- **Expediente Nº: EXP202204227**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 18 de octubre de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202204227

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO:Dª. ***A.A.A.*** (en adelante, la reclamante) con fecha 15 de marzo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.*** con NIF ***A48265169*** (en adelante, el BBVA). Los motivos en que basa la reclamación son los siguientes:

Manifiesta que el Departamento de Testamentarías de la entidad reclamada, en la tramitación de la testamentaría de la madre fallecida de la reclamante, ha facilitado a un tercero, información de siete fondos de inversión de la reclamante, de su exclusiva titularidad, sin que se tratasen de bienes afectos a la herencia.

La información ha sido facilitada, en fecha 27 de agosto de 2020, a través de un mensaje de correo electrónico enviado, desde atencionherederos@bbva.com, dirigido a la dirección de la reclamante y a la de un tercero, remitiendo dicha entidad certificados y estados de posiciones en relación con siete fondos de inversión titularidad exclusiva de la reclamante (correspondientes a su patrimonio), así como la misma información correspondiente a otros tres fondos de inversión titularidad exclusiva de su tío. Manifiesta que el tercero receptor de la información ha estado acosándola, llegando a enviar más de 1425 e-mails, acusándola de robar a su madre fallecida.

A raíz de la vulneración de sus datos, la reclamante interpone numerosas reclamaciones ante la entidad reclamada (la primera de ellas, de fecha 29 de agosto de 2020) recibiendo respuesta de la entidad (en fecha 3 de septiembre de 2020) indicando que "en ningún momento hemos remitido información sobre usted a terceras personas, puesto que no disponemos de ningún tipo de información ni estamos autorizados a facilitarla".

Finalmente, la reclamante presenta reclamación ante el Banco de España y recibe un escrito de la delegada de protección de datos de la entidad reclamada (de fecha 29 de noviembre de 2021) indicando, entre otros, lo siguiente: "Lamentamos profundamente la incidencia ocurrida el pasado 27 de agosto de 2020, donde, de forma totalmente involuntaria, se le adjuntó al correo enviado a D. E.E.E.... como documentos... información sobre varios fondos de inversión de los que usted es la única titular en nuestra entidad, y en los que la Sra. A.A.A.... solo constaba como autorizada". Por otro lado, manifiesta que, en relación con los datos de su tío que también fueron expuestos, la entidad reclamada envió una comunicación a la reclamante y al tercero receptor de la información indicando que esos fondos eran de titularidad exclusiva de su tío y que se habían comunicado por error, instando a que procedieran a destruir dicha información y solicitando que se abstuviesen de utilizarla.

No obstante, la reclamante manifiesta que, en relación con sus datos bancarios que también fueron expuestos, la entidad reclamada no procedió de la misma manera, además de no haber rectificado e informado a dicho tercero del error, indicando que los fondos son de titularidad exclusiva de la reclamante, siendo el origen de sus propios fondos. De hecho, manifiesta que presentó contra el tercero receptor de la información, denuncia por acoso ante el Juzgado y que, en el transcurso de las diligencias seguidas, este ha aportado la documentación bancaria controvertida correspondiente a la reclamante.

Junto a la notificación se aporta copia del mensaje de correo electrónico objeto de controversia y parte de la documentación adjunta, reclamación efectuada al respecto y copia de las respuestas recibidas.

Asimismo, se adjunta pantallazo de uno de los correos electrónicos enviados por el tercero a la reclamante, figurando el número de e-mails recibidos por parte de ese remitente, así como e-mail enviado por la entidad reclamada (en fecha 14 de julio de 2021) solicitando el borrado de la información bancaria recibida (relativa al tío de la reclamante).

D. ***B.B.B.*** (en adelante, el reclamante) con fecha 23 de marzo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF ***A48265169*** (el BBVA). Los motivos en que basa la reclamación son los siguientes:

Manifiesta que el Departamento de Testamentarías de la entidad reclamada, en la tramitación de la testamentaría de la hermana fallecida del reclamante, ha facilitado a dos personas (entre ellas su sobrina y a la vez representante), información de tres fondos de inversión del reclamante, de su exclusiva titularidad, sin que se tratasen de bienes afectos a la herencia.

La información ha sido facilitada, en fecha 27 de agosto de 2020, a través de un mensaje de correo electrónico enviado, desde atencionherederos@bbva.com, dirigido a la dirección de correo electrónico de dos terceras personas (interesadas en el expediente de testamentaría), remitiendo dicha entidad certificados y estados de posiciones en relación con tres fondos de inversión titularidad exclusiva del reclamante (correspondientes a su patrimonio), así como la misma información correspondiente a otros siete fondos de inversión titularidad exclusiva de su sobrina.

A raíz de la vulneración de sus datos, en fecha 29 de agosto de 2020, el reclamante interpone reclamación (a través de su representante) ante la entidad reclamada, recibiendo respuesta, en fecha 3 de septiembre de 2020, en la que dicha entidad niega los hechos, indicando que nunca han remitido información a terceras personas "puesto que no disponemos de ningún tipo de información ni estamos autorizados a facilitarla". No obstante, a raíz de una reclamación efectuada ante la CNMV, la entidad reclamada envía una comunicación (a través del correo electrónico) dirigida a los dos receptores de la información controvertida, en fecha 14 de julio de 2021, indicando lo siguiente: "En relación con los certificados adjuntos al correo electrónico de 27/8/20, como ustedes conocen, por error se adjuntaron dos certificados de fondos de titularidad única de B.B.B.... no tratándose por tanto de fondos de titularidad de la causante del expediente... Lamentamos las molestias que se hayan podido ocasionar y les instamos a que destruyan dicha información y se abstengan de utilizarla".

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 dichas reclamaciones al BBVA, para que procediesen a su análisis e informasen 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.

Los traslados, que se practicaron 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), mediante notificación electrónica, fueron recogidos en fecha 8 de abril de 2022, como consta en los acuses de recibo que obran en el expediente.

Con fecha 24 de mayo de 2022 se recibe en esta Agencia escrito de respuesta indicando que "…La incidencia que ha dado lugar a la solicitud de información a la que se está dando respuesta se debe a que en la tramitación del expediente de testamentaria nº 20027251, correspondiente a la fallecida ***C.C.C.***, la Sra. ***A.A.A.*** reclamante y heredera, solicitó el 28/07/2020 a BBVA un certificado que acreditara donde se encontraba depositado el importe que existía en un fondo de inversión suscrito por la causante en febrero de 1.993.
El departamento de tramitación de testamentarias de BBVA remitió, el día 27/08/2020, los certificados nominativos y estados de posición de 28 fondos de inversión, entre los cuales, por error, se encontraban 9 fondos en los que la causante figuraba exclusivamente como autorizada…
La incidencia que causa la presente reclamación se debe a que la Entidad cometió el error de facilitar al Sr. D.D.D., nieto de la causante y representante de su padre D. ***E.E.E.***, el estado de posición de 9 fondos de inversión donde la causante figuraba como autorizada pero no como titular. De los 9 fondos referidos; 6 son titularidad de la

hija de la causante, Dª***. A.A.A.***, y 3 titularidad del hermano de la causante, D. ***B.B.B.***… En dicho expediente y entre el 26/06/2020 y el 28/03/2022 se han intercambiado, entre BBVA y los herederos, un total de 4.803 correos electrónicos. Tratándose por tanto de un expediente muy voluminoso que ha dado lugar a una equivocación en el envío de una de las múltiples comunicaciones.
Debido a la antigüedad de la información solicitada, traspasos y movimientos de un fondo suscrito en 1993, BBVA realizó una búsqueda a partir del número de DNI de la causante, lo que motivo que por error se facilitaran certificados de todos los fondos en los que figuraba informado su DNI, tanto en su condición de titular como de autorizada. Dicha información se remitió por correo electrónico a la Sra. A.A.A. y a su sobrino el Sr. D.D.D. (representante de su padre D. E.E.E.) …".

TERCERO: Con fecha 15 de junio de 2022 y con fecha 23 de junio de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las reclamaciones presentadas por las partes reclamantes, respectivamente.

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
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el BBVA realiza, entre otros tratamientos, la recogida, conservación, utilización y difusión de los siguientes datos personales de personas físicas clientes de la entidad financiera, tales como: nombre y apellidos, DNI, teléfono, dirección de correo electrónico, dirección postal, datos bancarios y financieros.

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

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse remitido a un tercero por el Departamento de Testamentarías del BBVA, en la tramitación de la testamentaría de la madre fallecida de la reclamante y hermana fallecida del reclamante, información de siete fondos de inversión de la reclamante, de su exclusiva titularidad, sin que se tratasen de bienes afectos a la herencia.

La información se remitió, en fecha 27 de agosto de 2020, a través de un mensaje de correo electrónico enviado, desde atencionherederos@bbva.com, dirigido a la dirección de la reclamante y a la de un tercero, remitiendo dicha entidad certificados y estados de posiciones en relación con siete fondos de inversión titularidad exclusiva de la reclamante (correspondientes a su patrimonio), así como certificados y estados de posiciones en relación con tres fondos de inversión titularidad exclusiva del reclamante (correspondientes a su patrimonio).

Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, consta que los datos personales de las partes reclamantes, obrantes en la base de datos del BBVA, fueron indebidamente difundidos a terceros, vulnerándose el principio de confidencialidad; si bien y según consta en el expediente, el Servicio de Atención a Herederos comunica al tercero, Sr. ***D.D.D.***, a través de su correo electrónico, que la documentación que se le había trasladado el 27/08/2020 ado-

lecía de un error; ya que, se incluía información sobre fondos titularidad de la Sra. ***A.A.A.*** así como información sobre fondos titularidad de D. ***B.B.B.*** y no de la causante de la testamentaría, instándole a no hacer uso de la información y a su destrucción.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable al BBVA, por vulneración del artículo 5.1.f) del RGPD.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 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:

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica"*.

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

V
Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- *b) la intencionalidad o negligencia en la infracción;*

El BBVA informa a esta Agencia de que los hechos relatados se refieren a un error aislado e involuntario no existiendo intencionalidad en la infracción cometida.

En este mismo sentido, 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. **[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)].**

Como atenuantes:

- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

El día 4/04/2022 el Servicio de Atención a Herederos comunica al Sr. ***D.D.D.***, a través de su correo electrónico, que la documentación que se le había trasladado el 27/08/2020 adolecía de un error; ya que, se incluía información sobre fondos titularidad de la Sra***. A.A.A.*** y no de la causante de la testamentaría, instándole a no hacer uso de la información y a su destrucción.

El día 14/07/2021 el Servicio de Atención a Herederos comunica al Sr. D.D.D., a través de su correo electrónico, que la documentación que se le había trasladado el 27/08/2020 adolecía de un error, ya que se incluía información sobre fondos titularidad de D***. B.B.B.*** y no de la causante de la testamentaría, instándole a no hacer uso de la información y a su destrucción.

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

Como agravantes:
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

El Departamento de Testamentaria del BBVA facilita todas las gestiones bancarias necesarias en caso de herencia o fallecimiento.

En consecuencia y a efectos del cumplimiento de los requisitos legalmente establecidos, el ejercicio de dicha actividad implica necesariamente el conocimiento y aplicación de la normativa vigente en materia de protección de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar inicialmente una sanción de 10.000 € (DIEZ MIL EUROS).

VI
Artículo 32 del RGPD

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

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

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

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

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

En el presente caso, en el momento de producirse la brecha de seguridad, no consta que el BBVA dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

El BBVA manifiesta que el incidente pudo ser debido al gran número de correos electrónicos intercambiados en relación con dicho expediente, así como al volumen de este.

"…Debido a la antigüedad de la información solicitada, traspasos y movimientos de un fondo suscrito en 1993, BBVA realizó una búsqueda a partir del número de DNI de la causante, lo que motivo que por error se facilitaran certificados de todos los fondos en los que figuraba informado su DNI, tanto en su condición de titular como de autorizada. Dicha información se remitió por correo electrónico a la Sra. ***A.A.A.*** y a su sobrino el Sr. ***D.D.D.*** (representante de su padre D. ***E.E.E.)***

Si bien, que el incidente fuera debido a un error humano, al volumen del expediente, así como al gran número de correos electrónicos intercambiados con relación a dicho expediente; en ningún caso, justifican la vulneración de la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento…"

Por lo demás, la manera de actuar desde el Departamento de Testamentarias del BBVA comporta un cierto riesgo de que errores como este puedan producirse. La posibilidad de que este tipo de errores se produzcan, como ha acontecido en el supuesto examinado, ha de ser valorado por el responsable del tratamiento, a los efectos de implementar medidas de seguridad técnicas y organizativas para que no se materialicen los riesgos (incluyendo los errores humanos), no constando conforme a las evidencias actuales que existieran medidas adecuadas que hubieran podido evitarlo.

Además, el responsable del tratamiento ha de establecer medidas de seguridad que implementen mecanismos de comunicación seguros con sus clientes cuando remitan por correo electrónico documentación o datos de carácter personal, como podrían ser técnicas tan sencillas como el cifrado, que eviten la pérdida de confidencialidad.

La remisión a la dirección de un correo electrónico de terceros de información bancaria, no distinguiendo entre titularidad y autorización, y no relacionada con el expediente en tramitación, no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento.

Por todo ello, de conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable al BBVA, por vulneración del artículo 32 del RGPD.

VII
Tipificación de la infracción del artículo 32 del RGPD

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

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

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

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica"*.

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

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

(…)

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

VIII

Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- *b) la intencionalidad o negligencia en la infracción;*

El BBVA informa a esta Agencia de que los hechos relatados se refieren a un error aislado e involuntario no existiendo intencionalidad en la infracción cometida.

En este mismo sentido, 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. **[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]**

Como atenuantes:

- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

El día 4/04/2022 el Servicio de Atención a Herederos comunica al Sr. ***D.D.D.***, a través de su correo electrónico, que la documentación que se le había trasladado el 27/08/2020 adolecía de un error; ya que, se incluía información sobre fondos titularidad de la Sra***. A.A.A.*** y no de la causante de la testamentaría, instándole a no hacer uso de la información y a su destrucción.

El día 14/07/2021 el Servicio de Atención a Herederos comunica al Sr. ***D.D.D.***, a través de su correo electrónico, que la documentación que se le había trasladado el 27/08/2020 adolecía de un error, ya que se incluía información sobre fondos titularidad de D***. B.B.B.*** y no de la causante de la testamentaría, instándole a no hacer uso de la información y a su destrucción.

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

Como agravantes:
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

El Departamento de Testamentaria del BBVA facilita todas las gestiones bancarias necesarias en caso de herencia o fallecimiento.

En consecuencia y a efectos del cumplimiento de los requisitos legalmente establecidos, el ejercicio de dicha actividad implica necesariamente el conocimiento y aplicación de la normativa vigente en materia de protección de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar inicialmente una sanción de 6.000 € (SEIS MIL EUROS).

IX

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.***, con NIF ***A48265169***, por la presunta infracción del artículo 5.1 f), tipificada en el 83.5 del RGPD.

INICIAR PROCEDIMIENTO SANCIONADOR a ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.***, con NIF ***A48265169***, por la presunta infracción del artículo 32, tipificada en el 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructor a ***R.R.R.*** y, como secretario, a ***S.S.S.***, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el artículo 64.2 b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), la sanción que pudiera corresponder, sin perjuicio de lo que resulte de la instrucción, sería de:

DIEZ MIL EUROS (10.000€) por presunta infracción del artículo 5.1 f) tipificada en el artículo 83.5 del RGPD.

SEIS MIL EUROS (6.000€) por una presunta infracción del artículo 32 tipificada en el artículo 83.4 del RGPD.

QUINTO: NOTIFICAR el presente acuerdo a ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.***, con NIF ***A48265169***, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 12.800,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 12.800,00 euros y su pago implicará la terminación del procedimiento.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 9.600,00 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (12.800,00 euros o 9.600,00 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ES00 0000 0000 0000 0000 0000 abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-110422

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

>>

SEGUNDO**:** En fecha 26 de octubre de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **9600 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202204227**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***BANCO BILBAO VIZCAYA ARGENTARIA, S.A.***.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

936-040822

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