- **Expediente N.º: PS/00375/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 31 de mayo de 2021 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, la parte reclamada o BBVA). Los motivos en que basa la reclamación son los siguientes:

En fecha 25 de noviembre de 2020, en su condición de abogado de Dña. ***B.B.B.***, presentó en nombre de ésta un escrito de reclamación ante la entidad BBVA. Posteriormente, en fecha 1 de diciembre de 2020, la entidad reclamada entregó en mano a su cliente, Dña. ***B.B.B.***, un escrito relativo a la reclamación dirigido por BBVA a la parte reclamante en el que consta el domicilio particular de ésta, en lugar del correspondiente a su despacho profesional, vulnerando el deber de confidencialidad de datos (la parte reclamante también es cliente de la entidad). La parte reclamante advierte que BBVA ha revelado su domicilio particular, que no era conocido por Dña. ***B.B.B.***, el cual fue facilitado a la entidad por su condición de cliente de la misma, con ocasión de la apertura de una cuenta bancaria. Asimismo, añade que presentó reclamación ante BBVA solicitando una indemnización por estos hechos y recibió respuesta el 31 de diciembre de 2020.

Aporta la reclamación inicial presentada en calidad de abogado, en la que no se indica ninguna dirección postal de contacto, y copia del correo electrónico mediante el que se envía la misma a la entidad reclamada, fechado el 25/11/2020; respuesta de BBVA indicando a la parte reclamante el número de referencia asignado a la reclamación, dirigida a la parte reclamante a su domicilio particular; pantallazo de WhatsApp por el que Dña. ***B.B.B.*** envía dicha respuesta a la parte reclamante; y escrito de BBVA respondiendo a la segunda reclamación efectuada por la incidencia ocurrida con sus datos, en el que la entidad se disculpa e indica que han puesto los hechos en conocimiento de los responsables implicados con el objeto de poder adoptar, en su caso, las medidas que resulten procedentes.

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 22/06/2021 como consta en el acuse de recibo que obra en el expediente.

Con fecha 01/09/2021, se recibe en esta Agencia escrito de respuesta de BBVA indicando que la respuesta emitida por la entidad para acusar recibo de la reclamación presentada por la parte reclamante en nombre de su cliente, en la que no se indicaba ninguna dirección a efectos de comunicación, fue enviada a la única dirección conocida por BBVA, que constaba en la base de datos de clientela.

Además, BBVA manifiesta que el 1 de diciembre de 2020, Dña. ***B.B.B.*** se personó en la oficina de la entidad solicitando conocer el estado su reclamación y copia del expediente. En ese momento, el Director de la oficina entregó a dicha persona una copia del único documento que existía hasta la fecha, correspondiente al acuse de recibo de la reclamación.

Posteriormente, el 3 de diciembre de 2020, la parte reclamante presentó en otra oficina de BBVA un nuevo escrito de reclamación en nombre de su cliente en el que señalaba su dirección profesional como domicilio a efectos de notificaciones.

El 25 de diciembre de 2020, el SAC contestó a la reclamación presentada, enviando dicha contestación a la dirección indicada por la parte reclamante en su escrito de 3 de diciembre de 2020, esto es, su domicilio profesional.

TERCERO: Con fecha 6 de octubre de 2021, 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:

1. La entidad reclamada es una sociedad anónima de nacionalidad española. Según los datos obrantes en “Axesor” se trata de una gran empresa matriz de grupo ***(…)***. No se han encontrado en Sigrid expedientes anteriores al presente en relación con brechas de seguridad de esta entidad.

2. Se solicitó información y documentación a la entidad reclamada y, de la respuesta recibida, se desprende lo siguiente:

a) Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final.

En fecha 1 de diciembre de 2020, una persona clienta de la parte reclamante solicita copia de la reclamación que ésta interpuso en nombre de la misma ante BBVA. La entidad reclamada le entregó en mano a esta persona el escrito relativo a la

reclamación, a nombre de la parte reclamante y en el que consta el domicilio particular de ésta.

BBVA, el 23 de diciembre de 2020, respondió la reclamación de la parte reclamante disculpándose por lo ocurrido, trasladando que dicha incidencia se ha puesto en conocimiento de los responsables implicados que han adoptado medidas para evitar incidentes similares.

Conocida la incidencia por BBVA se han analizado los hechos y constatado que dicha incidencia tuvo lugar por un error puntual, que fue reparado de forma inmediata al informar la parte reclamante de la dirección de su despacho profesional.

El BBVA aclara que facilitar a la persona representada por la parte reclamante el acuse de recibo de la reclamación, sin ocultar la dirección particular de ésta (dirección utilizada por el SAC al no figurar en el escrito la dirección del despacho profesional), fue un error puntual y aislado.

b) Respecto de las causas que hicieron posible la brecha

La persona representada por la parte reclamante solicitó a la oficina de BBVA, el 1 de diciembre de 2020, copia del expediente de la reclamación que había presentado su representante, siendo que en ese momento todavía no se había resuelto la reclamación y solo figuraba el acuse de recibo de la reclamación, este documento le fue entregado por el Director de la oficina en el que se figuraba la dirección del domicilio de la parte reclamante.

c) Respecto de los datos afectados

Los datos afectados fueron la dirección particular del reclamante.

d) Respecto de las medidas de seguridad implantadas

El BBVA defiende que: (i) se trata de un error puntual e involuntario, pues el Director de la oficina desconocía que se trataba de una dirección particular y por lo tanto de un dato personal del representante; (ii) que fue corregido, así se acredita que se adoptaron de manera inmediata medidas para que no se repitiera, empleando mecanismos para revertir la situación y eliminar cualquier riesgo de reincidencia sin especificar ni certificar los mismos.

QUINTO: Con fecha 10/08/2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad BBVA, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por las presuntas infracciones siguientes:

. Infracción del artículo 5.1.b) del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD.

. Infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del mismo Reglamento, y calificada como grave a efectos de prescripción en el artículo 73.f) y g)

de la LOPDGDD.

. Infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD.

En el acuerdo de apertura se determinó que la sanción que pudiera corresponder, atendidas las evidencias existentes en el momento de la apertura y sin perjuicio de lo que resulte de la instrucción, ascendería a un total de 70.000 euros (setenta mil euros): 25.000 euros (veinticinco mil euros) por la presunta infracción del artículo 5.1.b) del RGPD, de 20.000 euros (veinte mil euros) por la presunta infracción del artículo 32 del RGPD y de 25.000 euros (veinticinco mil euros) por la presunta infracción del artículo 5.1.f) del RGPD.

Asimismo, se advertía que las infracciones imputadas, de confirmarse, podrán conllevar la imposición de medidas de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD.

SEXTO: La notificación a la parte reclamada del acuerdo de apertura reseñado en el antecedente anterior, en la que se concedía plazo para formular alegaciones y proponer prueba, se remitió mediante el Servicio de Notificaciones Electrónicas, y fue entregada a BBVA en fecha 11/08/2022.

SÉPTIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la LPACAP y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, las infracciones del RGPD atribuidas a la reclamada y las sanciones que podrían imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

1. La parte reclamante es cliente particular de BBVA, como titular de una cuenta bancaria. Con este motivo, facilitó a la citada entidad sus datos personales, incluido el relativo a la dirección postal correspondiente a su domicilio particular.

2. Con fecha 25/11/2020, en su condición de abogado, la parte reclamante presentó ante BBVA una reclamación en nombre y representación de uno de sus clientes.

3. En la misma fecha del 25/11/2020, BBVA acusó recibo de la reclamación reseñada en el Hecho Probado Segundo mediante escrito dirigido a la parte reclamante y a su domicilio personal, el asociado a su ficha de cliente particular como titular de una cuenta bancaria abierta en este Banco. Mediante este escrito, BBVA comunicó a la parte reclamante el número de referencia asignado a la reclamación.

4. Con fecha 01/12/2020, BBVA facilitó a la persona representada por la parte reclamante el documento de acuse de recibo de la reclamación reseñado en el Hecho Probado Tercero, poniéndole de manifiesto el dato relativo al domicilio personal de la parte reclamante.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

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

En el presente caso se ponen de manifiesto los hechos siguientes, sin que ninguno de ellos resulte controvertido:

La parte reclamante es cliente particular de BBVA, como titular de una cuenta bancaria. Con este motivo, facilitó a la citada entidad sus datos personales, incluido el relativo a la dirección postal correspondiente a su domicilio particular.

En su condición de abogado y actuando en nombre y representación de uno de sus clientes, la parte reclamante presentó ante BBVA una reclamación, de la que esta entidad acusó recibo mediante escrito dirigido a la parte reclamante y a su domicilio personal, el asociado a su ficha de cliente particular como titular de una cuenta bancaria abierta en este Banco.

Además, BBVA facilitó a la persona representada por la parte reclamante este documento de acuse de recibo de la reclamación formulada, poniéndole de manifiesto el dato relativo al domicilio personal de la parte reclamante, que no era conocido por

esta tercera persona.

III

Los hechos expuestos, en relación con la utilización del dato personal de la parte reclamante relativo a su domicilio particular para la tramitación de una reclamación formulada por el mismo en nombre y representación de un tercero, actuando bajo su condición de abogado, sin que exista causa legítima para ello, suponen un incumplimiento del principio de "limitación de la finalidad" regulado en el artículo 5.1.b) del RGPD, que establece lo siguiente:

"1.Los datos personales serán:
(…)
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad").

En relación con los principios regulados en el citado artículo 5 del RGPD se tiene en cuenta lo señalado en el Considerando 39 del citado RGPD:

"39. Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

En el presente caso, BBVA realizó un tratamiento de datos personales de la parte reclamante incompatible con las finalidades que determinaron la recogida de tales datos.
En consecuencia, los citados hechos vulneran lo dispuesto en el artículo 5.1.b) del RGPD, dando lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

IV

El artículo 32 del RGPD, *"Seguridad del tratamiento"*, establece lo siguiente:

"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".

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*.

Hay que señalar que el RGPD no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso

de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

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

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

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

De acuerdo con lo expresado en el Considerando 74 del RGPD, al responsable del tratamiento corresponde poder demostrar que las medidas adoptadas son eficaces:

"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas".

Estas medidas técnicas y organizativas se incluyen como parte del principio de responsabilidad activa, que exige una previa valoración por el responsable el tratamiento del riesgo que pudiera generar el tratamiento de los datos personales, a partir de la cual se adoptarán las medidas que procedan.

Con el RGPD se busca la anticipación a la infracción o lesión de derechos para evitarla. Este enfoque proactivo en la "*implementación permanente"* de las medidas de seguridad implica que las mismas no son estáticas, sino dinámicas, correspondiendo al responsable de tratamiento determinar en cada momento cuáles son las medidas de seguridad necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales y mitigar o eliminar los riesgos para los derechos de las personas. El primer paso es llevar a cabo un *"análisis de riesgos"* para evaluar las amenazas.

Es el responsable o encargado de tratamiento el que deberá acreditar dicha diligencia con un sistema de control interno sólido y eficaz. Por ello, no será suficiente la mera demostración formal de cumplimiento, sino que este principio exige una actitud previa,

consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

La obligatoriedad de estas medidas, o el modo en que se apliquen, dependerá de factores que habrá que tener en cuenta en cada caso, como el tipo de tratamiento y el riesgo que dicho tratamiento implica para los derechos y libertades de los interesados. En consecuencia, la diligencia debida debe adecuarse al nivel de riesgos en la protección de los datos y las características de la organización.

Se puede definir el concepto de diligencia debida como "*la medida de prudencia, actividad o asiduidad que cabe razonablemente esperar, y con la que normalmente actúa, una organización prudente y razonablemente en unas circunstancias determinadas; no se mide por una norma absoluta, sino dependiendo de los hechos relativos del caso en cuestión*". Por ello, la diligencia debida es un proceso en continua observación y prevención de los efectos negativos de las actividades de las entidades sobre la protección de datos.

En el presente caso, tal y como consta en los hechos, la parte reclamada utilizó los datos personales de la parte reclamante registrados en su ficha de cliente particular para la tramitación de una reclamación formulada por esta parte reclamante en nombre de un tercero. Además, facilitó a un tercero el documento de acuse de recibo de dicha reclamación, dándole a conocer el dato personal de la parte reclamante relativo a su domicilio particular.

Este hecho pone de manifiesto que la entidad reclamada no ha adoptado de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de los datos de sus clientes, especialmente las dirigidas a impedir el acceso a la información por terceros no autorizados, como de hecho ocurrió cuando la propia entidad reclamada facilitó al cliente de la parte reclamante el documento de acuse de recibo de la reclamación formulada, dirigido a la parte reclamante y a su domicilio personal.

En consecuencia, los citados hechos vulneran lo dispuesto en el artículo 32 del RGPD, dando lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

V

El ya mencionado artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona, entre ellos, el de *"integridad y confidencialidad"*:

"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").
(…)".

La documentación obrante ofrece indicios suficientes para entender que la entidad reclamada vulneró el artículo 5 del RGPD, que regula el deber de confidencialidad, materializado en la divulgación a terceros de los datos personales de la parte reclamante, en concreto, el relativo a su domicilio particular. Se trata de una difusión de datos personales para la que la parte reclamada no dispone de base jurídica que la legitime.

Este deber de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por sus titulares.

En consecuencia, los citados hechos suponen una vulneración de lo dispuesto en el artículo 5.1 f) del RGPD, que da lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

VI

BBVA, en su respuesta al trámite de traslado de la reclamación, ha manifestado que los hechos constatados tuvieron lugar por un error puntual y aislado, si bien ni siquiera ha explicado en qué ha consistido el error alegado.

A este respecto, es preciso considerar que las incidencias que motivan las actuaciones se producen en el ámbito de responsabilidad de BBVA y esta entidad debe responder por ello. En modo alguno puede considerarse que el error que alega haber cometido excluya su responsabilidad, puesto que, según reiterada jurisprudencia, no puede estimarse la existencia de tal error cuando éste es imputable a quien lo padece o pudo ser evitado con el empleo de una mayor diligencia. En este caso, el supuesto error es incompatible con la diligencia que la parte reclamada viene obligada a observar.

Esta diligencia debe manifestarse en el caso concreto que se analiza, respecto del que se alega el error, y no en circunstancias generales.

En el caso concreto de la parte reclamante, no puede admitirse que la actuación de la entidad reclamada derive de un error. Admitir que no procede exigir responsabilidad a BBVA por los hechos analizados, en base a un supuesto error, sería tanto como admitir que pueda ignorarse la aplicación del RGPD y la LOPDGDD.

A este respecto, debe recordarse que cuando el error es muestra de una falta de diligencia el tipo es aplicable. La Audiencia Nacional en Sentencia de 21 de septiembre de 2004 (RCA 937/2003), se pronuncia en los siguientes términos:

"Además, en cuanto a la aplicación del principio de culpabilidad resulta (siguiendo el criterio de esta Sala en otras Sentencias como la de fecha 21 de enero de 2004 dictada en el recurso 1139/2001) que la comisión de la infracción prevista en el artículo 44.3.d) puede ser tanto dolosa como culposa. Y en este sentido, si el error es muestra de una falta de diligencia, el tipo es aplicable…".

En esta línea cabe citar la SAN de 21 de enero de 2010, en la que la Audiencia expone:

"La recurrente también mantiene que no concurre culpabilidad alguna en su actuación. Es cierto que el principio de culpabilidad impide la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, también es cierto, que la ausencia de intencionalidad resulta secundaria ya que este tipo de infracciones normalmente se cometen por una actuación culposa o negligente, lo que es suficiente para integrar el elemento subjetivo de la culpa. La actuación de XXX es claramente negligente pues… debe conocer… las obligaciones que impone la LOPD a todos aquellos que manejan datos personales de terceros. XXX viene obligada a garantizar el derecho fundamental a la protección de datos personales de sus clientes e hipotéticos clientes con la intensidad que requiere el contenido del propio derecho".

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada o voluntaria, y a este respecto el artículo 28 de la Ley 40/2015 de Régimen Jurídico del Sector Público, bajo la rúbrica "Responsabilidad", dispone lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa".

Los hechos expuestos ponen de manifiesto que BBVA no obró con la diligencia a la que venía obligada, que actuó con falta de diligencia. El Tribunal Supremo (Sentencias de 16 y 22/04/1991) considera que del elemento culpabilista se desprende *"...que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable"*. El mismo Tribunal razona que *"no basta... para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa"* sino que es preciso acreditar *"que se ha empleado la diligencia que era exigible por quien aduce su inexistencia"* (STS 23 de enero de 1998).

Conectada también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la SAN de 17/10/2007 (Rec. 63/2006), que precisó: *"(...) 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"*.

A mayor abundamiento, la Audiencia Nacional, en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."* (SAN 29/06/2001).

VII

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los

siguientes:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
(…)
b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;"
(...)
d) 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;
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;".

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en la letra d) anterior es compatible con la sanción consistente en multa administrativa.

VIII

El incumplimiento de lo establecido en el artículo 5.1.b) y f) del RGPD supone la comisión de sendas infracciones tipificadas en el apartado 5.a) del artículo 83 del RGPD, que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone lo siguiente:

"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:

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

Por otra parte, la vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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 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 de la LOPDGDD indica:

"Artículo 72. Infracciones consideradas muy graves.

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".

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves"*:

"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
g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.
(…)".

En este caso, a tenor de los hechos expuestos, se considera que la sanción que correspondería imponer es de multa administrativa.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones del artículo 83, apartado 2, del RGPD, que señala lo siguiente**:**

"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".

Por su parte, en relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece:

"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".

De acuerdo con los preceptos indicados, a efectos de fijar el importe de las sanciones a imponer en el presente caso, se considera que procede graduarlas de acuerdo con los siguientes criterios que establecen los preceptos transcritos:

En este caso, se estiman concurrentes como agravantes los criterios de graduación siguiente:

. Artículo 83.2.b) del RGPD: *"b) la intencionalidad o negligencia en la infracción"*.

La negligencia apreciada en la comisión de la infracción, considerando que la parte reclamada utilizó los datos personales de la parte reclamante registrados en la entidad en su condición de cliente, sin tener en cuenta que intervenía en los hechos en nombre y representación de un tercero.

A este respecto, se tiene en cuenta lo declarado en Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006) que, partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos, 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".

Se trata de una entidad que realiza tratamientos de datos personales de manera sistemática y continua y que debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos.

Entiende esta Agencia que la diligencia tiene que deducirse de hechos concluyentes, que consten debidamente acreditados y directamente relacionados con los elementos que configuran la infracción, de tal modo que pueda deducirse que la misma se ha producido a pesar de todos los medios dispuestos por el responsable para evitarla. En este caso, la actuación de la parte reclamada no tiene este carácter.

. Artículo 76.2.b) de la LOPDGDD: *"b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales".*

La alta vinculación de la actividad del infractor con la realización de tratamientos de datos personales. Se considera el nivel de implantación de la entidad y la actividad que desarrolla, en la que se ven implicados datos personales de millones de interesados. Esta circunstancia determina un mayor grado de exigencia y profesionalidad y, consiguientemente, de la responsabilidad de la entidad reclamada en relación con el tratamiento de los datos.

. Artículo 83.2.k) del RGPD: *"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".*

. La condición de gran empresa y volumen de negocio de BBVA. Consta en las actuaciones que dicha entidad tiene ***(…).***

Se considera, asimismo, que concurre como atenuante la circunstancia siguiente:

. Artículo 83.2.a) del RGPD: *"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".*

La infracción es una anomalía que afecta únicamente a la parte reclamante.

Considerando los factores expuestos, la valoración que alcanzan las multas por las infracciones imputadas es de 25.000 euros (veinticinco mil euros) para las infracciones muy graves (vulneración de los artículos 5.1.b) y 5.1.f) del RGPD) y de 20.000 euros (veinte mil euros) para la infracción grave (vulneración de lo dispuesto en el artículo 32 del RGPD).

IX

Confirmadas las infracciones, 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…".*

En tal caso, esta Agencia podría requerir al responsable para que adecúe los tratamientos de datos personales que realiza a la normativa de protección de datos conforme a lo indicado en los Fundamentos de Derecho precedentes.

El presente caso afecta únicamente a la parte reclamante y tiene que ver con la utilización y comunicación indebida del dato personal de la parte reclamante relativo a su domicilio personal, con ocasión de una reclamación en la que intervenía bajo la condición de representante de la persona interesada; y la entidad BBVA ha manifestado que esta circunstancia fue posteriormente corregida. Siendo así, no cabe en este caso instar la adopción de medidas por parte del responsable del tratamiento.

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 BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF ***A48265169***, por una infracción del artículo 5.1.b) del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD, una multa de 25.000 euros (veinticinco mil euros).

SEGUNDO: IMPONER a BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF ***A48265169***, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del mismo Reglamento, y calificada como grave a efectos de prescripción en el artículo 73.f) y g) de la LOPDGDD, una multa de 20.000 euros (veinte mil euros).

TERCERO: IMPONER a BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF ***A48265169***, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD, una multa de 25.000 euros (veinticinco mil euros).

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

QUINTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, 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.

938-120722

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