- Expediente N.º: EXP202204512

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 31 de marzo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra OPEN BANK, S.A. con NIF A28021079 (en adelante, la parte reclamada u Openbank). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que ha tenido conocimiento de la apertura de una cuenta bancaria a su nombre con la entidad Openbank, sin su autorización.

Así las cosas, la parte reclamante expone que recibió una llamada de teléfono de la Policía de A Coruña en la que se le informa que se estaba utilizando una cuenta bancaria abierta a su nombre en Openbank para estafar a terceras personas.

Fecha en la que tuvieron lugar los hechos reclamados el 16 de agosto de 2021.

Documentos relevantes, aportados por la parte reclamante:

Denuncia presentada ante la Dirección General de la Policía (en adelante, DGP).

Correo electrónico enviado el día 17/03/2022 a las 21:10 horas por la parte reclamante (******EMAIL.1***) a la parte reclamada (ayuda@openbank.es), adjuntando la denuncia presentada ante la DGP, donde indica:

"*Adjunto denuncia de comisaria indicando que alguien se ha hecho pasar por mi utilizando mi DNI, para abrir una cuenta en su entidad bancaria lo cual supone un delito de suplantación y robo de identidad.*

Ruego cese y cierren la misma y borren mis datos de sus sistemas, ya que según comentarios de la Policía se está utilizando para cobrar estafas a la gente."

Correo electrónico enviado el día 17/03/2022 a las 21:14 horas por la parte reclamada (******EMAIL.2***) a la parte reclamante (******EMAIL.1***).

Correo electrónico enviado el día 18/03/2022 a las 13:02 horas por la parte reclamada (******EMAIL.3***), firmado por el Departamento Comercial de la parte reclamada, a la parte reclamante (******EMAIL.1***).

Correo electrónico enviado el día 25/03/2022 a las 11:24 horas por la parte reclamante (******EMAIL.1***) a la parte reclamada (*ayuda@openbank.es*) donde pregunta por el

estado en el que se encuentra su petición (cierre de cuenta bancaria y borrado de sus datos).

Correo electrónico enviado el día 28/03/2022 a las 10:02 horas por la parte reclamada (******EMAIL.3***), firmado por el Departamento Comercial de la parte reclamada, a la parte reclamante (******EMAIL.1***) donde le responden que han trasladado su consulta a su departamento de seguridad para que informen al respecto.

SEGUNDO: De conformidad con el artículo 65.4 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 dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 11 de mayo de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 10 y 23 de junio de 2022 se recibe en esta Agencia escrito de respuesta. En el primero de ellos la parte reclamada solo aportó la documentación contractual, y en el segundo expone que han procedido a la cancelación de los productos que se encontraban a nombre del reclamante y aportan el correo electrónico remitido a la parte reclamante el día 26 de mayo de 2022, en el que se indica:

"En relación con la reclamación presentada por Ud. ante la Agencia de Protección de Datos referida al uso sin su consentimiento de sus datos de carácter personal por parte de OPEN BANK, S.A. ("Openbank"), le confirmamos que hemos analizado la misma y procedemos a informarle lo siguiente:

Por un lado, le informamos que Openbank como entidad financiera, para iniciar una relación de negocio, está sujeta a lo establecido en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y su Reglamento, aprobado por Real Decreto 304/2014, de 5 de mayo, que requiere a los interesados información suficiente que permita acreditar su identidad.

En este sentido, hemos validado internamente que la información requerida para la apertura de cuenta ha sido proporcionada correctamente, en concreto, disponemos del documento de suscripción de contratos firmado el día 16 de agosto de 2021, una copia del documento de identidad y que se ha verificado la identidad a través de la titularidad de otra cuenta (método IBAN).

Por otra parte, tal y como se indicó en el correo electrónico enviado el día 18 de marzo de 2022, en cuanto Ud. se puso en contacto con Openbank su comunicación fue trasladada inmediatamente al equipo de Fraude y Seguridad para que procediesen a analizar la misma y tomar las medidas preventivas oportunas como el bloqueo de la operativa con la cuenta mientras se realiza el análisis correspondiente para validar en fraude denunciado y por un error humano de la persona que analizó su solicitud, no se le confirmaron las gestiones llevadas a cabo.

Le informamos que los productos que se encontraban a su nombre en nuestro sistema han sido cancelados por Openbank y los datos personales asociados sólo podrán ser tratados para la puesta a disposición de jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas, luego sus datos serán suprimidos para cumplir con los fines establecidos en el artículo 32 de la LOPDGDD".

TERCERO: Con fecha 28 de junio de 2022, de conformidad con el artículo 65 de la 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:

La contratación de la cuenta bancaria y tarjeta de débito (hechos reclamados) se llevó a cabo de forma no presencial el día 16 de agosto de 2021.

Los procedimientos de la parte reclamada indican que, para ello, es necesario la identificación fehaciente del interesado mediante varios métodos habilitados y establecidos por el SEPBLAC.

El método elegido por el interesado, en este caso, fue mediante IBAN que requiere la aportación de un número de cuenta de otro banco facilitado por el interesado y del que sea titular.

En este caso, el interesado ingresó una cuenta IBAN de otra entidad bancaria de la que la parte reclamante es titular, y adjuntó foto del anverso y reverso del DNI de la parte reclamante, tal y como establece el procedimiento de contratación de la parte reclamada.

La validación de la cuenta IBAN de otra entidad de la que es titular la parte reclamante fue realizada por Iberpay el mismo día de los hechos (16/08/2021).

Respecto al DNI proporcionado en el proceso de contratación, como documento que se adjuntó durante dicho proceso, el domicilio que figura en el mismo no coincide con el indicado por la parte reclamante en su denuncia ante la DGP.

Además, es importante destacar el hecho de que el domicilio que figura en el contrato de la cuenta bancaria y de la tarjeta de débito (hechos reclamados) no coincide ni con el que figura en el DNI aportado durante el proceso de contratación ni con el que indicó la parte reclamante en su denuncia ante la DGP.

En el certificado de firma electrónica proporcionado por un tercero de confianza, que acredita la validación de la contratación mediante envío de mensaje SMS, figura un

número de teléfono móvil distinto al aportado por la parte reclamante en su denuncia ante la DGP.

Además, en este certificado figura la firma manuscrita digitalizada del interesado que realiza la contratación de la cuenta bancaria y de la tarjeta de débito, pero dicha firma no coincide con la que figura en el DNI aportado por el interesado durante el proceso de contratación (DNI de la parte reclamante).

La parte reclamada señala que para poder activar la cuenta es necesario que su equipo de Back Office revise que toda la documentación proporcionada durante el proceso de contratación es válida. Sobre esto, hay que tener en cuenta dos hechos:

Primero, la parte reclamada no detalla las tareas que incluye dicha revisión ni tampoco acredita la validación que se llevó a cabo en este caso. Segundo, el domicilio del DNI proporcionado durante la contratación no coincide con el que figura en el propio contrato y tampoco coincide la firma manuscrita digitalizada que figura en el contrato con la que figura en el DNI proporcionado durante la contratación.

El procedimiento vigente de identificación no presencial mediante IBAN en el momento de los hechos reclamados perdió su eficacia el día 30/09/2022, según nota publicada por el SEPBLAC el día 13/05/2021.

En dicha nota el SEPBLAC hacía referencia a la necesidad de implantar unas medidas adicionales para comprobar que la persona que está participando en el proceso de identificación a distancia es titular de la cuenta objeto del procedimiento. De este modo, según indica la parte reclamada, ésta procedió a adoptar esas medidas adicionales.

Estas medidas adicionales están relacionadas con la realización de una transferencia, al número de cuenta de otro banco facilitado por el interesado y del que sea titular, que incluya en el concepto un código alfanumérico generado de forma aleatoria, el cual deberá ser ingresado por el interesado para verificar su identidad y poder continuar con el proceso de contratación.

En la fecha de los hechos reclamados (16/08/2021), esas medidas adicionales aún no estaban implantadas por la parte reclamada puesto que el procedimiento vigente en ese momento no perdía su eficacia hasta el día 30/09/2021.

De este modo, sólo cabe señalar que la parte reclamada actuó formalmente en consonancia a los procedimientos establecidos en el momento de los hechos reclamados, pero no ha acreditado que contrastara la identidad del contratante con los datos del DNI (dirección, firma) del reclamado.

QUINTO: Openbank es una entidad mercantil, cuya empresa matriz global es el Banco Santander, S.A. siendo ésta, según la información recogida en su propio “Informe anual 2022” 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 2021, fue de 52.117 millones de euros (ver página 836 del citado “Informe anual 2022”).

SEXTO: Con fecha 27 de abril de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD.

SÉPTIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley LPACAP, la parte reclamada presentó escrito de alegaciones, el 16 de mayo de 2023, en el que, en síntesis, manifestaba: << *que la AEPD indica que mi mandante actuó formalmente en consonancia con los procedimientos establecidos en el momento de los hechos reclamados, pero no ha acreditado que contrastara la identidad del contratante con los datos del DNI (dirección, firma) del reclamado nos gustaría destacar lo siguiente:*

Openbank es objeto de supervisión anual por parte de un experto externo, tal y como se requiere por el artículo 28 de la Ley de PBC/FT y que cuenta con cuenta con un informe positivo emitido el 22 de julio de 2022 donde, entre otros aspectos, se ha revisado el modelo de control relativo a los procedimientos de identificación y conocimiento de clientes, del periodo de abril de 2021 a abril de 2022 y donde se indica que no han puesto de manifiesto recomendaciones o propuestas de mejora.

Tal y como ha indicado previamente mi mandante en las diferentes comunicaciones intercambiadas con esta AEPD, los datos fueron tratados lícitamente siguiendo lo establecido en 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 su Reglamento de desarrollo, aprobado por el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante, el “RD304”), que requiere a los interesados información suficiente que permita acreditar su identidad. En particular, cabe destacar los siguientes preceptos en relación con la citad materia:

A nivel operativo, mi mandante ha compartido con esta AEPD en comunicaciones anteriores las evidencias de las comprobaciones que realiza para la identificación formal con carácter previo al establecimiento de la relación de negocios y ha indicado que, en caso de no poder comprobar la identidad, no se podría finalizar el proceso de contratación. En relación con este expediente, la identificación formal fue considerada válida y suficiente ya que mi mandante disponía con respecto al reclamante de la documentación requerida en la normativa vigente: copia del Documento Nacional de Identidad (en adelante, el “DNI”).

OPENBANK ha implantado las medidas necesarias para verificar la identificación formal mediante un documento fehaciente reconocido por la normativa, cuya validez no depende del domicilio recogido en este ni del declarado por el interesado en el formulario de apertura de cuenta. Hay que tener cuenta que esta situación también se da cuando un interesado realiza el proceso de alta como cliente presencialmente en las oficinas, dónde se requiere la personación física del interesado, así como que muestre su DNI para acreditar su identidad sin que sea requisito para su validez que el domicilio del DNI coincida con el declarado en el formulario de apertura de cuenta.

En línea con lo anterior, la normativa también permite la identificación mediante pasaporte u otra tarjeta oficial de identidad personal expedidos por las autoridades de origen, que no tienen por qué incluir ninguna mención al domicilio del interesado, circunstancia ésta que determina la validez de estos documentos, jurídicamente considerados suficientes para la acreditación de la identidad.

No puede ponerse en duda el proceso de identificación de los interesados por el mero hecho de que la dirección del DNI en vigor no coincida con declarada en el formulario de alta como cliente toda vez que esta obligación se refiere al momento de la renovación del documento por caducidad y que sólo será necesario acreditar el domicilio en caso de que haya cambiado por lo que, si el mismo no ha variado desde la renovación anterior, no será necesario aportar documento acreditativo actualizado.

Por lo que respecta a la firma del documento de suscripción de contratos (en adelante, el "DSC") mi mandante considera que –por sí solo- el hecho de que la firma manuscrita estampada en el DNI de un cliente no coincida con la grafía mediante la que se materializa la firma electrónica de ese mismo cliente durante su proceso de alta no le resta ni validez jurídica al proceso, ni fuerza probatoria a la firma electrónica.

Jurídicamente la grafía de ambos tipos de firma puede no coincidir en la práctica, circunstancia esta que no invalida automáticamente la firma electrónica, siempre y cuando la misma y el proceso mediante el que ésta se materialice se ajusten a las garantías y los requisitos legales, técnicos y en materia de seguridad previstos por la normativa aplicable en materia de servicios electrónicos de confianza, detallada más adelante en la presente alegación.

A mayor abundamiento, por si queda alguna duda sobre la validez de los documentos firmados electrónicamente y la no necesidad de coincidencia de grafías entre la firma en el entorno online y la analógica, debe recordarse que el Reglamento 910/2014, del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (en adelante, el "Reglamento eIDAS"), establece la existencia de tres (3) tipos de firmas electrónicas -la firma electrónica "simple", la firma electrónica avanzada y la firma electrónica cualificada- y determina en su artículo 25 que todas ellas poseen efectos jurídicos y, por lo tanto, pueden ser admitidas en procesos judiciales. En concreto, la firma electrónica mediante la que se firmó el DSC objeto de este procedimiento sancionador es una firma avanzada y reúne los siguientes requisitos previstos por el artículo 26 Reglamento eIDAS, esto es: i. estar vinculada al firmante de manera única; ii. permitir la identificación del firmante; iii. haber sido creada utilizando los datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo; y iv. estar vinculada con los datos firmados por la misma, de modo tal que cualquier modificación ulterior de los mismos sea detectable También a nivel nacional, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, la "Ley 6/2020"), que deroga la Ley 59/2003, de 19 de diciembre, de firma electrónica y adapta nuestro ordenamiento jurídico al marco regulatorio establecido por el Reglamento eIDAS, dispone en su artículo 3 que "1. Los documentos electrónicos públicos, administrativos

y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable".

(...)

En definitiva, en consonancia con lo que ha venido indicándose, no puede ponerse en duda la legitimación del tratamiento de datos llevado a cabo por mi mandante por el mero hecho de que la firma electrónica del DSC del reclamante no coincida con la firma de su documento nacional de identidad.

En el plano jurídico, la discordancia entre la grafía de ambos tipos de firma no obsta para que la firma electrónica sea válida siempre y cuando la misma se haya generado conforme a lo previsto por la normativa aplicable, como es el caso. Cosa distinta es que, maliciosamente, un suplantador se haya hecho pasar de forma fraudulenta por el reclamante y haya atacado su privacidad, valiéndose de un instrumento jurídicamente válido como es la firma electrónica para abrir una cuenta a nombre del reclamante sin su autorización.

La imposición de una sanción de la cuantía de la recogida en el Acuerdo de Inicio sólo puede considerarse desproporcionada y vulneradora del principio de proporcionalidad mencionado. En virtud de todo lo expuesto, solicito a la agencia española de protección de datos, se sirva admitir el presente escrito y los documentos que se adjuntan, tenga por formuladas las alegaciones que preceden y, en su virtud, tras las actuaciones que considere oportunas: i. Dicte resolución acordando el archivo del presente procedimiento, en méritos a lo establecido en el cuerpo del mismo. ii. De forma subsidiaria, en el en supuesto de que no aceptase el pedimento anterior, proceda a la aplicación de los artículos 83 del RGPD y 76 de la LOPDGDD, en el momento de determinar la sanción con el fin de minorar el importe de la multa propuesta.

OCTAVO: Con fecha 17 de mayo de 2023, el instructor del procedimiento acordó practicar las siguientes pruebas: *<<1.Se dan por reproducidos a efectos probatorios la reclamación interpuesta por D.* ***A.A.A.*** *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 AI/00281/2022. 2.Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por OPEN BANK, S.A., y la documentación que a ellas acompaña. El resultado de estas pruebas podrá dar lugar a la realización de otras>>*.

NOVENO: Con fecha 15 de junio de 2023 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a OPEN BANK, S.A., con NIF A28021079, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, con una multa de 70.000 euros (setenta mil euros).

DÉCIMO: Notificada la propuesta de resolución el día 23 de junio de 2023, el día 27 del mismo mes y año solicitó ampliación de plazo, así como la remisión del expediente administrativo, siéndole notificado el día 28 de junio acuerdo de la misma fecha por el que se accede a la ampliación en cinco días del mencionado plazo, siéndole

igualmente remitido el expediente administrativo en fecha 3 de julio de 2023, y con fecha 14 de julio de 2023 formula alegaciones en el que, en síntesis, se aduce: <<*que habiéndose cumplido todos los requisitos legalmente establecidos para identificar como solicitante del producto financiero al reclamante, mi mandante estaba completamente legitimada para proceder al tratamiento de tales datos al amparo de la relación contractual celebrada con el mismo, y por tanto por el artículo 6.1 b) del RGPD, por lo que imputar a aquélla la infracción del citado precepto no resulta conforme a la normativa de protección de datos personales.*

En resumidas cuentas, ni cabe exigir al interesado que consigne obligatoriamente el domicilio que conste en su DNI en el momento de solicitar la contratación de un producto financiero, ni mi representada podría, por este simple motivo considerar que aquél no se ha identificado adecuadamente en caso de que aportase copia de su DNI, como motivo que implicase la denegación de la contratación el citado producto, ni mi mandante puede exigir a quien pretenda celebrar un contrato con la misma la aportación de un certificado de empadronamiento, único documento que hace fe del domicilio de las personas conforme a lo dispuesto en la legislación vigente. Mi mandante verificó la identidad del interesado a través de la visualización de la copia del DNI que obra en el expediente administrativo, no habiéndose en ningún momento declarado, ni siquiera por el reclamante, que tal DNI no sea el suyo. De este modo, entiende respetuosamente mi representada que la AEPD a través de la Propuesta de Resolución está haciendo recaer sobre mi mandante, cuya diligencia en el presente supuesto fue la exigible conforme a la ley, el hecho de que el DNI del interesado obrase en poder de un tercero que, desafortunadamente, empleó el mismo para suplantar su identidad, abusando de las disposiciones establecidas en la ley para la verificación de la misma por parte de Openbank.

No debe a tal efecto olvidarse que el artículo 9.1 de la LOSC establece en su segundo inciso que el DNI "es personal e intransferible, debiendo su titular mantenerlo en vigor y conservarlo y custodiarlo con la debida diligencia".

De la supuesta falta de verificación del número telefónico del interesado. Si mi representada manifiesta su sorpresa ante el razonamiento al que se refiere el apartado precedente de esta alegación, dicha sorpresa se ve incrementada cuando en la misma se achaca una supuesta falta de diligencia motivada por el hecho de que "en el certificado de firma electrónica proporcionado por un tercero de confianza, que acredita la validación de la contratación mediante envío de mensaje SMS, figura un número de teléfono móvil distinto al aportado por la parte reclamante en su denuncia ante la DGP".

Es decir, mi mandante considera, con el debido respeto, que la afirmación contenida en la Propuesta de Resolución acerca de la falta de identidad del móvil declarado a la misma a efectos de firma y el facilitado por el interesado en su denuncia carece del más mínimo sentido, dado que resulta, en primer lugar, innecesario y, en segundo lugar, ilícito llevar a cabo una verificación de este dato.

De la validez de los documentos firmados a través de firma electrónica avanzada. Es decir, la norma aplicable a la firma electrónica establece expresamente que la firma electrónica avanzada, por sí sola, y al margen de toda grafía, produce el mismo efecto probatorio de la celebración del contrato que la firma manuscrita, no pudiendo

denegarse dicho valor por el mero hecho de que aquélla sea una firma electrónica avanzada. Es decir, si el documento firmado electrónicamente no contuviera grafía alguna el mismo seguiría produciendo todos sus efectos jurídicos, al contar el mismo con la firma electrónica de quien contrató el servicio. De este modo, el documento firmado electrónicamente conforme a un sistema de firma electrónica avanzada permite acreditar la identidad, integridad y no repudio de los documentos firmados, constituyendo los mismos un medio probatorio admisible para acreditar la celebración del contrato, y siendo enteramente irrelevante el grafo que pueda constar en el documento. En este sentido, debe tenerse en cuenta que incluso los sistemas de firma electrónica como el utilizado en el presente caso permiten que el grafo que se plasme en el documento se corresponda con una grafía generada por defecto por el propio sistema, dado que lo relevante a estos efectos no es el mencionado grafo, sino el hecho de que el documento ha sido firmado con una firma electrónica que le otorga validez e impide la alteración posterior del documento.

En el presente caso la identificación del firmante se llevó a cabo mediante la remisión a través de un SMS de una contraseña (código OTP) de un solo uso que debía utilizar el receptor para poder validarse y continuar el proceso de firma del documento. De este modo, como ya se indicaba en las alegaciones al Acuerdo de Inicio "los clientes deben confirmar su número de teléfono móvil, con el fin de que Openbank *les pueda remitir mediante SMS un código de acceso (one time password u "OTP", por sus siglas en inglés). Deberán introducir el código OTP en la web para acceder al contrato, dibujar una firma en el lugar indicado a tal efecto y pulsar en el botón "Finalizar" para la materialización de la misma. Si bien la firma que se genera no tiene por qué ser la representación gráfica de la firma del DNI del interesado, como se ha venido poniendo de manifiesto en el presente escrito, ello no resulta determinante para la identificación del cliente ni la validez del proceso". Y como también se indicaba en las citadas alegaciones "el procedimiento implantado por mi mandante para la firma del DSC por parte de sus clientes se basa en la solución de firma avanzada del proveedor DocuSign, pero además –como añadido- comporta la intervención de un tercero de confianza (TrustCloud, anteriormente denominado Branddocs), que actúa como testigo electrónico independiente y que genera un certificado que aporta evidencias digitales más sólidas sobre la integridad del documento".*

Teniendo en cuenta lo anterior, debe recordase que el solicitante de la apertura de la cuenta se había identificado ante mi representada mediante la remisión de una copia de su DNI, habiendo procedido Openbank a verificar la identidad del solicitante mediante el procedimiento autorizado a tal efecto por el SEPBLAC. Y una vez verificada dicha identidad y solicitado un número de teléfono móvil, que mi mandante obviamente únicamente podía vincular con la persona identificada, remitió a aquél un SMS conteniendo el OTP necesario para llevar a cabo la firma del documento que, verificada por un tercero de confianza, validaba el mismo desde el punto de vista jurídico, sin que el grafo de la firma resultase relevante a tales efectos.

Mi representada verificó que el mismo era titular de una cuenta corriente abierta en CaixaBank, constando en el expediente la titularidad del reclamante de la citada cuenta y utilizó un procedimiento de firma electrónica avanzada para la firma del documento. Pero además, mi mandante ya indicó en sus alegaciones al Acuerdo de Inicio, que sí desplegó y puso en funcionamiento los procedimientos internos de backoffice para verificar que se cumplían todos y cada uno de los requisitos exigidos

por su "Guía de validación Documental". En este sentido, en dichas alegaciones se aportó por mi representada copia de pantalla de la validación por el equipo de backoffice de Openbank del cumplimiento de los citados requisitos, indicándose que se había producido la verificación de la autenticidad del DNI. Mi representada cumplió todos y cada uno de los requisitos exigidos por la normativa actualmente vigente para la verificación de la identidad del solicitante de la apertura de la cuenta, contando (i) con su DNI en vigor; (ii) la acreditación de la titularidad de una cuenta abierta en CaixaBank; y (iii) el documento de suscripción del contrato firmado con una firma electrónica avanzada en los términos establecidos en el Reglamento eIDAS. De este modo, Openbank no tenía elemento alguno que permitiese dudar, ni siquiera indiciariamente, de la identidad del solicitante, verificada además por el procedimiento interno de backoffice establecido a tal efecto por mi representada, procediendo de forma completamente legítima a la apertura de la cuenta. Y ello implica que Openbank contaba con una base jurídica adecuada para el tratamiento de los datos del Reclamante, al haber quedado verificada su identidad, siendo el tratamiento perfectamente lícito al amparo del artículo 6.1 b) del RGPD y habiendo desplegado mi representada toda la diligencia exigible para verificar la licitud del tratamiento.

Openbank considera necesario poner además de manifiesto que la Propuesta de Resolución de esa AEPD contradice frontalmente el criterio sustentado en relación con mi representada en diversos procedimientos en los que las reclamaciones se referían a hechos completamente similares, siendo igualmente similar la información facilitada por mi mandante, finalizando todo ellos en resoluciones de archivo de las actuaciones dirigidas contra Openbank: EXP202206099; EXP202210508 y EXP202102069. En consecuencia, entiende esta parte, respetuosamente, que la AEPD con su actitud ha vulnerado los principios de confianza legítima y seguridad jurídica, adoptando un cambio radical de criterio que no puede sino calificarse de sorpresivo e inesperado.

Por último, y de manera subsidiaria para el hipotético supuesto de que, frente a lo alegado por mi mandante, se apreciase la existencia de una infracción de la normativa de protección de datos, debe particularmente tenerse en consideración en la determinación de la sanción que pudiera imponerse, la aplicación del principio de proporcionalidad.

En virtud de todo lo expuesto, solicito a la agencia española de protección de datos, se sirva admitir el presente escrito, tenga por formuladas las alegaciones que preceden y, en su virtud, tras las actuaciones que considere oportunas, dicte resolución acordando el archivo del presente procedimiento>>.

UNDÉCIMO: Con fecha 13 de diciembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó que este procedimiento debería concluir con la imposición de una infracción del artículo 6.1. del RGPD, tipificada en el artículo 83.5.a) del RGPD, a la que correspondería una sanción de multa administrativa, por una cuantía de 200.000 € (doscientos mil euros).

DUODÉCIMO: Notificado el acuerdo de la Directora de la Agencia Española de Protección de Datos, Openbank solicitó el 29 de diciembre de 2023 ampliación de plazo para formular alegaciones, y se accedió a dicha ampliación en cinco días, y con fecha 18 de enero de 2024 la parte reclamada formuló alegaciones en el que, en síntesis, se alega: "*ratificación de lo alegado por openbank a lo largo del presente*

procedimiento, y tal y como se detalló en el Escrito de Alegaciones anteriormente enviado a esta Agencia, OPENBANK actuó con la diligencia debida en ese momento para la identificación del interesado y para el tratamiento de sus datos por lo que no ha lugar a la sanción que propone esta Agencia."

(…) la AEPD aprecia la concurrencia de una mayor gravedad en la sanción a imponer a mi representada sobre la única y exclusiva base de que la misma se encuentra integrada en el Grupo Santander, lo que determina la modificación, sobre la base de un mero automatismo, del límite máximo de la sanción que podría imponerse en este caso, tomando como referencia la facturación anual del mencionado Grupo y no la de OPENBANK. Y para ello, la AEPD justifica esta agravación de la sanción en las Directrices, de forma que considera que el destinatario de la sanción, es decir, la "empresa" a los efectos establecidos en el RGPD, es el Grupo Santander y no mi representada. De este modo, y en virtud del automatismo mencionado, razona la AEPD, entendemos que basado, aunque no se mencione, en el considerando 150 del RGPD, que el responsable de la infracción en este caso ha de ser el resultante de la aplicación, sin más, de lo dispuesto en los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea (en adelante, el "TFUE").

No obstante, mi mandante considera necesario efectuar una serie de consideraciones que, a su juicio, resultan particularmente relevantes para determinar si procede la aplicación meramente automática de lo mencionado, que no dispuesto, por el citado considerando.

En primer lugar, debe tenerse en cuenta que el razonamiento mencionado se fundaría únicamente en una referencia contenida en un considerando del RGPD, el 150, que únicamente puede ser concebido como interpretativo de su parte dispositiva. Es decir, el contenido del RGPD no debe interpretarse en un sentido que difiera de su articulado sobre la simple base del contenido de uno de sus considerandos.

Y en este punto es preciso tener en cuenta que los apartados 18 y 19 del artículo 4 del RGPD regulan los conceptos de "empresa" y "grupo de empresas", considerando el primero de ellos que será empresa, "a los efectos del presente Reglamento", "toda persona física o jurídica que ejerza una actividad económica, cualquiera que sea su forma jurídica, incluidas las sociedades de personas o las asociaciones que ejerzan regularmente una actividad económica".
Por su parte, el artículo 4.19 define como grupo de empresas "una empresa que ejerce el control y sus empresas controladas".

Pues bien, el artículo 83.5 del RGPD, que la AEPD pretende aplicar a mi representada, indica que las infracciones "se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior". Es decir, el RGPD se refiere en este precepto al término "empresa", que a los efectos del propio texto es distinto del concepto de "grupo de empresas", siendo definido de forma separada y diferenciada del mismo.

Y si esto es así, no es posible, con independencia de lo que afirme el considerando 150 del RGPD, (cuyo contenido, como se ha dicho, sólo sería interpretativo, y nunca

dispositivo), aplicar para la determinación del límite superior de la sanción a imponer a mi representada el concepto "grupo de empresas", dado que el artículo 83.5 del RGPD, que es la norma aplicable, no se refiere al mismo, sino a otro distinto, que es el de "empresa".

En este sentido, los apartados 122 y siguientes de las Directrices obvian la existencia de estos dos conceptos diferenciados en el RGPD, señalando que "[e]n consonancia con la jurisprudencia consolidada del TJUE, el término empresa en los artículos 101 y 102 del TFUE puede referirse a una única unidad económica (SEU, por sus siglas en inglés), incluso si dicha unidad económica está formada por varias personas físicas o jurídicas", añadiendo que "[s]i varias entidades forman una SEU depende en gran medida de si la entidad individual es libre en su capacidad de toma de decisiones o de si una entidad principal, a saber, la sociedad matriz, ejerce una influencia decisiva sobre las demás. Los criterios para determinarlo se basan en los vínculos económicos, jurídicos y organizativos entre la sociedad matriz y su filial, por ejemplo, el importe de la participación, los vínculos de personal u organización, las instrucciones y la existencia de contratos de empresa", aplicando en los supuestos en los que "una sociedad matriz posee el 100 % de las acciones o casi el 100 % de las acciones de una filial que ha infringido el artículo 83 del RGPD y, por lo tanto, puede ejercer una influencia decisiva sobre el comportamiento de su filial" la presunción derivada de la sentencia del Tribunal de Justicia de la UE de 10 de septiembre de 2009 (asunto C-97/08 P, Akzo Nobel y otros/Comisión).

Pues bien, si se sigue la interpretación contenida en las Directrices, que obvia la existencia de un concepto diferenciado de "empresa" en el RGPD, se estaría equiparando dicho concepto con el de "grupo de empresas", contenido en el propio RGPD, dado que es la existencia de una control o influencia el que determina la aplicación del artículo 4.19 del RGPD. Es decir, la interpretación efectuada por las Directrices obvia que el concepto de "grupo de empresas" en el RGPD se diferencia del de "empresa", siendo así que es el primero de ellos y no el segundo el que se encontraría vinculado con la aplicación de los artículos 101 y 102 del TFUE. De este modo, la interpretación de las Directrices es diametralmente opuesta a lo establecido en el RGPD, dado que el artículo 83.5 del mismo se refiere a "empresa" y no a "grupo de empresas", que es el concepto que pretende aplicar la AEPD, sobre la única y exclusiva base del considerando 150 del RGPD y de unas directrices que, por su propia definición y contenido, carecen de valor normativo, no pudiendo suponer un criterio interpretativo contrario a la literalidad del RGPD.
Incluso desde el punto de vista teleológico, y sin perjuicio de todo lo indicado con anterioridad, la referencia a los artículos 101 y 102 del TFUE debe ser interpretada atendiendo a la ubicación sistemática de dichos preceptos en el Capítulo I del Título VII del Tratado, es decir, dentro de las normas reguladoras de la competencia en la Unión.

Y ello supone que, incluso en el negado supuesto de que por la AEPD no se considerase suficiente lo indicado hasta este lugar y obviase que el RGPD contiene un concepto específico de "grupo de empresas" no referenciado en el artículo 83.5, la aplicación extensiva del concepto de "empresa" a efectos del derecho de la competencia únicamente podría operar en los supuestos en que la conducta supuestamente infractora, respecto de la que se pretende determinar el importe de la sanción, pudiera dar lugar a una alteración o distorsión de la competencia.

En este sentido, cabe recordar que los criterios de aplicación de los artículos 101 y 102 del TFUE se encuentran recogidos en la Directiva (UE) 2019/1 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018, encaminada a dotar a las autoridades de competencia de los Estados miembros de medios para aplicar más eficazmente las normas sobre competencia y garantizar el correcto funcionamiento del mercado interior, cuyo artículo 1.1 establece que "[l]a presente Directiva establece determinadas normas para garantizar que las autoridades nacionales de competencia dispongan de las garantías de independencia, recursos y competencias de aplicación e imposición de multas, necesarias para poder aplicar efectivamente los artículos 101 y 102 del TFUE, de modo que no se falsee la competencia en el mercado interior y que los consumidores y las empresas no se vean perjudicados por el Derecho y las medidas nacionales que impiden la aplicación eficaz de las normas por parte de las autoridades nacionales de competencia".

Es decir, la aplicación de estos preceptos estaría vinculada a la garantía de la libre competencia en el mercado, lo que exigiría, mutatis mutandis, si se pretende su aplicación en materia de protección de datos, lo que ya se ha dicho que resulta contrario a la literalidad del artículo 83.5 del RGPD, que la conducta presuntamente infractora afectase a la libre competencia en el mercado (por ejemplo, porque como consecuencia de un tratamiento llevado a cabo por el encartado éste lograse una ventaja competitiva sobre el resto de sus competidores, basada precisamente en la realización de la conducta infractora).

Sin embargo, ni siquiera realizando esa interpretación teleológica cabría considerar que la conducta analizada en este expediente se encontrase remotamente vinculada con la obtención de beneficio o venta alguna que afectase o distorsionase la competencia en el sector de actividad de mi representada, dado que dicha conducta es meramente puntual y, como se ha expuesto anteriormente, mi representada cumplió en su actuación los criterios establecidos por el SEPBLAC para proceder a la contratación a distancia de los servicios, aplicando el método de verificación a través de IBAN, al que se ha referido extensamente mi mandante a lo largo de todo el procedimiento.

Y si ello es así, no cabría considerar que en este caso la valoración de la sanción que esa AEPD pretende imponer a mi representada deba partir del volumen de facturación del Grupo Santander, sino únicamente de OPENBANK, entendida ésta como "empresa", a los efetos previstos en el artículo 4.18 del RGPD, sin que quepa la remisión a los artículos 101 y 102 del TFUE.

Además, mi representada considera necesario poner de manifiesto a la AEPD que la aplicación automática de los artículos 101 y 102 del TFUE, basada únicamente en un considerando del RGPD y las Directrices no es una cuestión pacífica en el Derecho de la Unión. A tal efecto, OPENBANK desea llamar la atención de la AEPD sobre la existencia de un procedimiento en trámite ante el Tribunal de Justicia de la Unión Europea (asunto C-383/23), en que el Vestre Landsret (Tribunal Superior de Dinamarca Occidental) ha solicitado del Tribunal que responda a las siguientes cuestiones:

1. El término "empresa" que figura en el artículo 83, apartados 4 a 6, del Reglamento general de protección de datos, ¿debe entenderse como una empresa en el sentido

de los artículos 101 y 102 TFUE, en relación con el considerando 150 de dicho Reglamento, y de la jurisprudencia del Tribunal de Justicia de la Unión Europea relativa al Derecho de la competencia de la UE, de modo que el término "empresa" abarca cualquier entidad que ejerza una actividad económica, con independencia del estatuto jurídico de dicha entidad y de su modo de financiación?.

2.En caso de respuesta afirmativa a la primera cuestión, ¿debe interpretarse el artículo 83, apartados 4 a 6, del Reglamento general de protección de datos en el sentido de que, a la hora de imponer una multa a una empresa, debe tenerse en cuenta el volumen de negocios total anual a nivel mundial de la entidad económica de la que forma parte la empresa, o únicamente el volumen de negocios total anual a nivel mundial de la propia empresa?

(…)

De este modo, no sólo se plantea si serían aplicables de forma automática, como pretende la AEPD, los citados artículos 101 y 102 del TFUE, sino incluso si en ese caso procedería utilizar la base de cálculo que la AEPD pretende aplicar de forma automática en este caso.

(…)

Es decir, conforme a la doctrina del "acto claro" el hecho de que se haya producido el planteamiento de una cuestión prejudicial ante el Tribunal implica, al menos, que existe una duda interpretativa acerca de la cuestión planteada, sobre la que no existe ningún pronunciamiento del Tribunal.

Es decir, si bien la AEPD aplica en el presente caso un automatismo derivado de la consideración de que no cabe una interpretación de lo dispuesto en el artículo 83.5 del RGPD distinta de la que aquélla lleva a cabo, lo cierto es que dicha norma no puede ser considerada "clara" a los efectos de la aplicación de la doctrina transcrita, al existir una cuestión pendiente de decisión por el Tribunal de Justicia de la UE que debe, precisamente, valorar si es posible o no la aplicación para la determinación del límite superior de la sanción del concepto de empresa establecido en los artículos 101 y 102 del TFUE.

Y si existe una duda, puesta de manifiesto ante el mencionado Tribunal, que precisa que por el mismo se aclare la interpretación del alcance del artículo 83.5 del RGPD, el cumplimiento de los principios del derecho penal, aplicables al procedimiento sancionador, exige que la interpretación efectuada por el órgano que ha de aplicar esta norma resulte ser la más beneficiosa para el encartado en el procedimiento administrativo, por mor de los principios de seguridad jurídica e interpretación favorable de las normas sancionadoras, lo que debería conducir de forma inmediata a la inaplicación de lo razonado en el Escrito sometido a las alegaciones de mi representada

SUBSIDIARIAMENTE, INEXISTENCIA DE CONTROL REAL Y EFECTIVO DE OPENBANK POR EL GRUPO SANTANDER

Incluso en el negado supuesto de que por parte de la AEPD no se tomasen en consideración lo indicado en la alegación anterior, es preciso señalar que mi mandante

considera que en el presente caso no resultarían de aplicación lo dispuesto en los artículos 101 y 102 del TFUE, lo que excluiría la realización del cálculo efectuado en el escrito respecto del que se emiten estas alegaciones, dado que no cabe apreciar la existencia de un control real y efectivo de la actividad de mi representada por parte del Grupo Santander.

En este sentido, si bien OPENBANK es una entidad perteneciente al Grupo Santander, y desde un punto de vista societario Banco Santander, S.A. es su sociedad matriz, la entidad cuenta con un Consejo de Administración al que le corresponde la gestión, administración y representación de la sociedad en todos los actos comprendidos en su objeto social con las facultades que le atribuyen la Ley y los Estatutos Sociales. El Consejo de Administración dispone de las más amplias atribuciones para la administración de la sociedad y, salvo en las materias reservadas a la competencia de la Junta General, es el máximo órgano de decisión de la sociedad.

El Consejo de Administración es por tanto el órgano de gobierno encargado, entre otros, de definir y supervisar la estrategia de la compañía, no siendo ésta competencia de la Junta General de Accionistas, cuyas facultades se limitan a aquellas materias reservadas por Ley o por Estatutos (…)

(…)

Teniendo en consideración lo anterior, cabe mencionar que el Consejo de Administración de OPENBANK está compuesto por 4 consejeros dominicales, 4 consejeros independientes y 2 consejeros externos. El Consejo de Administración está por tanto compuesto por mayoría de consejeros externos e independientes, precisamente para asegurar la independencia de ideas respecto de la matriz y que no actúen siguiendo indicaciones de la misma, no debiendo presuponerse que Banco Santander, S.A., a través de los éstos, aprueba las decisiones comerciales estratégicas de la misma ni promueve necesariamente el interés comercial de la sociedad matriz.

(…)

De este modo, la apreciación, sin más, de que OPENBANK es objeto de control efectivo y real por el Grupo Santander no responde a la realidad de la actuación de mi representada, suponiendo una vulneración del principio de separación entre la propiedad y la gestión de las sociedades mercantiles, teniendo en cuenta que sólo un 40% de los miembros del órgano de administración y dirección de la sociedad es designado por el Grupo Santander.

Adicionalmente, en modo alguno se ha acreditado que el Grupo Santander ejerza un papel decisorio en las políticas de mi representada y, menos aún, que su actuación en lo que respecta al cumplimiento de las normas de protección de datos (incluida la realización de EIPDs o la determinación de las medidas técnicas u organizativas que hayan de adoptarse en relación con un determinado tratamiento) proceda o sea siquiera interferida en modo alguno por el Grupo Santander.

(…)

Y, finalmente, mi mandante quiere poner de manifiesto cómo el escrito objeto de las presentes alegaciones contradice la práctica totalidad de los numerosos precedentes en los que la AEPD, para la determinación del importe del volumen de facturación al que se refiere el artículo 85 del RGPD, no ha tomado en cuenta el importe global del Grupo al que pertenece una entidad y sino el de la propia entidad en particular. En este sentido, esta parte no conoce de la existencia de ninguna resolución de la AEPD relacionada con empresas integrantes de grupos bancarios, aseguradores, del sector de las telecomunicaciones o energéticos distintos de aquel al que pertenece mi representada en que se haya aplicado el criterio ahora sostenido en la Resolución recurrida, lo que conduciría a una situación de desigualdad de las empresas integrantes del Grupo Santander respecto de las restantes que operan en su sector, contraviniendo así el principio de igualdad ante la ley establecido en el artículo 14 de la Constitución.

Por ello, entiende mi representada que nuevamente debe invocarse el principio de confianza legítima, dado que la AEPD se aparta de la totalidad de los precedentes generados por la misma para determinar en este caso el volumen de facturación no de mi representada, sobre la que recae el, ya sea ha dicho que contrario a derecho, reproche sancionador, sino del Grupo Santander, sin acreditar que el mismo participe en la toma de decisiones, con independencia de que corresponda a aquél la tenencia de su capital íntegro, y de forma distinta a los restantes operadores en su sector de actividad, así como en otros sectores.

(…)

SOBRE LA VULNERACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD

Además de lo ya indicado en las alegaciones anteriores, mi representada considera preciso poner de manifiesto que el considerando 150 del RGPD, al que la AEPD parece remitirse únicamente para considera aplicable a este caso el volumen de facturación del Grupo Santander no sólo se refiere a la aplicación de los artículos 101 y 102 del TFUE, sino que indica asimismo que la autoridad de control "debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción".

Y recordemos que en el presente caso la AEPD no ha apreciado que exista una gravedad en la conducta que deba determinar un incremento en la gravedad de la sanción, sino que esa gravedad se basa única y exclusivamente en un simple automatismo que conduce a prácticamente triplicar el importe de la sanción sin evaluar ninguna circunstancia relacionada con la misma, más allá del hecho de que OPENBANK pertenezca al Grupo Santander."

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

HECHOS PROBADOS

PRIMERO.- La parte reclamante, manifiesta que con fecha 16 de agosto de 2021 se contrató por un tercero una cuenta bancaria y una tarjeta de débito a su nombre con la entidad bancaria Openbank, sin su autorización.

SEGUNDO.- Obra en expediente que el sistema que se utilizó para abrir la cuenta bancaría fue mediante IBAN que requiere la aportación de un número de cuenta de otro banco facilitado por el interesado y del que sea titular.

El interesado ingresó una cuenta IBAN de otra entidad bancaria de la que la parte reclamante es titular, y adjuntó foto del anverso y reverso del DNI de la parte reclamante, tal y como establece el procedimiento de contratación de la parte reclamada.

Consta que la validación de la cuenta IBAN de otra entidad de la que es titular la parte reclamante fue realizada por Iberpay el 16 de agosto de 2021.

Se constata que el domicilio del DNI proporcionado durante la contratación no coincide con la del propio contrato ni tampoco coincide la firma manuscrita digitalizada que figura en el contrato con la que figura en el DNI proporcionado durante la contratación.

TERCERO.- Obra en el expediente que, en el certificado de firma electrónica proporcionado por un tercero de confianza, que acredita la validación de la contratación mediante envío de mensaje SMS, figura un número de teléfono móvil distinto al aportado por la parte reclamante en su denuncia ante la DGP.

FUNDAMENTOS DE DERECHO

I
Competencia

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 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
Contestación a las alegaciones presentadas

1.- La parte reclamada manifiesta que cumplió las previsiones contempladas en la normativa de prevención de blanqueo de capitales en relación con las obligaciones de identificación formal del cliente. Afirma que para llevar a cabo la contratación siguió uno de los procedimientos establecidos por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias **(**SEPBLAC).

Aduce que el método elegido por el reclamante en la apertura la cuenta bancaría, fue mediante IBAN que requiere la aportación de un número de cuenta de otro banco facilitado por el interesado y del que sea titular.

En este sentido, el interesado ingresó una cuenta IBAN de otra entidad bancaria de la que la parte reclamante es titular, y adjuntó foto del anverso y reverso del DNI de la parte reclamante, tal y como establece el procedimiento de contratación de la parte reclamada.

La validación de la cuenta IBAN de otra entidad de la que es titular la parte reclamante fue realizada por Iberpay el mismo día de los hechos 16 de agosto de 2021.

Sobre esta cuestión, esta Agencia debe señalar que el objeto del presente procedimiento no es comprobar si se dio cumplimiento a la dispuesto en la normativa de prevención de blanqueo de capitales, sino valorar si la parte reclamada actuó con diligencia para dar cumplimiento a la normativa de protección de datos. Las obligaciones que la normativa de prevención de blanqueo de capitales impone a los sujetos obligados tienen como finalidad evitar y prevenir el blanqueo de capitales. Sin embargo, la normativa de protección de datos tiene un enfoque diferente, pues su objeto es procurar la protección del derecho a la protección de datos personales. Por ello puede ocurrir que alguna de las medidas adoptadas para la identificación formal de los clientes sea también adecuada para identificar a los titulares de los datos que van a ser sometidos a tratamiento y con ella se evite la materialización de los riesgos para los derechos y libertades de los clientes, pero no siempre será así, pues con el cumplimiento de las obligaciones de identificación formal no puede darse por cumplido el RGPD, que requiere una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan (principio de responsabilidad proactiva). De este modo la adopción de las medidas adecuadas debe realizarse sobre la base de un análisis de riesgos para los derechos y libertades de las personas físicas, y entre estos riesgos se encuentra el riesgo de fraude o suplantación de identidad.

Por ello, el cumplimiento del RGPD puede requerir la adopción de otras medidas adicionales o distintas a las previstas en la normativa de prevención del blanqueo de capitales, que serán las que se deriven de la valoración de los riesgos para los derechos y libertades de las personas, y para lo que se tendrán en cuenta las disposiciones del art. 28 de la LPDGDD que considera que para la adopción de las medidas han de valorarse los mayores riesgos que podrían producirse cuando el tratamiento pudiera generar situaciones de usurpación de identidad o fraude, o pérdidas financieras.

Sin perjuicio de lo anteriormente expuesto, ha de aclararse en este punto que, si bien la parte reclamada pudo seguir uno de los procedimientos aprobados por el SEPBLAC

para supuestos de relaciones de negocio y operaciones no presenciales, esto no acredita por sí sólo el cumplimiento de la normativa de prevención de blanqueo de capitales.

Así sobre esta cuestión la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante LPBC) dispone en su artículo 3.2, en cuanto a la identificación formal de los clientes, lo siguiente

"2. Con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualesquiera operaciones, los sujetos obligados comprobarán la identidad de los intervinientes mediante documentos fehacientes. En el supuesto de no poder comprobar la identidad de los intervinientes mediante documentos fehacientes en un primer momento, se podrá contemplar lo establecido en el artículo 12, salvo que existan elementos de riesgo en la operación.

Reglamentariamente se establecerán los documentos que deban reputarse fehacientes a efectos de identificación"

Y según el artículo 12 del Reglamento de desarrollo de la LPBC, aprobado por el Real Decreto 304/2014, de 5 de mayo, en las relaciones de negocio y operaciones no presenciales:

"*1. Los sujetos obligados podrán establecer relaciones de negocio o ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes, siempre que concurra alguna de las siguientes circunstancias:*

a) La identidad del cliente quede acreditada mediante la firma electrónica cualificada regulada en el Reglamento (UE) n.° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En este caso no será necesaria la obtención de la copia del documento, si bien será preceptiva la conservación de los datos de identificación que justifiquen la validez del procedimiento. En el resto de casos, cuando la firma electrónica utilizada no reuniese los requisitos de la firma electrónica cualificada seguirá siendo preceptiva la obtención en un mes de una copia del documento de identificación.

b) El primer ingreso proceda de una cuenta a nombre del mismo cliente abierta en una entidad domiciliada en España, en la Unión Europea o en países terceros equivalentes.

c) Se verifiquen los requisitos que se determinen reglamentariamente.

En todo caso, en el plazo de un mes desde el establecimiento de la relación de negocio, los sujetos obligados deberán obtener de estos clientes una copia de los documentos necesarios para practicar la diligencia debida.

Cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible o en poder del sujeto obligado, será preceptivo proceder a la identificación presencial.

Los sujetos obligados adoptarán medidas adicionales de diligencia debida cuando en el curso de la relación de negocio aprecien riesgos superiores al riesgo promedio.

2. Los sujetos obligados establecerán políticas y procedimientos para afrontar los riesgos específicos asociados con las relaciones de negocio y operaciones no presenciales." (el subrayado es de la AEPD)

En consecuencia, la LPBC prevé que en situaciones de mayor riesgo los sujetos obligados adopten de acuerdo con sus políticas internas medidas adicionales, siendo preceptiva la identificación presencial cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible o en poder del sujeto obligado.

Por tanto, procede desestimar esta alegación de la parte reclamada.

2.- Asimismo manifiesta la parte reclamada que el contrato fue firmado con firma avanzada.

La parte reclamada aporta certificado de firma electrónica avanzada que acredita la validación de la contratación mediante envío de mensajes SMS, pero este sistema no acredita la identidad sólo que el contrato se ha firmado. Openbank solicita la firma manuscrita y copia del DNI, para acreditar la identidad y la contratación, pero la firma manuscrita no coincide con la del DNI.

El certificado de firma electrónica proporcionado por un tercero de confianza acredita la validación de la contratación mediante envío de mensaje SMS, pero no acredita la identidad del contratante, como se ha dicho anteriormente, pues el SMS se envía a una línea de móvil aportada por la persona solicitante del préstamo, sin que la parte reclamada haya solicitado la documentación que acreditará la titularidad de la línea.

A este respecto, el TS en su sentencia de 13/12/2021, nº 1.456/2021, en relación con la contratación de un microcrédito y la diligencia desplegada, señalaba en su Fundamento Segundo lo siguiente:

"Respecto de la primera cuestión (falta de diligencia en la actuación) en el recurso de casación se reiteran las alegaciones que la entonces demandante hizo en el proceso de instancia, en el sentido de que Dineo Crédito, S.L. adoptó todas las medidas necesarias y oportunas, desde el punto de vista de la protección de datos personales, para tramitar la solicitud de microcrédito (registro en la plataforma; validación del DNI: con verificación de doble factor de 2 algoritmos que garantizan tanto la veracidad del número y la letra del documento como que el solicitante tiene en su poder el DNI, por original o copia; validación del número de teléfono móvil a través de un código PIN, validación de datos bancarios y validación de la tarjeta de crédito/débito aportada por el solicitante); y pese a la adopción de tales medidas, se podría haber cometido el delito de suplantación de identidad, de estafa y/o de uso indebido de documento verdadero.

Pues bien, hemos visto que el fundamento jurídico cuarto de la sentencia de instancia da cumplida respuesta a tales alegaciones. Señala allí la Sala de la Audiencia Nacional que en la resolución sancionadora se analiza de manera detallada el mecanismo de verificación de identidad del solicitante del crédito que Dineo Crédito, S.L. tenía establecido y queda de manifiesto su insuficiencia. Así, con el denominado "registro en la plataforma", trámite en el que se recaban del cliente determinados datos (entre ellos, el número de D.N.I., dos teléfonos y el correo electrónico) únicamente se demuestra que desde ese momento existe un tratamiento de datos personales, pero se ignora es si los datos facilitados por el cliente y recogidos por Dineo, son de la persona que los facilita como suyos o de un tercero. En cuanto a la fase que la recurrente denomina de "validación del DNI" (un algoritmo que permite determinar si el DNI facilitado por el cliente se corresponde o no con un DNI real o válido), tal medida únicamente demuestra que se trata de un número de documento que existe y que "alguien" es titular de ese DNI. Por su parte, la llamada "validación del número de móvil", que consiste en el envío al terminal móvil del contratante de una clave o pin de cuatro cifras que, posteriormente, el cliente debe introducir en el formulario al que accede desde la página web de Dineo, únicamente acredita que quien pretende contratar con Dineo, tiene acceso a ese número de móvil, pero nada dice sobre la identidad del contratante.

La fase del procedimiento de contratación del préstamo denominada "validación de datos bancarios", que consiste en verificar si la cuenta bancaria "es real" y está asociada efectivamente a una cuenta bancaria, es también irrelevante desde el punto de vista del respeto a las obligaciones impuestas por la normativa de protección de datos, pues sólo asegura el buen fin del préstamo, esto es, que el importe prestado se dirigirá a una cuenta abierta y activa, pero nada aporta en cuanto a que el titular de esa cuenta sea precisamente la persona que figura en el DNI utilizado. Y, por último, la fase denominada validación de la "tarjeta de crédito", consistente en que se carga en ella un céntimo que automáticamente resulta reintegrado, no consta que en el caso que nos ocupa se llevara a cabo, al no aparecer en los registros informáticos de la recurrente.

En definitiva, ninguna de las medidas adoptadas por la recurrente está destinada a acreditar que la persona que solicita el microcrédito coincide con el titular del DNI aportado. Y, en efecto, continua explicando la sentencia recurrida, las pruebas practicadas en la vía administrativa vinieron a poner de manifiesto que, respecto de la línea de teléfono facilitada cuando se solicitó el crédito, ni el nombre, apellidos y NIF del titular de la línea coinciden con los datos personales del denunciante (titular del DNI); y en relación con la cuenta bancaria que figura en los registros de Dineo, a la que se habría transferido el importe del micro préstamo, los datos del titular de la cuenta en la fecha de la contratación del crédito tampoco coinciden con los datos personales del denunciante. Ni siquiera el titular del móvil y el de la cuenta bancaria son la misma persona.

Estas apreciaciones de la Sala de instancia sobre la insuficiencia de las medidas adoptadas en el procedimiento de contratación on line, y, en definitiva, sobre falta de diligencia en la actuación por la recurrente, en modo alguno han quedado desvirtuadas en casación, donde la representación de Dineo Crédito, S.L. ha reiterado

las manifestaciones que hizo en el proceso de instancia, pero nada ha aportado que sirva para rebatir las conclusiones de la Sala sentenciadora.

En fin, compartimos el parecer de la Sala de la Audiencia Nacional acerca de la insuficiencia de las medidas aplicadas por la recurrente en el procedimiento de contratación. A las consideraciones que se exponen en la sentencia recurrida, que compartimos y hacemos nuestras, únicamente añadiremos dos observaciones:

En primer lugar, las medidas de verificación aplicadas por la recurrente parecen enteramente encaminadas asegurar el buen fin del préstamo, pero, en cambio, se desentienden enteramente del objetivo de verificar la veracidad y exactitud de los datos, y, en particular, de comprobar que quien solicita el crédito es precisamente quien dice ser. De este modo, en cualquier caso en el que un tercero utilice indebidamente un DNI sustraído o extraviado para realizar una compra o solicitar un crédito on line, siempre se consumaría el tratamiento inconsentido de los datos personales del titular del documento, aunque éste hubiese denunciado en su día ante las autoridades la pérdida o sustracción de su DNI, pues ninguna de las medidas enunciadas por la recurrente aparece mínimamente orientada a impedir o dificultar que ese resultado se produzca.

En segundo lugar, lo anterior no significa que se haga recaer sobre la empresa contratante la responsabilidad de impedir que se produzca un hecho ilícito o delictivo como es la utilización fraudulenta de un DNI por parte de quien no es su titular. Pero sí es exigible a dicha empresa contratante, como diligencia necesaria para que no se le pueda reprochar el incumplimiento de sus obligaciones en materia de protección de datos de carácter personal -tanto en lo que se refiere a la exigencia de consentimiento del interesado como en lo relativo al principio de veracidad y exactitud de los datos- la implantación de medidas de control tendentes a verificar que la persona que pretende contratar es quien dice ser, esto es, que coincide con el titular del DNI aportado".

Así las cosas, en este caso la reclamada no ha comprobado de forma diligente la veracidad de los datos aportados, y, en particular, que quien solicitaba el crédito era precisamente quien decía ser, de lo que se infiere la insuficiencia de las medidas adoptadas para verificar este extremo.

Además, el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, sólo considera equivalente a la firma manuscrita la firma cualificada, que no fue la utilizada en este caso.

3.- Añade la parte reclamada que verificó la titularidad de la cuenta bancaria de conformidad con el procedimiento aceptado por el SEPBLAC

Llegados a este punto, hay que reiterar que Openbank cumpla con la normativa de prevención de blanqueo de capitales no supone que cumpla también con la normativa de protección de datos, la simple introducción del número de una cuenta en el momento de la contratación no acredita por sí solo que la persona que facilita esa información sea la titular.

Lo que debe analizarse en este caso es si la parte reclamada en supuestos de alto riesgo de fraude o suplantación, como ocurre en la contratación no presencial, tuvo una actuación diligente para la protección de los derechos y libertades de los interesados.

Openbank seguía un procedimiento aceptado por SEPBLAC, pero esta organización ya había trasladado que ese procedimiento no era suficiente y debería reforzarse, si bien daba un plazo hasta que fuera obligatorio utilizar el nuevo. Por este motivo, al menos, Openbank sabía que el procedimiento era insuficiente pero no valoró el impacto que podría tener en sus clientes. No adoptó ninguna medida para evitar la suplantación de identidad.

Además, en el procedimiento adoptado por el SEPLAB se dispone que la autorización del "Procedimiento de solicitud de confirmación de datos sobre titularidad de cuentas entre entidades" se entiende sin perjuicio del cumplimiento por los sujetos obligados de cualesquiera otras obligaciones, en particular las establecidas por la normativa tributaria y de protección de datos de carácter personal.

Por otro lado, el reclamante se entera de que han abierto una cuenta a su nombre por una llamada de la policía, llama a la parte reclamada y le dicen que tiene que poner una denuncia. Envía la denuncia a Openbank el día 17 de marzo de 2022 y el día 28 del mismo mes y año, después de preguntar otra vez a la parte reclamada le contesta que lo está analizando el departamento de seguridad, por lo que tampoco se aprecia una actuación diligente por parte de la entidad reclamada.

4.- En respuesta a las alegaciones formuladas por Openbank, respecto a que esta Agencia archivó otras reclamaciones similares, hay que manifestar que estas se archivaron, pero siempre sin perjuicio de que la Agencia, aplicando los poderes de investigación y correctivos que ostenta, pudiera llevar a cabo posteriores actuaciones relativas al tratamiento de datos tal y como indican las resoluciones invocadas.

5.- Critica Openbank la agravación de la sanción, en el acuerdo de la Directora de 13 de diciembre de 2023, sobre la única y exclusiva base de que se encuentra integrada en el Grupo Santander.

Considera Openbank que *"la interpretación de las Directrices es diametralmente opuesta a lo establecido en el RGPD, dado que el artículo 83.5 del mismo se refiere a "empresa" y no a "grupo de empresas", que es el concepto que pretende aplicar la AEPD, sobre la única y exclusiva base del considerando 150 del RGPD y de unas directrices que, por su propia definición y contenido, carecen de valor normativo, no pudiendo suponer un criterio interpretativo contrario a la literalidad del RGPD."*

En este caso, el considerando 150 del RGPD aclara a qué se refiere el concepto de "empresa" a los efectos del RGPD.

Y es que el considerando 10 del RGPD indica que *"Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la*

Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea."

Para la consecución de tal aplicación uniforme de la normativa en materia de protección de datos de carácter personal, se han aprobado las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, tal y como indica el primer párrafo de tal documento:

"El Consejo Europeo de Protección de Datos (CEPD) ha adoptado estas directrices para armonizar la metodología que utilizan las autoridades de control al calcular el importe de la multa. Estas Directrices complementan las Directrices previamente adoptadas sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679 (WP253), que se centran en las circunstancias en las que se impone una multa."

Tales Directrices disponen lo siguiente:

"118. En cuanto al término «empresa», el legislador europeo proporciona aclaraciones adicionales explícitas. El considerando 150 del RGPD establece: «Cuando se impongan multas administrativas a una empresa, una empresa debe entenderse como una empresa de conformidad con los artículos 101 y 102 del TFUE a estos efectos».

119. Por lo tanto, el artículo 83, apartados 4 a 6, del RGPD, a la luz del considerando 150, se basa en el concepto de empresa de conformidad con los artículos 101 y 102 del TFUE, sin perjuicio de lo dispuesto en el artículo 4, apartado 18, del RGPD (que define lo que es una empresa) y en el artículo 4, apartado 19, del RGPD (que define lo que es un grupo de empresas). El primer concepto se utiliza principalmente en el capítulo V del RGPD, en la frase grupo de empresas que participan en una actividad económica conjunta. Además, el término se aplica en un sentido general, no como destinatario de una disposición u obligación.

120. Por consiguiente, en los casos en que el responsable o encargado del tratamiento sea (parte de) una empresa en el sentido de los artículos 101 y 102 del TFUE, el volumen de negocios combinado de dicha empresa en su conjunto puede utilizarse para determinar el límite máximo dinámico de la multa (véase el capítulo 6.2.2) y para garantizar que la multa resultante se ajuste a los principios de efectividad, proporcionalidad y disuasión (artículo 83, apartado 1, del RGPD).

121. El TJUE ha desarrollado una amplia jurisprudencia sobre el concepto de empresa. El término «empresa», «incluye a todas las entidades que ejercen una actividad económica, independientemente de la condición jurídica de la entidad y de la forma en que se financia». A efectos del derecho de la competencia, las «empresas» se identifican por tanto con unidades económicas y no con unidades jurídicas. Diferentes sociedades pertenecientes al mismo grupo pueden constituir una unidad económica y, por tanto, una empresa en el sentido de los artículos 101 TFUE y 102 TFUE.

122. En consonancia con la jurisprudencia consolidada del TJUE, el término empresa en los artículos 101 y 102 del TFUE puede referirse a una única unidad económica (SEU, por sus siglas en inglés), incluso si dicha unidad económica está formada por varias personas físicas o jurídicas. Si varias entidades forman una SEU depende en gran medida de si la entidad individual es libre en su capacidad de toma de decisiones o de si una entidad principal, a saber, la sociedad matriz, ejerce una influencia decisiva sobre las demás. Los criterios para determinarlo se basan en los vínculos económicos, jurídicos y organizativos entre la sociedad matriz y su filial, por ejemplo, el importe de la participación, los vínculos de personal u organización, las instrucciones y la existencia de contratos de empresa.

123. En consonancia con la doctrina del SEU, el artículo 83, apartados 4 a 6, del RGPD sigue el principio de responsabilidad corporativa directa, que implica que todos los actos realizados o descuidados por personas físicas autorizadas para actuar en nombre de empresas sean atribuibles a estas últimas y se consideren un acto y una infracción cometidos directamente por la propia empresa. El hecho de que algunos empleados no cumplieran un código de conducta no es suficiente para interrumpir esta atribución. Más bien, solo se perturba cuando la persona física actúa únicamente para sus propios fines privados o para fines de un tercero, convirtiéndose así en un responsable separado (es decir, la persona física ha actuado en exceso de su mandato permitido. Este principio del Derecho de la Unión Europea y el ámbito de aplicación de la responsabilidad corporativa tienen prioridad y no deben verse socavados limitándolo a los actos de determinados funcionarios (como los directivos principales) al contradecir el Derecho nacional. No es pertinente qué persona física actuó en nombre de cuál de las entidades. Por consiguiente, no debe exigirse a la autoridad de control y a los órganos jurisdiccionales nacionales que determinen o identifiquen a una persona física en las investigaciones o en la decisión de multa".

En el presente caso, teniendo en cuenta las circunstancias concurrentes, la regulación del RGPD y lo previsto en las Directrices precitadas, se ha de considerar a los efectos de la imposición de la multa administrativa al volumen de negocios del grupo y no sólo al volumen de negocios de Openbank.

No obstante, señala la parte reclamada que *"la aplicación automática de los artículos 101 y 102 del TFUE, basada únicamente en un considerando del RGPD y las Directrices no es una cuestión pacífica en el Derecho de la Unión."* Indicando, asimismo que existe al respecto *"un procedimiento en trámite ante el Tribunal de Justicia de la Unión Europea (asunto C-383/23)"*.

Hay que poner de manifiesto que tal cuestión prejudicial todavía no ha sido resuelta por el Tribunal de Justicia de la Unión Europea. A diferencia de lo acontecido en el asunto C-807/2021, respecto al que el mencionado tribunal ha dictado sentencia el 5 de diciembre de 2023, sentencia en la que se indica lo siguiente:

"55 Como ha señalado el Abogado General en el punto 45 de sus conclusiones, la remisión realizada en el considerando 150 del RGPD al concepto de «empresa», en el sentido de los artículos 101 TFUE y 102 TFUE, debe entenderse en este contexto específico del cálculo de las multas administrativas impuestas por las infracciones contempladas en el artículo 83, apartados 4 a 6, del RGPD.

56 A este respecto, procede subrayar que, a efectos de la aplicación de las normas de competencia, contempladas en los artículos 101 TFUE y 102 TFUE, este concepto comprende cualquier entidad que ejerza una actividad económica, con independencia del estatuto jurídico de esa entidad y de su modo de financiación. Designa, así, una unidad económica aunque, desde el punto de vista jurídico, dicha unidad económica esté constituida por varias personas físicas o jurídicas. Esta unidad económica consiste en una organización unitaria de elementos personales, materiales e inmateriales que persigue de manera duradera un fin económico determinado (sentencia de 6 de octubre de 2021, Sumal, C-882/19, EU:C:2021:800, apartado 41 y jurisprudencia citada).

57 Así pues, del artículo 83, apartados 4 a 6, del RGPD, que tiene por objeto el cálculo de las multas administrativas por las infracciones enumeradas en esos apartados, se desprende que, en el supuesto de que el destinatario de la multa administrativa sea una empresa o forme parte de ella, en el sentido de los artículos 101 TFUE y 102 TFUE, el importe máximo de la multa administrativa se calcula sobre la base de un porcentaje del volumen de negocio total anual global del ejercicio financiero anterior de la empresa de que se trate.

58 En definitiva, como ha señalado el Abogado General en el punto 47 de sus conclusiones, solo una multa administrativa cuya cuantía se determine en función de la capacidad económica real o material de su destinatario y, por tanto, impuesta por la autoridad de control basándose, por lo que respecta a su importe, en el concepto de unidad económica en el sentido de la jurisprudencia citada en el apartado 56 de la presente sentencia, puede reunir los tres requisitos enunciados en el artículo 83, apartado 1, del RGPD, a saber, ser a la vez efectiva, proporcionada y disuasoria." (el subrayado es nuestro).

6.- También alega la parte reclamada la inexistencia de control real y efectivo de Openbank por el Grupo Santander, *"lo que excluiría la realización del cálculo efectuado en el escrito respecto del que se emiten estas alegaciones, dado que no cabe apreciar la existencia de un control real y efectivo de la actividad de mi representada por parte del Grupo Santander."*

Añadiendo posteriormente que *"en modo alguno se ha acreditado que el Grupo Santander ejerza un papel decisorio en las políticas de mi representada y, menos aún, que su actuación en lo que respecta al cumplimiento de las normas de protección de datos (incluida la realización de EIPDs o la determinación de las medidas técnicas u organizativas que hayan de adoptarse en relación con un determinado tratamiento) proceda o sea siquiera interferida en modo alguno por el Grupo Santander."*

Openbank se integra por integración global en las cuenta anuales consolidadas del Banco Santander (Grupo Santander), como "Entidad dependiente", las cuales se definen en el Informe anual consolidado 2022 del Grupo Santander (https://www.santander.com/content/dam/santander-com/es/documentos/informe-financiero-anual/2022/ifa-2022-informe-financiero-anual-consolidado-es.pdf) (página 555) como *"Se consideran entidades dependientes aquellas sobre las que el Banco tiene capacidad para ejercer control. Banco Santander controla una entidad cuando está expuesto, o tiene derecho, a rendimientos variables procedentes de implicación en la entidad participada y tiene la capacidad de influir en esos rendimientos a través*

de su poder sobre la entidad participada. Los estados financieros de las entidades dependientes se consolidan con los de Banco Santander por aplicación del método de integración global. Consecuentemente, todos los saldos y efectos de las transacciones efectuadas entre las sociedades consolidadas se eliminan en el proceso de consolidación"

Y en el Anexo I de dicho Informe Anual 2022, página 807, aparece OPEN BANK S.A. como "Entidad dependiente" de Banco Santander, con una participación de Banco Santander en el capital de esta de 100% y un porcentaje de derechos de voto del 100%.

Luego no cabe duda alguna de que está acreditado que Openbank forma parte de Grupo Santander así como que éste ejerce una influencia decisiva sobre Openbank en relación con los fines y los medios en materia de protección de datos de carácter personal.

A tal efecto, se hace necesario traer a colación lo que establece el mencionado Informe Anual 2022 del Grupo Santander en relación con la privacidad, la protección de datos y ciberseguridad (página 50) de todo el grupo:

"3.4.3 Privacidad, protección de datos y ciberseguridad

Privacidad y protección de datos

Nuestros estándares permiten a las personas mantener el control de sus datos personales asegurando que solo utilizamos los datos estrictamente necesarios para los fines específicos para los que se recogen. Y aplicamos medidas que permiten la supresión o rectificación de los datos que puedan ser inoportunos, inexactos o incompletos, así como su conservación durante el tiempo estrictamente necesario para su uso legítimo. Nuestras medidas de seguridad garantizan la confidencialidad, la integridad, la disponibilidad y la resistencia de los sistemas y servicios asociados a las actividades de tratamiento de datos.

Nuestro programa de cumplimiento vela por una correcta gestión del riesgo en materia de protección de datos:

- *Criterios corporativos que marcan líneas de actuación generales ligadas a los requerimientos normativos.*
- *Responsabilidad de las unidades locales en el cumplimiento de las obligaciones contenidas en el Reglamento General de Protección de Datos (RGPD) y/o en las diferentes normativas locales aplicables en la materia.*
- *Un modelo de gobierno sólido basado en:*
  - *una política corporativa de referencia y sus diferentes trasposiciones locales;*
  - *la designación de la figura del delegado de protección de datos (DPO) y/o responsables en cada unidad, formalmente nombrados y debidamente comunicados a las autoridades de control locales;*
  - *un programa corporativo de supervisión basado en indicadores periódicos de gestión, un programa anual de revisiones; y una reunión anual de*

seguimiento presidida por el Chief Compliance Officer del Grupo, en la que se informa del estado de situación de las unidades y otras cuestiones relevantes en materia de protección de datos.

Otras medidas que sirven de refuerzo a nuestro compromiso con la protección de los datos son:

- *La aplicación de un modelo homogéneo de seguimiento y reporte de las unidades.*
- *Colaboración con terceros proveedores de servicios que deben cumplir los principios exigidos por la normativa de protección de datos.*
- *Las revisiones específicas que, como parte de su programa anual, lleva a cabo auditoría interna con relación al cumplimiento de la normativa de protección de datos.*
- *El uso de herramientas corporativas para tareas de gestión en materia de protección de datos, entre las que se incluye un inventario de actividades de tratamiento a nivel Grupo (más de 6.000 actividades de tratamiento), el reporting periódico de indicadores y la información sobre la gestión de incidentes de seguridad realizada por las unidades.*
- *El fomento de iniciativas corporativas y el intercambio de mejores prácticas entre unidades del Grupo, como la celebración de talleres y cursos formativos online.*
- *La formación técnica de los DPO y responsables en materia de protección de datos.*
- *El seguimiento continuo de las novedades regulatorias, que permite contar con criterios, metodologías y documentación sólidos y actualizados.*
- *La formación y concienciación de los empleados.*

Ciberseguridad

Promovemos en los empleados comportamientos que protegen la información de los clientes y al Grupo como parte de nuestra cultura. Ayudamos a nuestros clientes y la sociedad a mantenerse seguros y prosperar en el mundo digital. Y promocionamos colaboraciones público-privadas para combatir el cibercrimen a través del intercambio de conocimientos en materia de ciberseguridad.

En Santander la ciberseguridad está integrada en nuestra cultura de riesgos, siendo uno de los aspectos que se valoran en la evaluación del desempeño de nuestros empleados.
En 2022 hemos trabajado en la formación y concienciación continua de nuestro equipo:

- *Actualización del curso obligatorio sobre ciberseguridad.*
- *Formación específica sobre ciberseguridad para distintos colectivos (operadores de pago, administradores de Tecnología de la Información, desarrolladores) y para ejecutivos y miembros del Consejo.*
- *Campañas de comunicación para empleados incorporando las nuevas técnicas utilizadas por los atacantes.*
- *Pruebas periódicas de phishing ético para mejorar nuestra resiliencia ante posibles amenazas, al mismo tiempo que animamos a reportar cualquier incidente o mensaje sospechoso a través de canales específicos para ello. Asimismo, hemos*

realizado las siguientes iniciativas para ayudar a los clientes y la sociedad a mantenerse seguros online:

(…)"

También señala Openbank que *"no conoce de la existencia de ninguna resolución de la AEPD relacionada con empresas integrantes de grupos bancarios, aseguradores, del sector de las telecomunicaciones o energéticos distintos de aquel al que pertenece mi representada en que se haya aplicado el criterio ahora sostenido en la Resolución recurrida, lo que conduciría a una situación de desigualdad de las empresas integrantes del Grupo Santander respecto de las restantes que operan en su sector, contraviniendo así el principio de igualdad ante la ley establecido en el artículo 14 de la Constitución."*

Por ello entiende Openbank que *"debe invocarse el principio de confianza legítima, dado que la AEPD se aparta de la totalidad de los precedentes generados por la misma para determinar en este caso el volumen de facturación no de mi representada, sobre la que recae el, ya sea ha dicho que contrario a derecho, reproche sancionador, sino del Grupo Santander".*

Las previsiones del RGPD en cuanto a lo que comprende el concepto de empresa, interpretado por las Directrices precitadas, a los efectos de si debe considerarse el volumen de negocio total anual global de una concreta empresa o del grupo empresarial, en los términos del artículo 83.4, 5 y 6 del RGPD para el cálculo de la multa administrativa, no es un proceso automático, sino que depende del examen del supuesto concreto.

De esta forma, el principio de confianza legítima alegado no puede ser considerado cuando la actuación de la AEPD no ha variado, ni la AEPD se separa de precedentes anteriores, sino que cada procedimiento tramitado es distinto y con sus propias circunstancias.

A mayor abundamiento de lo anterior, no procede exigir igualdad en la ilegalidad. La jurisprudencia es clara respecto a esto. Así, la Sentencia de la Audiencia Nacional de 28 de abril de 2023 (Rec. 409/2021) indica que

"*Se alude a un trato sancionador discriminatorio puesto que esa multa o sanción económica puede sustituirse por las medidas del art. 58 RGPD, medidas menos gravosas como podría ser el apercibimiento. Y hace referencia a otras infracciones cometidas por otras entidades. Por supuesto la actora trata de comparar esta situación con otro procedimiento sancionador que se menciona, pero no estamos ante un trato discriminatorio o que se vulnere el principio de igualdad puesto que es un principio que solo opera en el marco de la legalidad cuando situaciones de hecho iguales tienen un tratamiento diferente sin justificación razonable. Como señala la STS de 20 de enero 2004, "la igualdad ha de predicarse dentro de la legalidad, de modo que si la actuación correcta de la Administración es la ahora enjuiciada, según hemos declarado, la invocada como contraria a ella no lo fue y, por consiguiente, no cabe esgrimirla para pedir que se le aplique al recurrente un trato igual, ya que, como esta Sala del Tribunal Supremo ha declarado en sus sentencias de 16 de junio de 2003 , 14 de julio de 2003 y 20 de octubre de 2003 que «el principio de igualdad carece de trascendencia para*

amparar una situación contraria al ordenamiento jurídico», y ello, como indica la propia Sala sentenciadora, al margen de no haberse acreditado la actuación administrativa aducida como contradictoria con la presente".

En igual sentido señala la Sentencia del Tribunal Supremo de 2 de abril de 2014 (Rec. 1916/2010) que indica lo siguiente:

"*la legalidad prevalece sobre una posible lesión del principio de igualdad". En este caso, estamos ante una infracción administrativa que se pretende comparar con otra que ha tenido diferente solución, pero de lo que se observa en la alegación que se formula por la parte actora escasamente se puede efectuar una comparación de una situación y otra. Recordemos que conforme a la doctrina constitucional consolidada para apreciar la concurrencia de una vulneración del principio de igualdad han de concurrir los siguientes presupuestos: 1) aportación de un término idóneo de comparación demostrativa de la identidad sustancial de las situaciones jurídicas que han recibido trato diferente, 2) que el trato desigual no esté fundado en razones objetivas que lo justifiquen, y 3) que el juicio comparativo se desarrolle en el marco de la legalidad, pues no cabe invocar el principio de igualdad en la ilegalidad para perpetuar situaciones contrarias a lo previsto por el ordenamiento jurídico. Así las cosas, la conducta por la que ha sido sancionada la parte actora y que es contraria a derecho no permite que su responsabilidad sea más atenuada por el hecho de que en otros supuestos, que se desconocen, la sanción impuesta no fuera económica y se considerase más beneficiosa*".

7.- Finalmente manifiesta la parte reclamada que la sanción vulnera el principio de proporcionalidad.

Sobre este particular ha de recordarse que el artículo 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 por tanto según se deduce del precepto han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

La cuantía a la que puede ascender la sanción por la infracción del artículo 6.1 del RGPD, de conformidad con el art. 83.5 del RGPD, es *de "20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".*

Por ello, independientemente de lo anterior, la multa impuesta a la parte reclamada por la infracción del artículo 6 del RGPD no es desproporcionada, pues incluso si solamente se tuviera en consideración únicamente el volumen de negocios de Openbank (de acuerdo con el informe recogido de la herramienta AXESOR, su volumen de negocios es de 15.626.315 de euros en el año 2021), la sanción no supera los 20.000.000 de euros ni alcanza el 4% del volumen de negocio total anual del ejercicio financiero anterior, en los términos del art. 83.4 del RGPD.

Por lo expuesto, no se aceptan las alegaciones presentadas ni al acuerdo de inicio ni a la propuesta de resolución ni al acuerdo de la Directora de fecha 13 de diciembre de 2023.

III
Obligación incumplida

El artículo 4.1 del RGPD define: *«datos personales»* como *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*

El artículo 6 del RGPD, "*Licitud del tratamiento*", señala en su apartado 1 los supuestos en los que el tratamiento de datos de terceros es considerado lícito:

"1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

En ese sentido el Considerando 40 del RGPD señala:

"*(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."*

En este caso, se considera que la parte reclamada, vulneró el artículo 6.1 del RGPD. toda vez que realizó el tratamiento de los datos personales de la parte reclamante sin legitimación para ello. Los datos personales del reclamante fueron incorporados a los sistemas de información de la compañía, sin que haya acreditado que dispusiera de base legal para la recogida y el tratamiento posterior de sus datos personales.

En consecuencia, ha efectuado un tratamiento de los datos personales sin que haya acreditado que cuente con la habilitación legal para ello.

A este respecto, y esto es lo esencial, la reclamada no acredita la legitimación para el tratamiento de los datos del reclamante.

El respeto al principio de licitud que está en la esencia del derecho fundamental de protección de datos de carácter personal exige que conste acreditado que la responsable del tratamiento desplegó la diligencia imprescindible para acreditar ese extremo. De no actuar así -y de no exigirlo así esta Agencia, a quien le incumbe velar por el cumplimiento de la normativa reguladora del derecho de protección de datos de carácter personal- el resultado sería vaciar de contenido el principio de licitud.

Así pues, se estima que los hechos que se someten a la valoración de esta Agencia son constitutivos de una infracción del artículo 6.1 del RGPD.

En el presente caso, resulta acreditado que Openbank trató indebidamente los datos de la parte reclamante, dado que abrió una cuenta bancaria a su nombre, sin legitimación para ello aunque el suplantador tenía los datos del reclamante, por parte de la reclamada no se comprobó que no coincidía la firma del DNI con la del contrato.

La actuación de la parte reclamada se considera grave, pues al tratar sin una de las bases de licitud del artículo 6 del RGPD los datos de la parte reclamante, ha causado en ésta daños como usurpación de identidad o daño para su reputación. Y todo ello desde que se abrió la cuenta el 16 de agosto de 2021 hasta que se canceló el 31 de marzo 2022.

Hay que resaltar, que Openbank, no verificó la personalidad del que solicitó la apertura de la cuenta bancaría, no tomó las cautelas necesarias para que estos hechos no se produjeran.

En base a lo anteriormente expuesto, en el caso analizado, queda en entredicho la diligencia empleada por Openbank para identificar a la persona que solicitó dicha apertura.

De conformidad con las evidencias de las que se dispone se estima que la conducta de Openbank vulnera el artículo 6.1 del RGPD siendo constitutiva de la infracción tipificada en el artículo 83.5.a) del citado Reglamento 2016/679.

IV
Tipificación y calificación de la infracción

La infracción se tipifica en el artículo 83.5 del RGPD, que considera como tal:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

1. *Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5,6,7 y 9."*

La LOPDGD, a efectos de la prescripción de la infracción, califica en su artículo 72.1 de infracción muy grave, siendo en este caso el plazo de prescripción de tres años, *"b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidos en el artículo 6 del Reglamento (UE) 2016/679"*.

V
Sanción

La determinación de la sanción que procede imponer en el presente caso exige observar las previsiones de los artículos 83.1 y 2 del RGPD, preceptos que, respectivamente, disponen lo siguiente**:**

"1. 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, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. 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). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) 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;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas

previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Dentro de este apartado, la LOPDGDD contempla en su artículo 76, titulado *"Sanciones y medidas correctivas"* lo siguiente:

"*1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.*

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679."

De acuerdo con los preceptos transcritos a efectos de fijar el importe de la sanción de multa a imponer a la entidad reclamada como responsable de una infracción tipificada en el artículo 83.5.a) del RGPD y 72.1 b) de la LOPDGDD, se estiman concurrentes en el presente caso los siguientes factores:

En calidad de agravantes:

- La evidente vinculación entre la actividad empresarial de la reclamada y el tratamiento de datos personales de clientes o de terceros (artículo 83.2.k, del RGPD en relación con el artículo 76.2.b, de la LOPDGDD).

Núm. de interesados afectados: El acuerdo de inicio recoge la reclamación formulada por un reclamante.

La Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), en la que, respecto de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica 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."*

En calidad de atenuantes:

Procedió la parte reclamada a solventar la incidencia objeto de la reclamación de forma efectiva (art. 83.2 c).

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 una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de 200.000 euros (doscientos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a OPEN BANK, S.A. con NIF A28021079.

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 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: CAIXESBBXXX)***, 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 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.

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