los hechos probados, era contestar al propio correo electrónico, y que dicho medio de envío no era un medio adecuado en función del riesgo que podía existir para los derechos y libertades de los interesados. En el caso concreto, OPENBANK no facilitó a su cliente un medio apropiado para aportar la documentación ni siquiera pese a las advertencias de la parte reclamante en este sentido, por lo que el envío se hizo sin las medidas de seguridad adecuadas.

Y ello pese a que los documentos 4 y 5 presentado por OPENBANK junto con sus alegaciones, denominados "Evaluación de impacto- Seguimiento de clientes y operaciones sensibles", versión agosto 2021 y octubre de 2022, respectivamente, en el apartado "13. Seguridad" se ha calificado el riesgo como de impacto alto. Además, en la versión de octubre de 2022, en la página 43 se ha incluido la siguiente indicación sobre "*Control y riesgo residual*": "*Se ha asegurado que los canales de comunicación con clientes como consecuencia asuntos relacionados con la prevención del blanqueo y financiación del terrorismo cuentas con medidas técnicas necesarias para garantizar la protección de sus datos personales. Los clientes se identificarán mediante su DNI y clave de acceso al área privada de cliente*".

Por todo lo expuesto, se desestima la presente alegación.

CUARTA.- ACERCA DEL CUMPLIMIENTO POR OPENBANK DEL PRINCIPIO DE PROTECCIÓN DE DATOS DESDE EL DISEÑO

OPENBANK alega que:

> • La privacidad desde el diseño se refiere al análisis integral del tratamiento y de los riesgos que el mismo puede deparar para los derechos y libertades de los interesados. De este modo, sólo podría considerarse que dicho principio ha sido incumplido en caso de acreditarse que el sancionado no había llevado a cabo ese proceso, de forma que el hecho de que el resultado del mismo no sea coincidente con lo que la AEPD considere adecuado no implica falta de cumplimiento del artículo 25 del RGPD sino, en su caso, la infracción de otra de sus previsiones.

La AEPD en su Propuesta de Resolución ni siquiera realiza una mínima valoración acerca de esta alegación, que ignora completamente, tratando nuevamente de vincular el supuesto incumplimiento del principio de privacidad desde el diseño con el simple hecho de no haberse ofrecido al interesado un medio alternativo para la remisión de

los documentos que le fueron solicitados por OPENBANK para acreditar el origen de los fondos de tres operaciones realizadas en el mismo, tal y como le impone la LPBCFT.

Al respecto, esta Agencia desea señalar que el artículo 25 del RGPD no entraña únicamente un "análisis integral del tratamiento y de los riesgos que el mismo puede deparar para los derechos y libertades de los interesados", sino que exige, además, que se apliquen medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos y se integren las garantías necesarias para cumplir los requisitos del RGPD y proteger los derechos de los interesados. En este sentido, el artículo 73. d) de la LOPDGDD considera infracción grave a los efectos de la prescripción "*La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679*".

En el presente caso, no se trata únicamente de que no se le ofrecía al interesado (ni a los clientes en general) un medio alternativo para la remisión de los documentos solicitados en virtud del Capítulo II de la LPBCFT, sino que se trata de que el responsable del tratamiento no preveía dicho tratamiento, lo que se pone de manifiesto en el documento de evaluación de impacto vigente en julio de 2021 (documento aportado durante la fase de prueba del presente procedimiento sancionador) en el que ni siquiera se contemplaba el citado tratamiento (el envío de tal documentación por parte de los clientes). Y que recién en agosto de 2021 se incorporó tal tratamiento en la evaluación de impacto de seguimiento de clientes, si bien no fue hasta octubre de 2022 que se incorporó la posibilidad de que los clientes enviaran la documentación a través del área de cliente de OPENBANK, posibilidad planteada por la parte reclamante ya en julio de 2021 y que el mismo documento de 2021 preveía como posibilidad a ser implementada. Y ello ni siquiera teniendo en cuenta que la misma evaluación de impacto de 2021 consideraba que el posible impacto para los derechos y libertades de los interesados era alto.

Alega también OPENBANK que el fundamento de derecho III de la Propuesta de Resolución añade una cuestión adicional que no se encontraba en el Acuerdo de Inicio y que ahora se incorpora a aquélla con la finalidad de justificar el cambio de enfoque en la imposición de esta sanción: la falta de privacidad desde el diseño se debe a que OPENBANK no ha previsto mecanismos que permitan "retroalimentar" el análisis previamente realizado y tener en cuenta el feedback que al responsable del tratamiento puedan proporcionar los interesados.

Es decir, la privacidad desde el diseño no sólo exige un análisis de los riesgos derivados del tratamiento que, necesario es decirlo, en este caso no se han materializado en modo alguno, sino que exige modificar las circunstancias y características de ese tratamiento en virtud del feedback recibido de los interesados, de forma que, ante una comunicación dirigida a OPENBANK por un interesado concreto, sólo se considerará cumplido el artículo 25 del RGPD si OPENBANK modifica la evaluación de los riesgos previamente realizada y modifica igualmente las medidas técnicas y organizativas que el tratamiento conlleve, incluso aun cuando

dicho feedback sólo se refiera a un supuesto riesgo potencial, y nunca acreditado, referido por un solo cliente.

Al respecto, esta Agencia desea señalar que OPENBANK acierta al afirmar que la protección de datos desde el diseño y por defecto implica adoptar los mecanismos necesarios para reevaluar de forma continua los tratamientos que se realicen, lo cual implica, entre otras medidas, contar con “mecanismos que permitan “retroalimentar” el análisis previamente realizado y tener en cuenta el feedback que al responsable del tratamiento puedan proporcionar los interesados”, en su caso.

En cuanto a la necesidad de que los riesgos derivados del tratamiento deban materializarse, cabe destacar que el artículo 25 del RGPD no exige que tales riesgos se produzcan, más bien al contrario, obliga a que se adopten las medidas apropiadas precisamente para evitar que tales riesgos pudieran materializarse.

Por último, esta Agencia desea indicar que no se pretende que por una comunicación realizada por un interesado concreto “sólo se considerará cumplido el artículo 25 del RGPD si OPENBANK modifica la evaluación de los riesgos previamente realizada y modifica igualmente las medidas técnicas y organizativas que el tratamiento conlleve, incluso aun cuando dicho feedback sólo se refiera a un supuesto riesgo potencial, y nunca acreditado, referido por un solo cliente”. Pero es que en el presente caso ni siquiera se le ha dado un curso debido a la problemática presentada por la parte reclamante ni tampoco ha quedado acreditado que se hubiera arbitrado mecanismos para proporcionarle otros medios, más adecuados en función del riesgo existente para sus derechos y libertades, por los cuales pudiera proporcionar la información solicitada. Es más, en agosto de 2021 el documento de evaluación de impacto de seguimiento de clientes ya había indicado que el impacto para los derechos y libertades de los interesados era alto y que debía implementarse la posibilidad de que los clientes aportaran la información solicitada a través del área privada del banco. Pero no fue hasta octubre de 2022, más de un año más tarde, que tal posibilidad fue habilitada. Todo ello no hace más que evidenciar que OPENBANK no tenía implantada en su organización un enfoque de protección de datos desde el diseño y por defecto, al menos en lo relativo al tratamiento objeto del presente procedimiento sancionador.

Alega OPENBANK que había llevado a cabo una adecuada evaluación de los riesgos derivados del tratamiento, estableciendo las medidas oportunas para paliarlos e incluso adoptando medidas relacionadas con la cuestión analizada en el presente expediente con anterioridad al momento en que la parte reclamante se puso en contacto con aquélla, aun cuando su implementación fuera posterior.

Y que en el momento en que se produjeron los hechos que han dado lugar al presente procedimiento, OPENBANK había llevado a cabo una evaluación de impacto en la protección de datos en relación con los tratamientos vinculados al cumplimiento de las obligaciones de diligencia debida previstas en la LPBCFT. Es decir, había efectuado un análisis detallado de los riesgos derivados del tratamiento e implementado las medidas oportunas para paliar dichos riesgos. En este sentido, el hecho de que la AEPD considere una medida supuestamente insuficiente no puede implicar que por la misma se niegue que las medidas fueron adoptadas, como parece indicarse en la Propuesta de Resolución.

Al respecto, esta Agencia desea señalar que el documento 4 aportado junto con las alegaciones al acuerdo de inicio del presente procedimiento sancionador indica que es de fecha agosto de 2021, mientras que el primer correo enviado a la parte reclamante es del 7 de julio de 2021. Por tanto, este documento es posterior a los hechos reclamados.

En cuanto al análisis de los riesgos efectuado en el citado documento, esta Agencia se reitera en lo ya indicado anteriormente sobre por qué se considera infringido el artículo 25 del RGPD.

Indica OPENBANK que ha aportado las diversas evaluaciones de impacto en la protección de datos que ha llevado a cabo en relación con este tratamiento, si bien no puede negar su extrañeza ante el hecho de que no figure en el expediente administrativo la remitida en respuesta al requerimiento de prueba efectuado por aquélla y que se adjuntó al escrito dirigido por OPENBANK a esa AEPD en fecha 19 de diciembre (folio 699 del expediente administrativo), al que no se acompaña la citada evaluación de impacto.

Al respecto, esta Agencia desea señalar que al generarse la copia del expediente para el envío a OPENBANK, el documento con la evaluación de impacto al momento de los hechos, por tratarse de un fichero de tipo Excel no aparece su contenido en la copia generada, pero sí que se encuentra incorporado en los sistemas de información de esta Agencia y se hace referencia a su contenido tanto en los hechos probados como en los fundamentos de derecho de la presente resolución.

Alega OPENBANK también que la AEPD parece negar la virtualidad de los citados documentos, llegando incluso a hacer referencia a calificar como “supuesta evaluación de impacto” aquélla que previó el establecimiento de mecanismos para que los documentos pudieran ser facilitados por los interesados en su área privada de la web y la App de OPENBANK, algo que consta expresamente en la evaluación efectuada por OPENBANK.

Y en este punto, OPENBANK desea clarificar que las evaluaciones aportadas (su contenido, en realidad) podrán no coincidir con lo que esa AEPD espera, pero en modo alguno pueden ser calificadas de “supuestas” a menos que la Agencia acredite contar con evidencias que permitan efectuar semejante aserto. Entiende OPENBANK que la consideración efectuada por esa AEPD carece del más mínimo fundamento y supone una imputación de suma gravedad dirigida contra OPENBANK que, cuanto menos, debería contar con algún soporte que permita convertir un documento adoptado por OPENBANK en un “supuesto” documento. Al propio tiempo, difícilmente puede ser calificado como “supuesto” un documento en el que se incorporan medidas que, con mayor o menor celeridad, han sido efectivamente implementadas por OPENBANK.

Al respecto, esta Agencia desea señalar que los documentos aportados por OPENBANK junto con sus alegaciones al acuerdo de inicio y durante la fase de prueba del presente procedimiento sancionador no se presentan debidamente firmados, por lo que resulta imposible acreditar su autenticidad e integridad ni garantizar su fecha. Tampoco ha entrado a valorar esta Agencia el contenido de los citados documentos en cuanto a si cumplen o no con los requisitos exigidos a una

evaluación de impacto de protección de datos personales en los términos exigidos por el RGPD. De ahí la calificación de “supuestos” que realizó esta Agencia en su propuesta de resolución.

Alega OPENBANK que la AEPD no acredita en modo alguno que los riesgos invocados por la misma a lo largo del procedimiento no sólo se hayan materializado, lo que en ningún caso ha sucedido, sino que existan en la realidad, por cuanto centra su fundamentación en la supuesta insuficiencia del correo electrónico como medio de comunicación, pese a que OPENBANK ya puso de manifiesto la validez de este medio para la transmisión de la información.

Al respecto, esta Agencia se reitera en que el artículo 25 del RGPD no exige que tales riesgos se produzcan, más bien al contrario, obliga a que se adopten las medidas apropiadas precisamente para evitar que tales riesgos pudieran materializarse.

Igualmente, alega OPENBANK que, teniendo en consideración que tanto la AEPD como el EDPB consideran que la evaluación del impacto del tratamiento en los derechos de los interesados debe ser un proceso dinámico y sucesivamente revisado, OPENBANK llevó a cabo sucesivas evaluaciones. No obstante, la AEPD niega valor alguno al hecho de que ese proceso implicase la adopción posterior de otras medidas complementarias para la aportación de los documentos, dado que la revisión continua de los tratamientos, defendida por la propia AEPD, es ahora considerada por la AEPD un proceso reactivo (incluso aunque en el momento de producirse no existiera reclamación alguna sobre el particular) y constitutivo de un mero “parche”. Y si por “parche” debe entenderse, según el Diccionario de la Real Academia Española, una “solución provisional, y a la larga poco satisfactoria, que se da a algún problema”, parece resultar que esa solución aparentemente insuficiente es la que la AEPD considera aplicable en este caso.

OPENBANK considera, en este punto, que la Propuesta de Resolución no puede mantener simultáneamente una idea y la contraria con el objetivo de sancionarle: no es posible decir que OPENBANK no adoptó medidas desde el diseño para lograr la minimización de los riesgos del tratamiento mediante la sucesiva revisión de las evaluaciones de impacto llevadas a cabo en relación con el tratamiento y, al mismo tiempo, considerar que las medidas adoptadas como consecuencia de esa evaluación, que coinciden con las que la AEPD entiende adecuadas, son un mero parche, es decir, no resultan satisfactorias para resolver el supuesto problema planteado en relación con el medio utilizado para la remisión de documentos.

Tampoco resulta posible imputar a OPENBANK que las medidas no se implantasen “antes de que el sistema esté en funcionamiento”, volviendo a hacer referencia a la consideración de las medidas implementadas como “parche”. Como ya se ha dicho, OPENBANK se encuentra obligada a exigir a sus clientes la acreditación del origen de los fondos, es decir, a poner en funcionamiento el “sistema” mencionado, desde al menos la entrada en vigor de la LPBCFT. Y en esa fecha no existía norma alguna que hiciera referencia al principio de privacidad desde el diseño o a la obligación de realización de una evaluación de impacto en la protección de datos, sin perjuicio de que OPENBANK adoptase las medidas técnicas y organizativas que consideró procedentes para mitigar cualquier riesgo que el tratamiento pudiera ocasionar en el derecho a la protección de datos personales de sus clientes. La AEPD parece

considerar que OPENBANK debía ser consciente de una serie de obligaciones que, sin embargo, no se adoptarían en un texto legal hasta seis años después del inicio del tratamiento y no resultaban plenamente aplicables hasta transcurridos ocho años desde dicha fecha.

OPENBANK considera que no es razonable exigir a la misma obligaciones desconocidas ni que proceda a interrumpir los procesos de cumplimiento de la normativa de prevención del blanqueo de capitales, con el consiguiente incumplimiento de esa normativa, como consecuencia de la entrada en vigor del RGPD, si bien en todo caso reitera que llevó a cabo la correspondiente evaluación de impacto en la protección de datos así como la adopción de las medidas técnicas y organizativas que permitían mitigar cualesquiera riesgos derivados del tratamiento.

Al respecto, esta Agencia reconoce que es posible que la utilización del término "parche" en su propuesta de resolución no ha sido lo más acertado, razón por la cual se dará una nueva redacción, lo cual no obsta a que esta Agencia se mantiene en que OPENBANK no ha implementado la protección de datos desde el diseño y por defecto, en lo que refiere al tratamiento objeto del presente procedimiento sancionador, por todas las razones anteriormente detalladas de forma extensa. La respuesta ha sido reactiva y no proactiva, y generada una vez conocida la reclamación planteada por el interesado ante la autoridad de control.

Por último, esta Agencia se reitera en que si bien es cierto que el enfoque del RGPD y la LOPDGDD resultó completamente novedoso respecto la normativa de protección de datos anterior, no es menos cierto que OPENBANK contó con tiempo más que suficiente a lo largo de los tres años (seis años si se cuenta desde la adopción del texto RGPD) que transcurrieron entre que se aprobó el RGPD (abril de 2016), hasta que resultó de aplicación el RGPD (mayo 2018, lo que concedía dos años largos para la preparación y adaptación al RGPD) y los hechos objeto de la reclamación a que dio lugar el presente procedimiento sancionador (julio de 2021) para adecuar sus tratamientos a lo dispuesto en los artículo 25 y 32 del RGPD (cuatro años si se tiene en cuenta que recién se adoptaron las medidas para que los clientes pudieran compartir la información solicitada a través de su área privada en octubre de 2022). Por supuesto que hubiera sido imposible que se tuviera un enfoque de protección de datos desde el diseño antes de realizar el tratamiento, cuando éste tuvo lugar muchos años antes de que el RGPD existiera, pero resulta innegable que el principio de protección de datos desde el diseño no implica únicamente que las medidas debían ser previas al tratamiento, sino que el propio artículo 25 del RGPD indica "*tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento*", esto es, no solo de forma previa sino a lo largo de que ese tratamiento tenga lugar y siempre que se determinen los medios de tratamiento, lo cual es una decisión que se va tomando también a lo largo del tiempo, conforme van cambiando las circunstancias y las posibilidades de cada momento.

Por todo lo expuesto, se desestima la presente alegación.

QUINTA.- ACERCA DE LA PRETENDIDA VULNERACIÓN POR OPENBANK DEL ARTÍCULO 32 DEL RGPD

Se alega que la medida adoptada por OPENBANK, no podía considerarse contraria a lo establecido en el artículo 32 del RGPD, resultando la medida existente al tiempo de producirse los hechos, es decir, el envío de la documentación acreditativa del origen de los fondos, adecuada a la vista de los riesgos que el tratamiento podría producir en los derechos de los clientes.

Y que en ningún caso podía alcanzarse la conclusión de que el correo electrónico no fuera el medio adecuado para la realización de dichos envíos a la vista de lo señalado por el Centro Criptológico Nacional, que, lejos de considerar el uso del correo como indeseable, ponía de manifiesto cómo los principales proveedores de este servicio habían adoptado medidas tendentes al cifrado y autenticación de los correos electrónicos.

No obstante, se reconoce que el informe del Centro Criptológico Nacional indicaba que existen usuarios que hacen un uso “descuidado” del servicio de correo electrónico. Sin embargo, alega que no es posible que OPENBANK haya de adoptar las medidas técnicas y organizativas aplicables al tratamiento de datos que el mismo efectúa atendiendo al uso más o menos descuidado que los usuarios puedan hacer de los servicios de correo electrónico, pues ello implica desplazar a OPENBANK la responsabilidad por la actuación de sus clientes, lo que en modo alguno puede considerarse ajustado al principio de responsabilidad consagrado en nuestra normativa sancionadora.

Se alega que frente a estos argumentos, la Propuesta de Resolución, no obstante al llevar a cabo la reproducción del contenido del Acuerdo de Inicio en su fundamento de derecho VIII, se limita a rebatir lo alegado con la categórica afirmación de que “esta Agencia si pone en duda que el correo electrónico constituye una vía de comunicación segura para el envío de documentación cuando debe garantizarse su confidencialidad, como es el caso, este es el motivo de la imputación de la infracción del artículo 32 del RGPD”, invocando posteriormente lo señalado en el citado informe del Centro Criptológico Nacional.

En este sentido, alega OPENBANK que, salvo error por su parte, en los numerosos informes, resoluciones, guías y directrices procedentes de esa AEPD, así como en los emanados del EDPB no se conoce indicio alguno que permitiera a OPENBANK considerar que el uso del correo electrónico debía ser una medida que había de ser proscrita en lo que a la recepción de datos personales para su posterior tratamiento se refiere. No cabe duda de que esta medida constituye la técnica usual y habitual de comunicación entre los sujetos obligados por las normas de protección de datos, pertenecientes a cualquier sector de actividad, y sus clientes y, sin embargo, no se conoce que la misma hubiera sido puesta en cuestión por esa AEPD hasta el presente expediente sancionador.

Ello supone un cambio de criterio que, cuanto menos, puede ser calificado de sorpresivo para OPENBANK y que, no obstante, implica la imposición al mismo de sendas sanciones por un importe total de 2.500.000 euros. Y dicha sanción se impone sobre la base de la mera existencia de una comunicación dirigida a OPENBANK por un cliente en la que en modo alguno se acredita la producción, y menos aún la materialización, de un riesgo para su derecho a la protección de datos. De este modo, nos encontraríamos ante lo que la sentencia de la Sala de lo Contencioso-

Administrativo de la Audiencia Nacional de 23 de diciembre de 2022 (recurso 104/2021) califica como “una infracción potencial que no está castigada por las normas de protección de datos”.

Al respecto, esta Agencia desea señalar que, en el presente caso, debido a la especial protección que requerían los datos aportados por los clientes, por el mayor riesgo que implicaba para sus derechos y libertades, tal y como se explicó de forma detallada anteriormente, debieron adoptarse medidas de seguridad reforzadas.

En el presente caso, esta Agencia considera que el envío de la información solicitada en virtud del Capítulo II de la LPBCFT mediante un simple correo electrónico no era una medida adecuada en función del riesgo para los derechos y libertades de las personas físicas. Y ello no sólo por el uso descuidado que pudiera hacerse del correo electrónico. El citado informe del Centro Criptológico Nacional indicaba que algunas de las medidas que se hacía referencia, adoptadas por los proveedores de correo más conocido, eran susceptibles de ser atacadas y que, incluso en el caso de que se establezca la comunicación de forma satisfactoria, los servidores de correo por los que pasa el email hasta alcanzar el destino tendrían acceso a su contenido. Por lo que concluía que “se deduce que no es suficiente con delegar la seguridad del correo electrónico a las tecnologías subyacentes encargadas de hacer llegar el mismo a su destinatario”.

Tampoco se preveía en los protocolos de seguimiento de clientes brindar algún tipo de asistencia al cliente para cifrar los documentos enviados ni cualquier otra facilidad, por lo que la información enviada a través del correo electrónico cabía esperar que tampoco contara con tal medida de seguridad adicional, la cual tampoco se encuentra extendida entre los usuarios y requiere de ciertos conocimientos técnicos. En este sentido esta Agencia indicaba que hacer depender la seguridad del nivel de los conocimientos técnicos del propio cliente y de que tenga las herramientas adecuadas para ello suponía una transferencia del riesgo de OPENBANK al cliente.

En cuanto a que OPENBANK debió adoptar las medidas atendiendo al uso más o menos descuidado que los usuarios puedan hacer de los servicios de correo electrónico, esta Agencia considera que en modo implica una transferencia del riesgo a OPENBANK por la actuación de sus clientes, pero sí que se trata de un riesgo más que probable y esperable, que OPENBANK debió valorar e intentar impedir que se produzca, en especial teniendo en cuenta que el propio banco valoró que el impacto que podía tener tal tratamiento en los derechos y libertades de las personas físicas era alto, tal y como constaba en la evaluación de impacto de agosto 2021.

En cuanto a que ni en los informes, resoluciones, guías y directrices de la AEPD ni del EDPB se conoce indicio alguno que permitiera a OPENBANK considerar que el uso del correo electrónico debía ser una medida que había de ser proscrita en lo que a la recepción de datos personales para su posterior tratamiento se refiere, es necesario recordar que no se trata de que el envío de correo electrónico constituya un medio no seguro en cualquier caso y respecto de cualquier tratamiento, pero resulta innegable que en el presente caso no era un medio adecuado para compartir la información exigida en virtud del Capítulo II de la LPBCFT, el cual exigía la adopción de unas medidas reforzadas.

En cuanto a que se sanciona con una multa de 2.500.000 euros sobre la base de una comunicación dirigida a OPENBANK por un cliente en la que no se acredita la materialización de un riesgo para su derecho a la protección de datos, esta Agencia desea señalar que la infracción del artículo 32 del RGPD si bien se tuvo conocimiento como consecuencia de la reclamación de un cliente de OPENBANK, no es menos cierto que la infracción que se constata no lo es únicamente respecto de ese cliente sino de todos los clientes de OPENBANK, toda vez que la única posibilidad proporcionada a sus clientes para el envío de la documentación solicitada en virtud del Capítulo II de la LPBCFT hasta octubre de 2022 era enviar la citada información mediante un simple correo electrónico. Y respecto de que no se ha materializado el riesgo para sus derechos y libertades, esta Agencia señala que el artículo 32 del RGPD no exige que tal riesgo se materialice, más bien al contrario, se trata de que se adopten las medidas apropiadas para evitar que tal riesgo se materialice. Por tanto, no se trata en el presente caso de "una infracción potencial que no está castigada por las normas de protección de datos", sino que se ha constatado que las medidas adoptadas para el envío de la documentación solicitada en virtud del Capítulo II de la LPBCFT no eran las apropiadas en función del mayor riesgo que esta información podía implicar para los derechos y libertades de las personas físicas.

Por último, OPENBANK quiere clarificar que aportó como Documento número 9 junto con su escrito de alegaciones al Acuerdo de Inicio (folio 654 del expediente administrativo), certificación emitida por el Director de Tecnología y Operaciones de OPENBANK, en la que literalmente se indicaba lo siguiente:

> "*Que de conformidad con lo definido en el Plan de Desarrollo Tecnológico de Openbank, a 13 de octubre de 2022, la entidad tiene habilitado dentro del área privada de la página web (se requiere usuario y contraseña de acceso) un espacio para que los clientes puedan facilitar la documentación requerida en cumplimiento de lo dispuesto en el artículo 6 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo cuyo texto reza así:*
>
> > *"Artículo 6. Seguimiento continuo de la relación de negocios.*
> > *Los sujetos obligados aplicarán medidas de seguimiento continuo a la relación de negocios, incluido el escrutinio de las operaciones efectuadas a lo largo de dicha relación a fin de garantizar que coincidan con el conocimiento que tenga el sujeto obligado del cliente y de su perfil empresarial y de riesgo, incluido el origen de los fondos y garantizar que los documentos, datos e información de que se disponga estén actualizados"."*

Y que la propuesta de resolución se limita a indicar que OPENBANK no acredita la fecha de la puesta a disposición de sus clientes del procedimiento descrito.

Al respecto, esta Agencia desea señalar que tiene por cierto que se habilitó a 13 de octubre de 2022 la posibilidad de que los clientes puedan proporcionar la información requerida en virtud del Capítulo II de la LPBCFT a través de su área privada de la página web de OPENBANK.

SEXTA.- ACERCA DE LA VULNERACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD

Alega OPENBANK que las agravantes por la infracción del artículo 25 del RGPD y del artículo 32 del RGPD de la propuesta de resolución contienen casi literalmente las mismas consideraciones, lo cual, a su juicio, ello no hace sino poner de manifiesto la absoluta identidad de las dos conductas imputadas a OPENBANK, siendo así aplicable el principio non bis in idem, ya invocado con anterioridad.

Al respecto, esta Agencia se reitera en lo ya señalado en su respuesta a la alegada vulneración del principio non bis in idem.

Señala OPENBANK que la AEPD considera que la sanción es proporcional, dado que resulta sensiblemente inferior a los 885 millones de euros que constituye el 2% del volumen de facturación del Grupo Santander, al que pertenece OPENBANK, en el año 2021. Y que a tal efecto invoca la doctrina del Tribunal de Justicia de la Unión Europea en relación con la consideración del término “empresa”, con cita de diversas sentencias.

Sin embargo, OPENBANK considera preciso discrepar de esta consideración, dado que la AEPD en modo alguno ha demostrado en ningún momento del procedimiento que, más allá de la tenencia del 100% del capital social de OPENBANK, el Grupo Santander ejerza un papel decisorio en las políticas de OPENBANK y, menos aún, que su actuación en lo que respecta al cumplimiento de las normas de protección de datos (incluida la realización de evaluaciones de impacto en la protección de datos o la determinación de las medidas técnicas u organizativas que hayan de adoptarse en relación con un determinado tratamiento) proceda o sea siquiera interferida mínimamente por el Grupo Santander, siendo este poder de influencia el determinante utilizado por la jurisprudencia invocada en la Propuesta de Resolución para que proceda aplicar el concepto de empresa establecido en el derecho de la Unión y que, por tanto, pueda calcularse el importe de la sanción a partir del volumen de facturación del Grupo Santander y no exclusivamente de OPENBANK.

Y en este sentido, es preciso reiterar que corresponde a la AEPD la acreditación de ese poder de decisión, más allá de la titularidad del accionariado, sin que se haya efectuado prueba de cargo alguna en este sentido. Por el contrario, como resultará evidente a simple vista mediante la mera consulta de sus sitios web, las políticas de privacidad de OPENBANK y de las restantes sociedades del Grupo Santander son distintas, contando OPENBANK con un delegado de protección de datos que ninguna vinculación mantiene con los de las restantes empresas del Grupo.

Por tanto, no es dable efectuar el cálculo que establece la Propuesta de Resolución y que, a lo sumo, deberá efectuarse sobre el volumen de negocio de OPENBANK, por más que OPENBANK sea una empresa que forme parte del Grupo Santander.

Por el contrario, como resultará evidente a simple vista mediante la mera consulta de sus sitios web, las políticas de privacidad de OPENBANK y de las restantes sociedades del Grupo Santander son distintas, contando OPENBANK con un delegado de protección de datos que ninguna vinculación mantiene con los de las restantes empresas del Grupo.

Al respecto, esta Agencia desea recordar que, según consta en el "Informe anual 2021" del Grupo Santander, Banco Santander S.A. posee el 100% de la participación directa de OPENBANK, así como el 100% de los derechos de voto en OPENBANK. Por tanto, el poder de decisión que posee Banco Santander S.A. sobre OPENBANK resulta más que determinante, es absoluto. El hecho de contar con políticas de privacidad distintas o un delegado de protección de datos sin ninguna vinculación con los de las restantes empresas del Grupo tampoco modificaría tal situación.

En este sentido, el artículo 39.1 "*Funciones del delegado de protección de datos*" del RGPD establece que:

"1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto".

Como puede observarse, en ninguna de estas funciones se hace referencia a que el delegado de protección de datos tenga algún tipo de poder de decisión, lo cual queda reservado al responsable de tratamiento de los datos personales, como es lógico.

Por tanto, se desestima la presente alegación.

Alega OPENBANK que la Propuesta de Resolución considera que no procede tener en cuenta las medidas adoptadas para permitir la subida de documentos relacionados con el origen de los fondos a través del área privada de los clientes, aunque no aporta un solo argumento en este sentido.

Y que, no obstante, la AEPD es perfecta conocedora de que tal medida ya fue acordada como correctora en el momento de llevarse a cabo la evaluación de impacto en la protección de datos efectuada en agosto de 2021 y que consta en el expediente, si bien, como esa AEPD conoce perfectamente, los procesos de implementación de medidas técnicas en el marco de una organización como la de OPENBANK implican sucesivos procesos que se dilatan en el tiempo.

Por el contrario, alega OPENBANK que la propuesta no duda en considerar que el hecho de haberse adoptado esta medida debe perjudicar o agravar la conducta del

banco, dado que, sorprendentemente entiende la AEPD que ello corrobora la falta de diligencia de OPENBANK, lo cual le resulta incomprensible, dado que perjudicaría al que adopta un proceso aún más garantista que el exigible en beneficio de quien no lleva a cabo medida alguna en este sentido.

Al respecto, esta Agencia desea señalar que al momento de iniciarse el presente procedimiento sancionador (26 de agosto de 2022), ni tan siquiera a la firma del acuerdo de inicio en el cual se fijaron los agravantes de las infracciones de los artículos 25 y 32 del RGPD (3 de octubre de 2022), OPENBANK aún no había implementado la posibilidad de que los clientes facilitaran la información solicitada en virtud del Capítulo II de la LPBCFT a través de su área privada de la página web, la cual fue recién habilitada a partir del 13 de octubre de 2022, por lo que no puede ser valorada como atenuante. No obstante, sí que esta circunstancia se ha tenido en cuenta a la hora de valorar la duración de las infracciones así como para no imponer medidas que deba adoptar OPENBANK en este sentido.

En cuanto a que el haber adoptado esta medida parece perjudicar al banco, esta Agencia desea rechazar tal afirmación. No se trata de que le perjudique sino que esta Agencia considera que el hecho de que en el documento de evaluación de impacto de agosto de 2021 ya se hubiera solicitado la posibilidad de implementar tal medida, teniendo en cuenta el posible alto impacto que podía tener tal tratamiento en los derechos y libertades de las personas físicas y que no fuera hasta octubre de 2022, más de un año después, que tal posibilidad fuera implementada, por más que los procesos de implementación requieran de ciertos plazos, a juicio de esta Agencia los citados plazos han excedido de lo razonable y ha evidenciado una actitud negligente por parte de OPENBANK al respecto.

Por último, esta Agencia desea destacar que por supuesto que este criterio en modo alguno “perjudicaría al que adopta un proceso aún más garantista que el exigible en beneficio de quien no lleva a cabo medida alguna en este sentido”, sino que al contrario, quien no adoptara ninguna medida en este sentido evidentemente tendría un reproche mayor, su actitud sería valorada como aun más gravemente negligente, la duración de la infracción sería mayor y además de la multa se le impondrían medidas para dar cumplimiento a lo dispuesto por el RGPD.

En cuanto al número de personas afectadas por el tratamiento, alega OPENBANK que la Propuesta de Resolución contiene dos párrafos que no pueden considerarse, en modo alguno aceptables en lo que respecta a sus propios términos. En efecto, la argumentación efectuada por la AEPD en este punto es, íntegramente la siguiente:

“Desde OPENBANK se califica la aplicación de este criterio como “apriorismo carente del más mínimo fundamento”. Sin embargo, obedece a la más pura lógica considerar que no puede graduarse una sanción de la misma forma cuando, ante la falta de medidas apropiadas, el tratamiento afecta de forma potencial a cerca de dos millones de clientes, como en el presente caso. Si se sancionase de igual manera a una entidad con un pequeño número de interesados que pudieran ser potenciales afectados que a una gran empresa, entonces sí se estaría infringiendo el principio de proporcionalidad.

Además, alega OPENBANK que según el certificado aportado por el banco, el número de clientes impactados por este tipo de operaciones, una media cercana a los 13.000 interesados en los dos últimos años viene a confirmar que la falta de unas medidas técnicas y organizativas apropiadas puede poner en riesgo a un gran número de personas, la mayoría de los cuales envían por correo electrónico datos personales relativos a su patrimonio sin ninguna medida que proteja su confidencialidad."

Indica OPENBANK que la más elemental regla aritmética permite concluir que no es posible hacer referencia, como términos iguales o equivalentes a dos millones de clientes y a 13.000 (en total, y no como media anual). Sin embargo, del razonamiento de la AEPD parece deducirse que ambos términos son iguales, dado que el reproche que se incorporaba en el Acuerdo de Inicio, que sólo tenía en cuenta la potencial afectación a dos millones de clientes se mantiene en la propuesta de Resolución que, no obstante, parece considerar que es 13.000 la cifra que ha de tenerse en cuenta. Y téngase en cuenta que la sentencia de la Audiencia Nacional de 23 de diciembre de 2022, ya citada, niega a la AEPD la capacidad de imponer sanciones por incumplimientos potenciales de la normativa de protección de datos personales, siendo la doctrina sustentada en dicha sentencia perfectamente extrapolable al presente caso.

Al respecto, esta Agencia se reitera en que en el presente caso no se trata de "incumplimientos potenciales de la normativa de protección de datos personales" sino que los incumplimientos de los artículos 25 y 32 del RGPD han tenido lugar, aun cuando los riesgos que estos artículos pretenden evitar no se hubieran materializado, lo cual es la finalidad de tal normativa.

En cuanto a la cifra de afectados, esta Agencia tendrá en consideración que el número de potenciales afectados es el número total de clientes de OPENBANK (dos millones de clientes), que son aquellos a los que el banco podía solicitar que aportaran la documentación requerida en virtud del Capítulo II de la LPBCFT, mientras que el número de interesados directamente afectados ha sido de 13.000 clientes como media anual, lo cual daría un total de 65.000 clientes, teniendo en cuenta que habría 13.000 clientes directamente afectados por año, desde mayo de 2018 (cuando resultó de aplicación el RGPD) a octubre 2022 (cuando se habilitó la posibilidad de aportar la documentación a través del área privada de la web del banco), que sería el número de clientes a los que OPENBANK ha requerido que aporten la documentación en virtud de lo previsto en el Capítulo II de la LPBCFT, a los que no se les ha proporcionado un medio apropiado para su envío.

En cuanto a la supuesta agravación de la sanción como consecuencia de la presunta negligencia apreciada, y al margen de que se niegue de plano la concurrencia de aquélla en su conducta, OPENBANK alega que de lo afirmado por la AEPD se desprende que la existencia de dolo o negligencia en la actuación de un responsable o encargado del tratamiento deberá ser tomada en consideración para agravar su responsabilidad, cuando en realidad este hecho no puede sin más considerada agravante, sino condición sine qua non para poder apreciar la concurrencia de responsabilidad, como elemento imprescindible para que el mismo pueda ser objeto de reproche sancionador por una determinada conducta.

Es decir, con el razonamiento efectuado por la AEPD se llega a la conclusión de que un elemento que, en todo caso, debe ser valorado para apreciar la responsabilidad de una entidad opera asimismo como agravante. De este modo, cualquier vulneración de la normativa de protección de datos nace agravada a radice por el hecho de concurrir responsabilidad en el encartado.

Al respecto, esta Agencia desea señalar que la negligencia apreciada en la conducta de OPENBANK no es la mera negligencia exigida por nuestro ordenamiento jurídico, como elemento subjetivo de la infracción. Sino que se trata de una negligencia especialmente grave, toda vez que toda vez que la empresa no realizó un análisis en condiciones de los riesgos para los derechos y libertades de los interesados, que podía acarrear el compartir la documentación requerida en virtud de la LPBCFT a través un medio no suficientemente seguro, ni tampoco se adoptaron las medidas de seguridad apropiadas para facilitar un medio que no pusiera en riesgo la confidencialidad de esta información, ni siquiera cuando un cliente (como en el caso concreto de la parte reclamante) solicitó un medio alternativo para proporcionar la documentación exigida se le proporcionó una respuesta a su inquietud ni se le facilitó un medio de comunicación segura para ello, ni se le dio un curso adecuado a tal solicitud que permitiera reevaluar la adecuación del medio de comunicación elegido por la entidad para compartir tal información.

Alega OPENBANK también que la Propuesta de Resolución se refiere a la naturaleza de los datos objeto de tratamiento como circunstancia agravante, limitándose a indicar que la misma no tiene en consideración el hecho de que los mismos son calificados como “datos financieros”, algo que OPENBANK considera desvirtuado. No obstante, al margen de la naturaleza de tales datos, lo que no puede negarse es que la AEPD ha considerado producidas las infracciones a las que se refiere la Propuesta de Resolución en atención a la naturaleza de los datos objeto de tratamiento, de forma que convierte lo que ha sido considerado un elemento del tipo en una circunstancia agravante, conculcando así los más elementales principios del derecho administrativo sancionador.

Al respecto, esta Agencia rechaza que en el presente caso la naturaleza de los datos objeto de tratamiento constituyan un elemento del tipo infractor. 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 de las personas físicas, debe cumplirse con independencia de la naturaleza de los datos objeto de tratamiento. Lo que sí es cierto es que en el presente caso se trata de datos que merecen una especial protección, por lo que resulta de aplicación el agravante detallado en el apartado g) del artículo 83.2 del RGPD.

Por último, OPENBANK alega que la AEPD toma en consideración el giro o tráfico del banco en reiteradas ocasiones para agravar la cuantía de la sanción. Así, (i) la primera de la circunstancia es tomada en consideración para reforzar la potencial afectación de los hechos; (ii) al propio tiempo, respecto de la negligencia, se agrava la conducta de OPENBANK al entender que por su sector de actividad se le debe exigir una especial diligencia; y (iii) finalmente, se considera que el giro o tráfico de OPENBANK está vinculado a la realización de tratamientos, lo que debe suponer esa triple agravación derivada de este hecho. Es decir, a juicio de la AEPD cuando una entidad perteneciente al sector bancario comete una supuesta infracción, su conducta ha de

verse triplemente agravada por el mero hecho de cuál sea su actividad, lo que difícilmente puede considerarse acorde con el principio de proporcionalidad.

Al respecto, esta Agencia desea señalar que únicamente considera el giro o tráfico del banco para agravar la cuantía de la sanción respecto al agravante contemplado en el artículo 76.2 de la LOPDGDD, sobre la vinculación de la actividad del infractor con la realización de tratamientos de datos personales, toda vez que la actividad empresarial de OPENBANK requiere un tratamiento continuo de datos personales. No obstante, no es menos cierto que en la valoración del grado de diligencia exigible se pondera también la profesionalidad del sujeto, por lo que cuando la actividad del responsable es de “constante y abundante manejo de datos de carácter personales” se exige una mayor diligencia, en consonancia con lo dispuesto en la Sentencia de la Audiencia Nacional de 17/10/2007 (Rec. 63/2006).

IV
Valoración de la prueba practicada

La carencia de un medio seguro de envío de documentación en el “Protocolo de comunicaciones a clientes por alertas de PBC/FT: APERTURA Y GESTIÓN DE GAPS Versión de marzo de 2021”, argumentada en el acuerdo de inicio, motivó la necesidad de comprobar el cumplimiento efectivo de los principios de protección de datos del tratamiento en cuestión, para lo cual se estimó oportuno analizar la evaluación de impacto de protección de datos realizada por OPENBANK.

Con ocasión de las alegaciones al acuerdo de inicio presentadas, se presentaron el documento 4.- “Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles (versión agosto 2021)”, y el documento 5.-, “Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles (versión octubre 2022)”, ambos documentos incorporados al expediente de este procedimiento. Sin embargo, ninguno de estos documentos estaba vigentes en el momento de producirse los hechos, ya que la petición realizada por OPENBANK a la parte reclamante se produjo el 7 de julio de 2021. En consecuencia, se estimó oportuno la apertura de un período de prueba.

En el documento aportado por OPENBANK durante el período de prueba no se contempla en su valoración de riesgos la actividad de recogida de datos cuando sus clientes debían enviar documentación en cumplimiento de la LPBCFT, tal y como ocurre en el supuesto objeto del presente procedimiento sancionador.

IV
Especial protección de los datos proporcionados en virtud del Capítulo II de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBCFT)

La necesidad de una especial protección de los datos personales de carácter financiero es un criterio compartido con el Comité Europeo de Protección de Datos (CEPD), el cual, en cumplimiento del objetivo de garantizar la aplicación coherente del Reglamento General de Protección de Datos (según le atribuye el artículo 70 del RGPD) ha elaborado unas orientaciones para proporcionar una base clara y transparente para la fijación de sanciones por parte de las autoridades de supervisión

nacionales (Directrices 04/2022 sobre el cálculo de las sanciones administrativas bajo el RGPD).

En el apartado 4.2.3 de las citadas Directrices, se expresa lo siguiente (traducción no oficial):

"*Categorías de datos personales afectados*
58. En cuanto al requisito de tener en cuenta las categorías de datos personales afectados (artículo 83, apartado 2, letra g), del RGPD), el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por lo tanto, una respuesta más estricta en términos de multas. Esto se refiere, como mínimo, a los tipos de datos cubiertos por los artículos 9 y 10 del RGPD, y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión causa daños inmediatos o angustia al interesado (por ejemplo, datos de ubicación, datos sobre comunicaciones privadas, números de identificación nacionales o datos financieros, como resúmenes de transacciones o números de tarjetas de crédito)."

Por su parte, el artículo 32 bis de Ley 10/2010, añadido por el art. 3.15 del Real Decreto-ley 7/2021, de 27 de abril, exige unas medidas reforzadas a los sujetos obligados al tratamiento de datos personales relacionados con el ámbito de aplicación de norma:

"… *4. Los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos". (el subrayado es nuestro)*

En cumplimiento de la LPBCFT, las entidades obligadas pueden tratar datos financieros, pero no sólo datos de esta categoría también son tratados datos personales de diversa naturaleza: de identificación, de contacto o económicos (empresariales, profesionales, de inversiones…). La protección de datos en cumplimiento de la LPBCFT no puede verse limitada por los criterios aplicables tan sólo a uno de estos datos, cuando lo que trata de proteger es el acceso a la información que suponen todos estos datos personales, no sólo de forma individual, sino a su tratamiento de forma conjunta.

Por su parte, las "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679", en lo que aquí interesa indican: "*Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo (…) se deben considerar los nueve criterios siguientes: 1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito*

o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes…" (el subrayado es nuestro).

La actividad realizada por OPENBANK en virtud de lo dispuesto en el Capítulo II de la LPBCFT, por la que se le solicita a los clientes que aporten los "soportes que justifican un determinado ingreso, por cuanto permitirán de clarificar el origen de los fondos que han sido ingresados en la cuenta del cliente en OPENBANK" se enmarca dentro de una institución financiera que investigue a sus clientes en una posible base de datos contra el blanqueo de capitales y la financiación del terrorismo, razón por la que son operaciones que entrañan probablemente un mayor riesgo.

Y tanto ello es así, que son operaciones que entrañan probablemente un mayor riesgo, que la misma LPBCFT consideró conveniente incorporar la necesidad de realizar una evaluación de impacto de la protección de datos de los tratamientos a los que se refiere dicho artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

A mayor abundamiento, el Capítulo 9.2 del Manual de legislación europea en materia de protección de datos, elaborado por la Agencia de la Unión Europea para los Derechos Fundamentales, el Consejo de Europa, el Tribunal Europeo de Derechos Humanos y el Supervisor Europeo de Protección de Datos donde se refiere a los "datos financieros": "*A pesar de que los datos financieros no se consideran datos sensibles en virtud del Convenio 108 o del Reglamento general de protección de datos, su tratamiento requiere garantías especiales que garanticen la exactitud y la seguridad de los datos. En particular, los sistemas de pago electrónico necesitan incorporar medidas de protección de datos, es decir, protección de la privacidad o de los datos desde el diseño y por defecto".* La mención a la protección de la privacidad respecto a los sistemas de pago electrónico viene a resaltar la importancia de éstos, pero no excluye que, de igual manera, otros datos financieros puedan requerir garantías especiales, tal y como ocurre en el presente caso con los datos recogidos en virtud de lo dispuesto en el Capítulo II de la LPBCFT.

En cuanto a la Guía sobre la gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD, se diferencia entre tres tipologías de datos económicos que deben valorarse a la hora de determinar el nivel de riesgo de un determinado tratamiento para la realización de la DPIA, diferenciando entre estas tres categorías de datos:

- Datos relacionados con la "[s]*ituación económica, (P.ej., sin ser exhaustivos, renta personal, Ingresos mensuales, Patrimonio (bienes muebles/inmuebles), Situación laboral)*". A estos datos se les asigna un "riesgo medio".
- Datos relacionados con el "[e]*stado financiero (P. ej,. sin ser exhaustivos, solvencia financiera, capacidad de endeudamiento, nivel de deuda (Préstamos personales, hipotecas), listas de solvencia, impagos, activos (fondos de inversión, rendimientos generados, acciones, cuentas a cobrar, rentas percibidas, etc.), pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; o deudas u obligaciones)*". A estos datos también se les asigna un "riesgo medio".
- "*Datos de medios de pago (P. ej., sin ser exhaustivos, tarjetas de crédito e información de acceso a servicios de monedas virtuales)*". En el caso de estos datos sí se asigna un "riesgo alto".

La documentación solicitada por OPENBANK en virtud de lo dispuesto en el Capítulo II de la LPBCFT, es decir, “el soporte documental relacionado con el origen de un fondo de su cuenta bancaria (P.ej., su nómina, contrato laboral, contrato de compraventa si se trata de una operación inmobiliaria, donación o herencia, la factura por los servicios prestados que le son satisfechos por el beneficiario de aquéllos, la resolución por la que se declare la percepción de una determinada ayuda, etc.)” contiene datos relacionados con la situación económica y el estado financiero de los clientes, de los que permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que requieren de una mayor protección.

La información relativa al origen de los ingresos en cuentas bancarias de los clientes es información que está íntimamente relacionada con tales movimientos bancarios y que contiene datos relacionados con la situación económica y el estado financiero de los clientes, de los que permiten determinar la situación financiera o la solvencia patrimonial de una persona, por lo que requieren de una mayor protección.

En resumen, todo lo anterior supone:

1.- Que los datos personales solicitados en virtud del Capítulo II de la LPBCFT merecen una protección especial, debido al mayor riesgo que implican para los derechos y libertades de las personas físicas.

2.- Que los sujetos obligados deben realizar una evaluación de impacto de protección de datos para este tipo de tratamientos, a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

VI
Protección de datos desde el diseño y por defecto

El Artículo 25 “*Protección de datos desde el diseño y por defecto*” del RGPD establece:

“*1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*

2.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales

medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

Este artículo se encuadra dentro de las obligaciones generales que el Capítulo IV del RGPD establece al responsable del tratamiento, imponiendo una obligación de diseño en el momento de determinar los medios de tratamiento, los cuales deben garantizar de forma efectiva el cumplimiento de los principios de protección de datos.

En el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de OPENBANK, toda vez que no se ha incluido la actividad de recogida de datos de los clientes en el denominado "ciclo de vida del tratamiento" de su fichero Excel de documento de evaluación de impacto de protección de datos (aportado durante el período de prueba del presente procedimiento) vigente al momento de los hechos reclamados; por ello, al no preverse siquiera esta actividad, no se han aplicado las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos (entre otros, la confidencialidad) y cumplir los requisitos del RGPD y proteger los derechos de los interesados.

En cuanto a los análisis realizados por OPENBANK en los documentos denominados "Evaluación de Impacto - Seguimiento de clientes y operaciones sensibles", en su versión de agosto de 2021, la cual ni siquiera estaba vigente al momento de los hechos objeto de la reclamación, los cuales tuvieron lugar en el mes de julio de 2021, sólo se había previsto como una posibilidad que los clientes remitieran la información mediante mensaje cifrado remitiendo la contraseña mediante otro canal. E incluso en el citado documento se menciona que se "ha solicitado una demanda interna para que los interesados puedan subir documentos directamente a través del apartado de la web, una vez que se hayan logado en la misma". No obstante, se ha podido comprobar que a la parte reclamante nunca se le dio esa posibilidad, ni en la comunicación inicial remitida por OPENBANK ni posteriormente cuando solicitó una vía alternativa segura para el envío de esa comunicación. También se comprobó que en el modelo de comunicación que se enviaba a los clientes no se daba ninguna de estas opciones, sólo se hacía mención a la posibilidad de responder el correo electrónico que se enviaba sin dar más indicaciones sobre cómo podía protegerse dicha información.

Resulta curioso que, pese a no facilitar ningún medio lo suficientemente seguro a sus clientes para proporcionar la información a que estaban obligados, ambos documentos en sus versiones de 2021 y 2022 reconocen que el riesgo inherente a tal tratamiento era de alto impacto para los derechos y libertades de los interesados.

Y, no obstante, recién es en la versión de octubre de 2022 cuando OPENBANK indica que "los clientes se identificarán mediante DNI y clave de acceso al área privada de cliente".

Lo que sí es cierto es que la comunicación dirigida al cliente cumplía lo previsto en el documento aportado por OPENBANK como protocolo para solicitar la documentación a los clientes en virtud de la LPBCFT y la comunicación dirigida a los clientes no indicaba medio alguno para proporcionar esa información, más allá de la posibilidad de responder el citado correo electrónico.

En cualquier caso, para cumplir con la protección de datos desde el diseño y por defecto no es suficiente con simplemente contar con un documento de protocolo o de modelo de comunicación, si luego al revisar dichos documentos se comprueba que no se realizó una previsión en condiciones sobre las medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados, tal y como dispone el artículo 25.1 del RGPD.

Tampoco es suficiente con contar con documentos que establezcan protocolos o modelos a seguir, si luego en la práctica al realizar el tratamiento no se proporcionan tampoco medidas apropiadas para aplicar los principios de protección de datos ni se integran las garantías necesarias para cumplir con los requisitos del RGPD.

En el presente caso, ha quedado acreditado que en la evaluación de impacto vigente al momento de los hechos reclamados no se contemplaba siquiera el tratamiento de los datos proporcionados por los clientes en virtud de lo dispuesto en el Capítulo II de la LPBCFT. Y que en julio de 2021 se le solicitó a la parte reclamante que enviara determinada información, que podía tener un alto impacto para sus derechos y libertades, mediante correo electrónico, sin darle más indicaciones sobre cómo podía enviar dicha información a través de un canal seguro.

También ha quedado acreditado que la parte reclamante había manifestado al banco su preocupación en este sentido y había solicitado se le facilitara un medio seguro para compartir tal información. Pero, ante la negativa del banco, no le quedó otra opción que enviar la información solicitada a través de un simple correo electrónico, para su disgusto y pese a haber expresado sus reticencias. E incluso la parte reclamante pidió expresamente que se tuviera en cuenta su preocupación y se habilitara un medio seguro a futuro para compartir este tipo de información.

No obstante, en los documentos de agosto de 2021 que aportó OPENBANK junto con sus alegaciones al acuerdo de inicio, tampoco se prevé otro medio.

Del contenido de la documentación que figura en el expediente, ha quedado acreditado:

- Que en el “Anexo I - Comunicaciones a clientes para solicitar información y/o documentación por PBC” del documento ““PROTOCOLO DE COMUNICACIONES A CLIENTES POR ALERTAS DE PBC/FT: APERTURA Y GESTIÓN DE GAPS”, de fecha marzo 2021, en la primera comunicación que se dirige al cliente, en la que se le solicite que acredite el origen de los fondos, no se prevé indicar un medio específico por el cual deba facilitar tal información a OPENBANK. Y que en la segunda comunicación que se dirige al cliente no se prevé indicar tampoco un medio por el cual facilitar tal documentación al banco, pero

se incluye en el texto la amenaza de que en caso de no recibir la documentación solicitada en los próximos 15 días OPENBANK puede impedir la realización de nuevos ingresos en sus cuentas.

- Que el 7 de julio de 2021 OPENBANK solicitó a la parte reclamante que enviara la documentación que acreditaba el origen de determinados fondos, bajo la amenaza de que en 15 días podían impedir nuevos ingresos en su cuenta, sin indicarle medio alguno por el cual debía facilitar tal información.

- Que el 10 de julio de 2021 la parte reclamante aportó la documentación solicitada manifestando su disconformidad porque cuando preguntó por la forma de remitir tal información, le indicaron que lo hiciera por correo electrónico, sin más. Y en este correo electrónico que envía, la parte reclamante indica que no lo considera un medio seguro, que lo realiza a través de este medio porque se vio obligado a ello, e incluso él mismo proporciona como ejemplo de medio seguro la posibilidad de remitirlo "a través del portal del cliente", posibilidad que no se le proporcionó desde OPENBANK. También ruega que comprueben el proceso desde el punto de vista de la protección de datos y tomen las medidas oportunas. No obstante, este correo electrónico sólo recibió un acuse de recibo automático por parte del banco, el 13 de julio de 2021.

- En el documento "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles*", de agosto 2021, se prevé que el interesado puede responder al correo electrónico con un mensaje cifrado remitiendo la contraseña mediante otro canal. Y que se ha solicitado que se pudiera realizar directamente a través del apartado de la web, una vez logados.

- En el documento "*Evaluación de impacto- Seguimiento de clientes y operaciones sensibles"*, octubre de 2022, se prevé que los clientes se autenticarán mediante su DNI y clave de acceso al área privada de cliente.

- En el documento "PROTOCOLO DE COMUNICACIONES A CLIENTES POR ALERTAS DE VIGILANCIA TRANSACCIONAL DE PREVENCIÓN DE BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO (PBC/FT)", de octubre 2022, se indica que se informará a los clientes de que suban la documentación a través del área privada de la web de OPENBANK. Y en el *"Anexo I- Comunicaciones a clientes para solicitar información y/o documentación por una alerta de vigilancia transaccional de PBC/FT*" se indica al cliente que envíe la documentación a través del "Área Clientes" de la web de OPENBANK.

Es decir, el protocolo vigente al momento de los hechos (de marzo de 2021) no preveía proporcionar información sobre el método de envío de la documentación solicitada.

En julio de 2021 la parte reclamante llama la atención sobre esta cuestión en el correo que envía el 10 de julio de 2021 a OPENBANK. Pero el banco hace caso omiso y ni siquiera se le dio una respuesta a su inquietud, que versaba claramente sobre una cuestión de protección de datos personales, lo cual evidencia también la falta de un procedimiento interno de OPENBANK para canalizar estas cuestiones.

En agosto de 2021, OPENBANK prevé la posibilidad de que los clientes envíen la referida documentación a través de un correo electrónico cifrado y facilitando la contraseña mediante otro correo (sin especificar cuál). Y se indica que se solicitó la posibilidad de que se pudiera proporcionar esta documentación a través del área del cliente de la web de OPENBANK.

Y no es hasta octubre de 2022 que los protocolos de comunicación y los documentos de supuesta evaluación de impacto de esta cuestión incorporan de forma específica que los clientes puedan aportar la documentación solicitada a través de la página web de OPENBANK, logándose en su área de cliente.

Es decir, se adoptó la solución de poder proporcionar esta información a través del área de cliente un año y medio más tarde de que se adoptara el protocolo de actuación de marzo 2021 y más de un año más tarde de que la parte reclamante hubiera llamado la atención sobre esta cuestión en concreto y que el documento de supuesta evaluación de impacto de esta cuestión ya lo hubiera previsto como una posibilidad a la que había que realizar seguimiento.

Todo ello evidencia que OPENBANK no aplicó un enfoque de protección de datos desde el diseño ni antes ni durante la realización del tratamiento.

En el artículo 25 del RGPD el bien jurídico que se protege es el cumplimiento del RGPD, en cuanto a la obligación de diseño del tratamiento en toda su extensión, identificando y valorando los riesgos en los derechos y libertades de los interesados a los efectos de implementar medidas técnicas y organizativas apropiadas para aplicación efectiva de los principios de protección de datos, para cumplir con la gestión del cumplimiento del RGPD; lo que no ha ocurrido en este caso, al no haberse siquiera evaluado (ni antes ni durante la realización del tratamiento) la posibilidad de que los clientes enviaran la información requerida en virtud del Capítulo II de la LPBCFT y cómo garantizar el cumplimiento de lo dispuesto en el RGPD. Y ni tan siquiera se le dio respuesta a la inquietud planteada por la parte reclamante respecto a la protección de sus datos personales en esta cuestión. El sistema ni tan siquiera tenía prevista una alarma ante cualquier cuestión que pudiera afectar los derechos y libertades de los clientes en materia de protección de datos, esto es un procedimiento que se pusiera en marcha ante cualquier fallo del propio sistema. Al contrario, el sistema se limitó a contestar con una respuesta automática, sin analizar el fondo de lo planteado por la parte reclamante y sin proporcionarle una respuesta satisfactoria (esto es, sin brindarle un medio apropiado para compartir tal información).

Por tanto, en el presente caso, no se trata únicamente de que no se le ofrecía al interesado (ni a los clientes en general) un medio alternativo para la remisión de los documentos solicitados en virtud del Capítulo II de la LPBCFT, sino que se trata de que en el documento de evaluación de impacto vigente en julio de 2021 (documento aportado durante la fase de prueba del presente procedimiento sancionador) ni siquiera se contemplaba el citado tratamiento (el envío de tal documentación por parte de los clientes). Y que recién en agosto de 2021 se incorporó tal tratamiento en la evaluación de impacto de seguimiento de clientes, si bien no fue hasta octubre de 2022 que se incorporó la posibilidad de que los clientes enviaran la documentación a través del área de cliente de OPENBANK, posibilidad planteada por la parte reclamante ya en julio de 2021 y que el mismo documento de 2021 preveía como posibilidad a ser implementa-

da. Y ello ni siquiera teniendo en cuenta que la misma evaluación de impacto de 2021 consideraba que el posible impacto para los derechos y libertades de los interesados era alto.

De conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable a OPENBANK, por vulneración del artículo 25 del RGPD.

VII
Tipificación de la infracción del artículo 25 del RGPD

La citada infracción del artículo 25 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> (…)
> *d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679. (…)"*

VIII
Sanción por la infracción del artículo 25 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de resolución de procedimiento sancionador, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): Por no haber aplicado unas medidas técnicas y organizativas apropiadas, que garanticen la aplicación efectiva de los principios de protección de datos personales, e integrar las garantías necesarias a fin de cumplir los requisitos del RGPD y proteger los derechos de dos millones de clientes potencialmente afectados y 65.000 clientes directamente afectados, al menos desde mayo 2018 hasta octubre 2022.

  El apartado 54.b.iv de las Directrices 04/2022 del CEPD recoge, como una de las circunstancias a valorar en la graduación de la sanción: "*El número de interesados concretamente, pero también potencialmente afectados*", y, aclara con relación a ese criterio*: "Cuanto más alto es el número de interesados implicados, mayor ponderación podrá tener la autoridad de control atributo a este factor. En muchos casos también puede considerarse que la infracción asume connotaciones «sistemáticas» y, por lo tanto, puede afectar, incluso en diferentes momentos, sujetos de datos adicionales que no han presentado quejas o informes a la autoridad supervisora. La autoridad de control podrá, en función de las circunstancias del caso, considere la relación entre el número de interesados afectados y el número total de interesados en ese contexto (por ejemplo, el número de ciudadanos, clientes o empleados) con el fin de evaluar si la infracción es de carácter sistémico".*

  - La intencionalidad o negligencia en la infracción (apartado b): OPENBANK ha sido gravemente negligente, toda vez que toda vez que la empresa no realizó un análisis en condiciones sobre cómo aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el envío de la documentación solicitada a los clientes en virtud de la LPBCFT, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados ni siquiera cuando un cliente (como en el caso concreto de la parte reclamante) llamó la atención sobre esta cuestión, ni se le dio un curso adecuado a tal solicitud que permitiera reevaluar la adecuación del medio de comunicación elegido por la entidad para compartir tal información. A propósito del grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la Sentencia de la Audiencia Nacional de 17/10/2007 (Rec. 63/2006). Si bien se dictó antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que nos ocupa. La citada Sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que "(...) *el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto*".

- Las categorías de los datos de carácter personal afectados por la infracción (apartado g): En el presente caso, se solicita que se pruebe el origen de varias cantidades recibidas en la cuenta del interesado, lo cual, implica un mayor riesgo para los derechos y libertades del titular de los datos, por lo que son datos que merecen especial protección.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravante:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): El desarrollo de la actividad empresarial que desempeña OPENBANK requiere un tratamiento continuo de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 25 del RGPD, permite imponer una sanción de 1.500.000 € (un millón y medio de euros).

IX
Medidas de seguridad

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, ni en el protocolo de marzo 2021 ni en el correo electrónico remitido por OPENBANK a la parte reclamante con fecha 7 de julio de 2021 se indicaba ningún medio de comunicación para el envío de la documentación solicitada por OPENBANK. El único canal de comunicación para el envío de documentos era contestar al propio correo electrónico, puesto que, además, ningún otro se ofrecía al cliente.

En el caso concreto, OPENBANK no facilitó a su cliente un medio apropiado para aportar la documentación ni siquiera pese a las advertencias de la parte reclamante en este sentido, por lo que el envío se hizo sin las medidas de seguridad adecuadas.

Y ello pese a que los documentos 4 y 5 presentado por OPENBANK junto con sus alegaciones, denominados "Evaluación de impacto- Seguimiento de clientes y operaciones sensibles", versión agosto 2021 y octubre de 2022, respectivamente, en el apartado "13. Seguridad" se ha calificado el riesgo como de impacto alto. Recién en la versión de octubre de 2022, en la página 43 se ha incluido la siguiente indicación sobre "*Control y riesgo residual*": "*Se ha asegurado que los canales de comunicación con clientes como consecuencia asuntos relacionados con la prevención del blanqueo y financiación del terrorismo cuentas con medidas técnicas necesarias para garantizar la protección de sus datos personales. Los clientes se identificarán mediante su DNI y clave de acceso al área privada de cliente*".

En este sentido, el correo electrónico no puede considerarse un medio apropiado para garantizar un nivel de seguridad adecuado al riesgo en el envío de documentación que contenga datos personales de los proporcionados en virtud del Capítulo II de la LPBCFT, de los que requieren una especial protección, teniendo en cuenta la normativa de prevención de blanqueo de capitales, el carácter de los datos que se están tratando y el RGPD.

Respecto a la seguridad del correo electrónico, el "Informe de buenas prácticas" de mayo de 2021, CNN-CERT BP02, del Centro Criptológico Nacional, servicio adscrito al Centro Nacional de Inteligencia, cuya misión es contribuir a la mejora de la ciberseguridad española, recoge una serie de vulnerabilidades del correo electrónico y de las diversas formas en que éstos pueden ser atacados, así como recomendaciones de seguridad. En el apartado 4.2 de dicho Informe se describe la "*Seguridad de las comunicaciones vía email*", con las siguientes aseveraciones en sus páginas 37 a 39: "*El protocolo involucrado en este proceso de envío es SMTP. Este protocolo ha sido utilizado desde 1982 y cuando fue implementando no se tuvieron en cuenta medidas*

de seguridad tales como el cifrado o la autenticación de las comunicaciones. Esto quiere decir que todo el proceso de envío descrito anteriormente se realizaría en texto plano, es decir, que en cualquier punto de la trasmisión un atacante podría ver y manipular el contenido de los correos. Debido a estas carencias en SMTP se han ido desarrollado diversas tecnologías y extensiones que permiten incorporar medidas de seguridad para garantizar la autenticación, integridad y cifrado a las comunicaciones vía correo electrónico. Algunas de las tecnologías más conocidas son STARTTLS, SPF, DKIM y DMARC…Aunque los proveedores de correo más conocidos como Google, Yahoo y Outlook cifran y autentican los emails utilizando este tipo de tecnologías, muchas organizaciones siguen haciendo un uso descuidado del correo electrónico. Téngase en cuenta, además, que estas tecnologías deben ser implementadas tanto en el origen como en el destino para que puedan utilizarse. Asimismo, algunas de estas medidas son susceptibles de ser atacadas. Por ejemplo, STARTTLS es susceptible a ataques downgrade, en donde un atacante en una situación man-in-the-middle puede forzar a que no que lleve a cabo la negociación TLS (bastaría con reemplazar la cadena STARTTLS).
Incluso en el caso de que se establezca la comunicación TLS de forma satisfactoria, los servidores de correo por los que pasa el email hasta alcanzar el destino tendrían acceso a su contenido. Debido a estos hechos, se deduce que no es suficiente con delegar la seguridad del correo electrónico a las tecnologías subyacentes encargadas de hacer llegar el mismo a su destinatario."

A tenor de las carencias de seguridad señaladas anteriormente, se pone de manifiesto la necesidad de adoptar medidas reforzadas para garantizar de forma apropiada la integridad y confidencialidad de los datos personales enviados por correo electrónico, cuando se comuniquen datos personales que merezcan una especial protección, como en el presente caso, medidas que no se han aplicado, lo cual ha supuesto un riesgo mayor para los clientes de OPENBANK que envíen datos personales a través de este medio.

Cabe señalar que el RGPD no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que, en virtud del principio de responsabilidad proactiva del artículo 5.2 del propio RGPD, el cual comporta la exigencia de que el responsable del tratamiento asegure la efectiva privacidad e integridad de los datos, tanto el responsable como el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas. Además, el responsable tiene que estar en condiciones de demostrar que ha implantado esas medidas y que las mismas son las adecuadas para lograr la finalidad perseguida.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

Por todo lo expuesto, las medidas técnicas y organizativas aplicadas por OPENBANK en la solicitud de información a sus clientes (y en concreto a la parte reclamante), en cumplimiento de la normativa de prevención del blanqueo de capitales, no garantizaban un nivel de seguridad adecuado al riesgo, tal y como exige el artículo 32 del RGPD, en virtud del carácter de los datos personales que son tratados, los cuales merecen una especial protección en cuanto a su confidencialidad e integridad.

De forma subsidiaria, en cuanto a la aplicación de las medidas técnicas y organizativas reforzadas al tratamiento en cuestión, cabe afirmar que el hecho de que un tratamiento en su conjunto no sea considerado de alto riesgo y que no tenga que realizarse una evaluación de impacto de protección de datos, no significa que no deban aplicarse medidas de seguridad apropiadas al riesgo que presente alguna de las actividades o etapas del tratamiento en cuestión, conforme a lo dispuesto en el artículo 32 del RGPD.

En el ciclo del tratamiento, que comprende diversas y distintas actividades, no todo el riesgo tiene porqué ser uniforme, pueden existir diversos niveles de riesgos en las distintas etapas del tratamiento, dependiendo de las actividades que lo constituyen. Y si en una fase hay un riesgo alto, aunque no todo el tratamiento sea de alto riesgo, deberían aplicarse medidas adecuadas.

De conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable a OPENBANK, por vulneración del artículo 32 del RGPD.

X

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> (…)
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*

XI

Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de resolución de procedimiento sancionador, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): Por no contar con un medio apropiado para el envío de la documentación solicitada en virtud de la LPBCFT, desde mayo de 2018 hasta octubre 2022, afectando de forma directa los derechos y libertades de 65.000 interesados y de forma potencial a dos millones de clientes.

  El apartado 54.b.iv de las Directrices 04/2022 del CEPD recoge, como una de las circunstancias a valorar en la graduación de la sanción: "*El número de*

interesados concretamente, pero también potencialmente afectados", y, aclara con relación a ese criterio*: "Cuanto más alto es el número de interesados implicados, mayor ponderación podrá tener la autoridad de control atributo a este factor. En muchos casos también puede considerarse que la infracción asume connotaciones «sistemáticas» y, por lo tanto, puede afectar, incluso en diferentes momentos, sujetos de datos adicionales que no han presentado quejas o informes a la autoridad supervisora. La autoridad de control podrá, en función de las circunstancias del caso, considere la relación entre el número de interesados afectados y el número total de interesados en ese contexto (por ejemplo, el número de ciudadanos, clientes o empleados) con el fin de evaluar si la infracción es de carácter sistémico".*

- La intencionalidad o negligencia en la infracción (apartado b): OPENBANK ha sido gravemente negligente a la hora de determinar el medio de envío de la documentación requerida a los clientes en virtud de la LPBCFT, toda vez que la empresa no adoptó las medidas de seguridad apropiadas en función del riesgo para los derechos y libertades de las personas físicas, ni siquiera cuando un cliente (como en el caso concreto de la parte reclamante) llamó la atención sobre esta cuestión, ni aun cuando su propio documento de evaluación de impacto había indicado la necesidad de adoptar el envío de la información solicitada en virtud de la LPBCFT a través del área privada de la web del banco y había indicado que se trataba de un tratamiento de alto impacto para los derechos y libertades. A propósito del grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la Sentencia de la Audiencia Nacional de 17/10/2007 (Rec. 63/2006). Si bien se dictó antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que nos ocupa. La citada Sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que "(...) *el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto*". Por el alto impacto que ello podría acarrear para los interesados, OPENBANK estaba obligada a encontrar soluciones que no supusieran un mayor riesgo para los derechos y libertades de sus clientes y que garantizaran la seguridad de los datos.

- Las categorías de los datos de carácter personal afectados por la infracción (apartado g): En el presente caso, se solicita que se pruebe el origen de varias cantidades recibidas en la cuenta del interesado, el cual, al facilitar esa información sin unas medidas de seguridad adecuadas, podía aumentar su vulnerabilidad ante posibles ataques, lo que implicaba un mayor riesgo para los derechos y libertades del titular de los datos.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravante:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): El desarrollo de la actividad empresarial que desempeña OPENBANK requiere un tratamiento continuo de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite imponer una sanción de 1.000.000 € (un millón de euros).

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **OPEN BANK, S.A.**, con NIF A28021079, por la infracción del artículo 25 del RGPD una multa de 1.500.000,00 (UN MILLÓN QUINIENTOS MIL EUROS), por la infracción del artículo 32 del RGPD una multa de 1.000.000,00 (UN MILLÓN DE EUROS), tipificadas ambas en el artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a **OPEN BANK, S.A.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00 0000 0000 0000 0000 0000 (BIC/Código SWIFT: XXXXXXXXXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de

publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-010623

Mar España Martí
Directora de la Agencia Española de Protección de Datos