- **Expediente Nº: EXP202213406**

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 5 de mayo de 2023, 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). Notificado el acuerdo de inicio y tras analizar las alegaciones presentadas, con fecha 21 de diciembre de 2023 se emitió la propuesta de resolución que a continuación se transcribe:

<<

**Expediente N.º: EXP202213406**

PROPUESTA DE RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 21/10/2022, tuvo entrada en esta Agencia un escrito presentado por ***A.A.A.*** (en adelante, la parte reclamante), mediante el que formula reclamación contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF A48265169 (en adelante, BBVA), por un posible incumplimiento de lo dispuesto en la normativa de protección de datos de carácter personal.

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante, casada en régimen de separación de bienes, manifiesta que se encuentra en proceso de divorcio. En el transcurso de dicho proceso, la otra parte ha aportado documentación relativa a una "Consulta de Movimientos de Planes de Pensiones" relativo a un producto de su exclusiva titularidad.

A raíz de lo ocurrido, presenta una reclamación ante el Servicio de Atención al Cliente de BBVA y solicita que se le facilite información acerca de la sucursal y el terminal desde el que se efectuó la consulta, así como la identidad de las personas que hayan tenido acceso al mismo y la apertura del correspondiente expediente disciplinario.

En fecha 02/06/2022, recibe respuesta de BBVA indicando lo siguiente: *"Lamentamos las molestias si se le ha trasladado a un tercero información de sus datos personales. En este sentido, tenga la seguridad de que evaluaremos los hechos que nos relata y, a tal efecto, lo hemos puesto en conocimiento de los responsables implicados con el fin de que se adopten las medidas que se estimen oportunas, para corregir situaciones como las que ha tenido a bien trasladarnos"*.

Junto a la reclamación se aporta la siguiente documentación:

- Documento nº 1: copia del Decreto judicial de ******FECHA.1*** por el que se admite la demanda de divorcio por la parte reclamante contra ***B.B.B.***.

- Documento nº 2: copia de la "Consulta de Movimientos Económicos de Planes de Pensiones" expedida por BBVA el 12/05/2021. En el apartado "Titular" figuran el nombre, apellidos y DNI de la parte reclamante.

- Documento nº 3: fotografía de la respuesta de BBVA, de fecha 02/06/2022, a la solicitud de información enviada por la parte reclamante.

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), el 16/12/2022 se dio traslado de dicha reclamación a BBVA, 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 19/12/2022 como consta en el acuse de recibo que obra en el expediente.

TERCERO: Con fecha 21/01/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 24/01/2023, el BBVA solicitó a esta Agencia *"ampliación del plazo de diez días hábiles otorgados para formular alegaciones"*; y, el 30/01/2023, se recibió escrito de BBVA en el que manifestaba lo siguiente:

- BBVA inició las actuaciones pertinentes al objeto de aclarar los hechos objeto de reclamación, comunicándole esta decisión a la parte reclamante mediante carta de 18/01/2023. Tras informar a su departamento de Auditoría Interna de los hechos, este verificó que el extracto de "Consulta de Movimientos Económicos de Planes de Pensiones" fue generado por la oficina de BBVA ***(...)***, sita en ******LOCALIDAD.1***, correspondiéndose con la sucursal donde la parte reclamante contrató el plan de pensiones en cuestión. BBVA señaló que, el empleado no reconoció los hechos y que los empleados de la entidad son conocedores de la normativa interna de Protección de Datos de Carácter Personal, por lo que no existía, a su juicio, ningún indicio o prueba que concluya que BBVA o sus empleados han podido incurrir en algún tipo de cesión no consentida de datos de carácter personal.

- BBVA tenía implementadas diferente normativa interna para garantizar y proteger el tratamiento que realiza de los datos personales de sus clientes.

Junto con el escrito se aporta la siguiente documentación:

- Como Documento nº1: comunicación, de 18/01/2023, que BBVA envió a la parte reclamante.

- Como Documento nº2: copia del "Protocolo de Protección de Datos. Data Protection Office (DPO)".

- Como Documento nº3: copia del boletín de noticias "Hoy", de 12/03/2018, que BBVA envía a sus empleados.

- Como Documento nº4: copia de "Norma de protección de datos de carácter personal. Abril 2022".

QUARTO: De acuerdo con el informe recogido de la herramienta AXESOR, en fecha 12/04/2023, la entidad BBVA es una matriz de grupo constituida en el año 1990. En los apartados "Ventas" y "Total Activo" del "Grupo Económico" constan más de 1.000.000.000€, respectivamente.

QUINTO: Con fecha 05/05/2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a BBVA, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por las presuntas infracciones de los artículos 5.1.f) y 32 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), tipificadas en los artículos 83.5.a) y 83.4.f) del RGPD, respectivamente.

Este acuerdo de inicio, que se notificó conforme a las normas establecidas en la LPACAP mediante notificación electrónica, fue entregado a BBVA el 08/05/2023.

SEXTO: Con fecha 13/06/2023, BBVA presentó escrito ante esta Agencia en el que aduce alegaciones al acuerdo de inicio.

En estas alegaciones, en síntesis, manifestaba que:

- BBVA tenía implementadas medidas de seguridad adecuadas al riesgo. A fin de acreditar esta afirmación, aportó la siguiente documentación:

    - Documento nº 1 "Código de Conducta del Grupo BBVA".
    - Documento nº 2 "Política General de Privacidad y Protección de Datos".
    - Documento nº 3 "Norma corporativa de protección de datos personales".
    - Documento nº 4 "Norma Protección de datos de carácter personal".
    - Documento nº 5 "Norma para la admisión, identificación y conocimiento de los clientes".
    - Documento nº 6 "Política de protección de datos personales derivados de tu relación laboral".

- Documento nº 7 “Boletín diario de información de fecha 12/03/2018”.
- Documento nº 8 “Protocolo de Protección de Datos”.
- Copia de un correo electrónico enviado (***CORREO.1*) el 13/06/2023 a las 13:28 horas, con el título “Información cursos GDPR del colectivo España”.

- Es errónea la interpretación efectuada por esta Agencia en relación con el artículo 32 del RGPD, ya que se trata de una obligación de medios, no de resultado; de acuerdo con la Sentencia del Tribunal Supremo de 15/02/2022 (recurso de casación 7359/2020).

- BBVA adoptó medidas disciplinarias contra el empleado que accedió a los datos personales de la parte reclamante tras haberse producido *“un resultado indeseado”*. Se aporta:

  - Documento nº 10 que certifica la formación recibida por el empleado/a en materia de protección de datos de carácter personal.

- Se ha vulnerado el principio *non bis in idem*, toda vez que la falta de medidas de seguridad constituiría dos infracciones (artículo 5.1.f) y 32 del RGPD) del mismo bien jurídico protegido.

- Y, subsidiariamente, que existe concurrencia de las infracciones del artículo 5.1.f) y 32 del RGPD.

SÉPTIMO: Con fecha 17/11/2023, se remitió copia íntegra de las actuaciones incorporadas al presente procedimiento sancionador y se concedió la ampliación de plazo para formular alegaciones, tras el escrito de 17/05/2023 de BBVA.

OCTAVO: Con fecha 18/12/2023, el órgano instructor del procedimiento acordó la apertura de un período de pruebas, teniéndose por incorporados la reclamación interpuesta por la parte reclamante y su documentación, así como las alegaciones al acuerdo de inicio del presente procedimiento sancionador presentadas por BBVA y la documentación que a ellas acompaña.

NOVENO: Se acompaña como anexo relación de documentos obrantes en el procedimiento.

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

## HECHOS PROBADOS

PRIMERO: En la reclamación de 21/10/2022, la parte reclamante pone de manifiesto que, en el proceso de divorcio contra ***B.B.B.***, este aportó como prueba una “Consulta de Movimientos Económicos de Planes de Pensiones” expedida por BBVA y cuya titularidad pertenece a la parte reclamante.

En el Documento nº 2 que acompaña a la reclamación se observa, entre otros, los siguientes datos:

- Día y hora de expedición: 12/05/2021 a las 09:28 horas.
- Titular: ******NIF.1 A.A.A.***
- Cuenta contrato: ******CUENTA.1***

SEGUNDO: El 02/06/2022, según consta en el Documento nº 3 que acompaña a la reclamación, BBVA envió una carta a la parte reclamante en la que responde a su solicitud de información. El contenido es el siguiente:

*"*****A.A.A.:***
*Hemos recibido el escrito que nos envió con fecha 22 de abril de 2022. Su número de referencia es (....).*
*El objeto de su reclamación, expuesto en su comunicación, es mostrar su disconformidad porque en el transcurso de un procedimiento de liquidación de la sociedad de gananciales, la otra parte presentó documento adjunto junto a su escrito.*
*Manifiesta usted en su escrito que dicho documento se refiere a un producto financiero de su titularidad, del que no ha facilitado su consentimiento, por lo que nos solicita que se facilite distinta información detallada en su escrito sobre el documento objeto de su reclamación.*
*Porque en BBVA nuestro objetivo es la transparencia con nuestros clientes, tras haber revisado cuidadosamente los hechos que usted nos describe, le indicamos que lamentamos las molestias si se la ha trasladado a un tercero información de sus datos personales.*
*En este sentido, tenga la seguridad de que evaluaremos los hechos que nos relata y a tal efecto, lo hemos puesto en conocimiento de los responsables implicados con el fin de que se adopten las medidas que se estimen oportunas, para corregir situaciones como las que ha tenido a bien trasladarnos."*

TERCERO: Según consta en el Documento nº 1 del escrito de fecha 30/01/2023 de contestación al traslado de la reclamación, el 18/01/2023 BBVA envió una comunicación a la parte reclamante con el siguiente contenido:

*"*****A.A.A.:***
*Nos dirigimos a usted con relación al escrito que envió a esta entidad con fecha 19 de diciembre de 2022, a través de la agencia española de Protección de Datos. Su número de referencia es (…).*
*El objeto de su reclamación está relacionado con su reclamación anterior enviada a este servicio, con número de referencia **(....)**, en la que solicitaba información acerca de la persona que había tenido acceso al terminal desde el que, según indica, se había accedido para facilitar información sobre un producto de su titularidad a una tercera persona ajena a usted.*
*Respecto a la cuestión que nos plantea, relativa a la identificación del empleado de la Entidad que haya accedido a sus productos y facilitado información a terceras personales queremos aclararle que el derecho de acceso que reconoce el Reglamento (UE) 2016/679 (…), se circunscribe a los siguientes términos "El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen, y en tal caso, el derecho de acceso*

*a los datos personales, y a la información contenida en el artículo 15 del Reglamento general de protección de datos".*
*Adicionalmente, debemos informarle de que facilitarle la información que nos solicita, supondría la vulneración de datos de carácter personal por parte de esta Entidad.*
*Sin otro particular, reciba un cordial saludo."*

CUARTO: Con fecha 30/01/2023, en contestación al traslado realizado por esta Agencia, desde BBVA se aporta:

1. Protocolo de Protección de Datos. Data Protection Office (DPO) (Documento nº 2), sin fecha y sin firma, enumera una serie de recomendaciones dirigidas a los empleados de la entidad sobre cómo tratar los datos personales de clientes. En concreto, se recogen varios ejemplos reales como el siguiente:

*"Ejemplo: Una persona se presenta en una oficina como familiar de un cliente y solicita información de este cliente con el Banco. El supuesto familiar no es ni cotitular de cuenta corriente, ni prestatario en otras operaciones de financiación del cliente. NO DEBES informar de los datos de tus clientes ni de sus operaciones a terceros."*

1. Boletín de noticias "Hoy" de 12/03/2018 (Documento nº 3) que informa a los empleados de la entidad del protocolo mencionado anteriormente.

2. Norma de protección de datos de carácter personal (Documento nº 4), en cuyo contenido aparece "*aprobada el 01/04/2022*", establece los principios que regirán la protección de tales datos y las responsabilidades de BBVA como responsable de su tratamiento, así como otros aspectos operativos relativos a esta materia.

En el punto 4.1.1 "Responsabilidad proactiva", se señala:

*"Medidas de seguridad*
*En relación con la seguridad de los datos, el Banco, como responsable del tratamiento, está obligado a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad adecuada de los datos de carácter personal y eviten su alteración, pérdida, destrucción, daño accidental tratamiento o acceso no autorizado o ilícito, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que estén expuestos, ya provengan de la acción humana o del medio físico o natural.*
*En cumplimiento de esta obligación, el Banco debe implementar medidas de seguridad adecuadas al nivel de riesgo de cada uno de los tratamientos que se realizan, en base a los estándares más exigentes, desde el diseño de cada iniciativa.*
*Los empleados que accedan a datos personales bajo control del Banco están obligados a respetar todas y cada una de las medidas de seguridad implementadas.*
*Sin perjuicio de la correspondiente normativa operativa que el Banco establezca en cada momento, se recogen a continuación algunos aspectos esenciales sobre la materia:*
*1. Los empleados tendrán acceso autorizado, única y exclusivamente a aquellos datos que precisen para el desarrollo de sus funciones, todo ello de conformidad con la definición del perfil de cada puesto de trabajo.*

*2. Los empleados están obligados a cumplir las normas de seguridad establecidas para los datos personales relacionados con el desarrollo de sus funciones.*
*3. El acceso no autorizado a datos personales por parte de empleados implica una transgresión de las medidas de seguridad y, a su vez, la exposición del Banco a potenciales sanciones.*
*4. Los empleados están obligados a poner en conocimiento del CERT cualquier incidencia que afecte directa o potencialmente a la confidencialidad, integridad o a las políticas y normativas internas que rigen el uso de los datos personales bajo control del BBVA."*

En el punto 4.1.4 "Deber de secreto", se señala:

*"El Banco, como responsable del tratamiento, está obligado a guardar secreto profesional respecto a los datos personales contenidos en los mismos, y a utilizarlos exclusivamente para la realización de las funciones que desempeñe. Dicha obligación perdurará incluso una vez finalizadas las relaciones con el cliente.*
*Por tanto:*
*1. Los datos personales de los clientes no pueden ser comunicados a terceros, ni tampoco las elaboraciones, análisis o procesos similares, ni duplicar o reproducir toda o parte de la información, salvo autorización expresa del titular de estos.*
*2. Debe prestarse especial atención a fin de no entregar ningún documento que contenga datos de carácter personal como pueden ser extractos de cuenta, movimientos, datos económicos, información de tipo laboral, etc. a quienes no sean titulares de los datos y/o del producto bancario específico, incluso siendo familiares o allegados de los mismos, todo ello sin perjuicio de los derechos que puedan tener los descendientes, herederos o personas interesadas en la herencia de titulares bancarios fallecidos lo cual será objeto de análisis en cada caso concreto."*

En el punto 4.1.5. "Comunicación de datos a un tercero", se indica:

*"Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados o cedidos a terceros para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario, con el previo consentimiento expreso del interesado. (…)"*

3. Norma para la admisión, identificación y conocimiento de los clientes (Documento nº 5), aprobada en diciembre de 2022, recoge en el punto 7.6 lo siguiente:

*"La comprobación de la identidad se verificará con carácter previo al establecimiento de la relación de negocios o de la ejecución de operaciones ocasionales, sin perjuicio de que tengan lugar con clientes que no se encuentren físicamente presentes, siempre que concurra alguna de las circunstancias detalladas en el apartado 7.22 y siguientes, sobre Procedimientos de identificación aplicables en los canales web y móvil"*.

QUINTO: Con fecha 13/06/2023, en el escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, BBVA aporta:

1. Código de Conducta del Grupo BBVA (Documento nº 1), en cuyo contenido figura *"aprobado por el Consejo de Administración de BBVA el 09/02/2022*", detalla las pautas de conducta de obligado cumplimiento para todos los empleados del grupo.

En el punto 4.8 "Confidencialidad y protección de datos personales", se señala:

*"4.8.1. En el desarrollo de tu actividad profesional puedes llegar a conocer y tratar datos personales. Recuerda que la protección de los datos personales es un derecho fundamental y debes velar por proteger los datos de nuestros clientes, accionistas, proveedores, compañeros de BBVA y de cualquier otra persona. Si tienes dudas, consulta con el delegado de protección de datos.*

*4.8.2. La información de clientes, empleados o de cualquier tercero a la que hayas accedido por razón de tu actividad profesional es confidencial; mantenla reservada y adopta las medidas necesarias para recabar, almacenar y acceder a esos datos conforme a la normativa aplicable, evitando el acceso indebido y cumpliendo la regulación interna en la materia. 4.8.2 Mantén la confidencialidad y reserva sobre los planes, proyectos y actividades estratégicas del Grupo BBVA, así como sobre cualquier otra información de carácter estrictamente profesional a la que hayas accedido por razón de tu trabajo. Si detectas un acceso inapropiado a la información, sé responsable y comunícalo a la Unidad de Seguridad Corporativa.*

*4.8.3. La obligación de confidencialidad y reserva persiste una vez terminada tu relación con BBVA."*

En el punto 6.4.4 "El Canal de Denuncia", se indica:

*"La Unidad de Cumplimiento tramitará las denuncias recibidas con diligencia y prontitud, promoviendo su comprobación e impulsando las medidas para su resolución, de acuerdo con los procedimientos de gestión del Canal de Denuncia. La información será analizada de manera objetiva, imparcial y confidencial. Se mantendrá reserva sobre quien haya denunciado. La información se pondrá exclusivamente en conocimiento de aquellas áreas cuya colaboración sea necesaria para las actuaciones de comprobación, evitando perjudicar el resultado de la investigación o el buen nombre de las personas a las que afectan. El Grupo BBVA cuenta con mecanismos adecuados a fin de prevenir potenciales conflictos de intereses durante el proceso de investigación de las denuncias. El resultado de las actuaciones de comprobación será comunicado a las áreas que hayan de aplicar las medidas de mitigación o corrección que correspondan, además de al denunciado y al denunciante, cuando proceda."*

1. Política General de Privacidad y Protección de Datos (Documento nº 2), en cuyo contenido aparece *"aprobada por el Consejo de Administración de BBVA el 28/09/2022",* que establece los principios generales y las directrices básicas de gestión y control que habrá de seguir el Grupo en materia de privacidad y protección de los datos de las personas físicas y jurídicas en los procesos y tratamientos de datos que se realicen en el Grupo BBVA, cumpliendo con lo dispuesto en la normativa aplicable.

En el punto 3 “Principios generales, se señala:

*“Principio de confidencialidad: Los datos deberán mantenerse y guardarse de manera que se garantice su confidencialidad. En particular, no se podrá difundir, transmitir o revelar a terceros cualquier información o datos a los que se tenga acceso como consecuencia del desempeño de la actividad, ni utilizar tal información en interés propio, salvo que se cuente con autorización expresa o contractual o la información haya sido solicitada por una autoridad administrativa o judicial. Esta obligación subsistirá aún finalizada la relación contractual.”*

En el punto 5.3 “Modelo de control”, se señala:

*“5.3 Modelo de control*
*El control sobre el grado de cumplimiento tanto de esta Política como de su desarrollo se llevará a cabo de acuerdo con el modelo de control interno establecido en cada momento por el Grupo, dirigido a una adecuada gestión de los riesgos en el mismo, que se articula sobre la base de tres líneas de defensa, independientes entre sí. Las distintas funciones de control cooperarán activa y regularmente en la supervisión de la aplicación de esta Política, de acuerdo con las atribuciones que les hayan sido conferidas. Toda norma y procedimiento relacionado con la privacidad o protección de los datos deberá cumplir con esta Política.”*

2. Norma corporativa de protección de datos personales (Documento nº 3), en cuyo contenido figura *“fecha 19/05/2023*”, que *“supone la derogación de la actual Norma de Protección de Datos de Carácter Personal, vigente hasta el momento para BBVA y sus filiales en la geografía de España”*. En su contenido se detalla las directrices que regirán la protección de los datos de carácter personal, así como las principales responsabilidades de las áreas que intervienen en la protección del dato a lo largo de su ciclo de vida o en los procesos que conllevan tratamiento de datos personales, cumpliendo siempre con lo dispuesto en la normativa aplicable.

En el punto 3.2 “Principio de la Norma”, se señala:

*“Principio de confidencialidad: Los datos deberán mantenerse y guardarse de manera que se garantice su confidencialidad. En particular, no se podrá difundir, transmitir o revelar a terceros cualquier información o datos a los que se tenga acceso como consecuencia del desempeño de la actividad, ni utilizar tal información en interés propio, salvo de conformidad con lo establecido en la regulación aplicable. Esta obligación subsistirá aún finalizada la relación contractual.”*

En el apartado c) del punto 4.5.1 “Privacidad desde el diseño y por defecto”, se indica:

*“Medidas de seguridad*
*La Entidad deberá adoptarlas medidas técnicas, jurídicas y organizativas pertinentes para los datos de carácter personal con objeto de evitar su alteración, pérdida, destrucción, daño accidental, tratamiento o acceso no autorizado o ilícito, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que estén expuestos, ya provengan de la acción humana o del medio físico o natural. En cumplimiento de esta obligación, se deberán implementar las medidas de seguridad*

*adecuadas al nivel de riesgo de cada uno de los tratamientos de datos de carácter personal que se llevan a cabo."*

En el punto 4.5.3 "Deber de secreto", se señala:

*"La Entidad está obligada a guardar secreto profesional respecto de los datos de carácter personal de los que es responsable o encargado, y a utilizarlos exclusivamente para la realización de las funciones que desempeñe. Dicha obligación perdurará incluso una vez finalizadas las relaciones con el interesado."*

3. Norma Protección de datos de carácter personal (Documento nº 4), en cuyo contenido aparece *"fecha 23/03/2023*", que trata sobre los principios que regirán la protección de los datos personales y las responsabilidades de BBVA como responsable de su tratamiento, así como otros aspectos operativos relativos a esta materia.

El contenido del punto 4.1.1 "Responsabilidad proactiva", 4.1.4 "Deber de secreto" y 4.1.5 "Comunicación de datos a un tercero" es idéntico a la versión de 01/04/2022 señalada en el apartado cuarto de Hechos Probados.

4. Norma para la admisión, identificación y conocimiento de los clientes (Documento nº 5), en cuyo contenido aparece *"fecha 02/12/2022"*, recoge la obligación de identificar a los clientes con seguridad, y con carácter previo al establecimiento de la relación de negocios o de la ejecución de operaciones ocasionales.

El contenido del punto 7.6 "Identificación formal de los clientes" es idéntico al señalado en el apartado cuarto de Hechos Probados.

5. Política de protección de datos personales derivados de tu relación laboral (Documento nº 6), en cuyo contenido aparece *"fecha 24/04/2023"*.

6. Boletín diario de información de fecha 12/03/2018 (Documento nº 7) y Protocolo de Protección de Datos, cuyo contenido es idéntico al señalado en el apartado cuarto de Hechos probados.

7. Copia de un correo electrónico enviado (******CORREO.1***) el 13/06/2023 a las 13:28 horas, con el título "Información cursos GDPR del colectivo España", con el siguiente contenido:

*"Buenas tardes:*
*En relación a la empleada* (anonimizado) *según la información obtenida de los informes que nos trasladó Formación España, consta la realización de los siguientes cursos:*
*- GDPR, realizado el 26/11/2018.*
*- Código de Conducta, realizado el 14/11/2022.*
*Por otro lado, os facilitamos los datos de la consecución del colectivo España de los siguientes cursos, obtenido de los informes de la plantilla que nos facilitan Talento y cultura de los de Formación España:*
*Curso GDPR, Datos a 31/05/2023:*

*Total plantilla: 16.453. Formados antes de 2023: 13.758. Formados en 2023: 453. No formados: 2.242.*
*Curso Código de Conducta, datos a 31/05/2023:*
*Total plantilla, 16.543. Formados antes de 2023: 7.560. Formados en 2023: 8.339. No formados: 554."*

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

De acuerdo con los poderes que el artículo 58.2 del RGPD, otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que BBVA realiza la recogida y conservación de, entre otros, los siguientes datos personales de personas físicas: nombre y apellidos, dirección, teléfono, número de cuenta, entre otros.

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 artículo 4.7 del RGPD.

III
Alegaciones aducidas

En relación con las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas.

**1. Sobre la pretendida vulneración por BBVA del artículo 5.1.f) y 32 del RGPD**

Alega BBVA disponer de medidas de seguridad de índole técnica u organizativas apropiadas y adecuadas al riesgo. A fin de acreditar la existencia de tales medidas, aporta la documentación señalada en el apartado quinto de Hechos Probados.

Indica BBVA que esta Agencia realiza una interpretación errónea del RGPD, toda vez que considera que la obligación impuesta por el artículo 32 del RGPD al responsable

de tratamiento es de resultado. Pues, de acuerdo con lo establecido en la Sentencia del Tribunal Supremo de 15/02/2022 (recurso de casación 7359/2020), se trata de una obligación de medios.

Y reconoce BBVA que se ha producido un resultado indeseado como consecuencia de la actuación indebida de uno de sus empleados, el cual tenía acceso a los datos personales de la parte reclamante al prestar servicios en la oficina bancaria donde esta tenía contratado el producto financiero; adoptándose una serie de medidas. No obstante, a juicio del BBVA, el empleado disponía de la información y formación suficiente en materia de protección de datos para entender que su actuación no era adecuada.

Al respecto, esta Agencia desea señalar que los documentos que acompañan al escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador se centran en cuestiones genéricas relacionadas, no solo con la materia de protección de datos de carácter personal, sino también con la conducta y forma de trabajo de los empleados. En ningún caso, se establecen medidas concretas a implementar por BBVA para evitar situaciones parecidas a la cuestión que dio origen al presente procedimiento.

Por otro lado, esta Agencia no considera que la obligación de implementación de medidas de seguridad impuesta por la normativa de protección de datos tenga una naturaleza de obligación de resultado y no de medios

Pero no es menos cierto que BBVA no adoptó medidas apropiadas que *“conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado”*. No puede entenderse que una entidad grande como podría ser BBVA, con un volumen de negocio de miles de millones de euros y que trata continuamente datos de millones de personas, no dispusiera de sistemas o mecanismos suficientes para impedir que uno de sus empleados divulgara información de uno de sus clientes a un tercero no autorizado.

Es más, la actuación del empleado no exime de responsabilidad a BBVA. La responsabilidad de la empresa en el ámbito sancionador por la actuación de un empleado que suponga el incumplimiento de la normativa de protección de datos ha sido confirmada por la jurisprudencia del Tribunal Supremo. A este respecto, cabe indicar que la Sentencia del Tribunal Supremo núm. 188/2022 (Sala de lo Contencioso, Sección 3ª), de 15 de febrero de 2022 (rec. 7359/2020), mencionada por BBVA en su escrito de alegaciones al acuerdo de inicio; señala en su Fundamento de Derecho Cuarto: *“El hecho de que fuese la actuación negligente de una empleada no le exime de su responsabilidad en cuanto encargado de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de registro de datos diseñado. Como ya sostuvimos en la STS nº 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros.”*

Continúa la sentencia argumentando acerca de la de la responsabilidad de las personas jurídicas: *"…Sencillamente sucede que, estando admitida en nuestro Derecho Administrativo la responsabilidad directa de las personas jurídicas, a las que se reconoce, por tanto, capacidad infractora, el elemento subjetivo de la infracción se plasma en estos casos de manera distinta a como sucede respecto de las personas físicas, de manera que, como señala la doctrina constitucional que antes hemos reseñado -SsTC STC 246/1991, de19 de diciembre (F.J. 2) y 129/2003, de 30 de junio (F.J. 8)- la reprochabilidad directa deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma."* (el subrayado es de esta Agencia).

Por todo lo expuesto, se desestima la presente alegación.

**2. Vulneración del principio *non bis in idem***

Indica BBVA que el Acuerdo de Inicio incluye una primera propuesta de sanción por incumplimiento del artículo 5.1.f) del RGPD por la *"ausencia o insuficiencia de esas medidas de seguridad conducen a la apreciación de que mi mandante no ha cumplido los principios de seguridad en el tratamiento de los datos personales* y una segunda propuesta de sanción por incumplimiento del artículo 32 del RGPD porque BBVA *"no ha adoptado las medidas técnicas y organizativas adecuadas en función de los posibles riesgos estimados (además de la información y formación dirigida a sus empleados)"*. Así pues, unos mismos hechos (las insuficientes medidas de seguridad adoptadas por BBVA para tratar datos personales) serían constitutivos de dos infracciones del mismo bien jurídico protegido; concurriendo la triple identidad propia del principio *non bis in idem*.

Al respecto, esta Agencia desea señalar que el artículo 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales, lo que puede producirse, o no, por ausencia o deficiencia de las medidas de seguridad. Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita "mediante la aplicación de medidas técnicas y organizativas apropiadas", que no son estrictamente de seguridad.

Concluye BBVA que las medidas técnicas y organizativas apropiadas a las que hace mención este precepto son las medidas de seguridad del artículo 32 del RGPD. Esto sería simplificar la esencia del RGPD cuyo cumplimiento no se limita a la implantación de medidas técnicas y organizativas de seguridad; significaría, en nuestro caso, reducir la garantía exigida mediante el principio de integridad y confidencialidad a su logro únicamente con medidas de seguridad.

Como hemos señalado anteriormente, cuando el artículo 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD lo hace en el sentido previsto en el artículo 25 del RGPD relativo a la privacidad desde el diseño.

Este precepto determina que,

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

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

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

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo mientras que en el caso del artículo 5.1.f) del RGPD se debe garantizar la confidencialidad e integridad. Como se puede observar los dos artículos persiguen fines distintos, aunque puedan estar relacionados.

Entrando ya de lleno en el examen del *non bis in idem*, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que:

*"(…) Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.*

*Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):*

*a) La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.*

*b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.*

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

Tomando como referencia lo anteriormente explicitado en el procedimiento sancionador no se ha vulnerado el principio *non bis in idem*, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una violación de seguridad de los datos personales, la infracción del artículo 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad, la infracción del artículo 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la violación de seguridad de los datos personales. De hecho, si estas medidas de seguridad que tenía implantadas BBVA se hubieran detectado por esta Agencia sin que se hubiera producido la pérdida de confidencialidad, únicamente habría sido sancionada por el artículo 32 del RGPD.

Y todo ello frente a las alegaciones formuladas por BBVA que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el artículo 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Como hemos indicado, mediante el artículo 5.1.f) del RGPD se sanciona una pérdida de confidencialidad, únicamente, y mediante el artículo 32 del RGPD la ausencia y deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes, añadimos, que infringen el RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad y de disponibilidad.

Por lo que no se considera vulnerado el principio *non bis in idem* en el presente procedimiento sancionador.

**3. Subsidiariamente, existencia de concurso medial entre las dos conductas imputadas a BBVA**

Alega BBVA que el Acuerdo de Inicio identifica una pluralidad de infracciones que, supuestamente, habría cometido la entidad cuando, en realidad, una de ellas se encontraría subsumida en la otra, dando lugar un concurso medial en los términos previstos en el artículo 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Pues, *"la falta de aplicación de medidas que la AEPD considera necesario implementar traería su causa del, a juicio de la AEPD y frente al criterio de mi mandante, inadecuado cumplimiento del principio de seguridad del dato, del que se derivaría la falta de aplicación de dicha medida"* (en adelante, LRJSP).

Al respecto, esta Agencia desea recordar que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuestos por el RGPD.

El RGPD es una norma comunitaria directamente aplicable en los Estados miembros, que contiene un sistema nuevo, cerrado, completo y global destinado a garantizar la protección de datos de carácter personal de manera uniforme en toda la Unión Europea.
En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne

su finalidad última que es la garantía efectiva y real del Derecho Fundamental a la Protección de Datos de Carácter Personal. Lo contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

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

A lo anterior hemos de sumar que el RGPD no permite el desarrollo o la concreción de sus previsiones por los legisladores de los Estados miembros, a salvo de aquello que el propio legislador europeo ha previsto específicamente, delimitándolo de forma muy concreta (por ejemplo, la previsión del artículo 83.7 del RGPD). La LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que este le permite y con el alcance que éste le permite.

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

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

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

Sigue indicando el considerando 13 del RGPD que,

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

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

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

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

Por lo expuesto, y deteniéndose en el presente supuesto, se debe destacar que no hay concurso medial.

El artículo 29.5 de la LRJSP establece que *“Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*” Así pues, el concurso medial tiene lugar cuando en un caso concreto la comisión de una infracción es un medio necesario para cometer otra distinta.

Los hechos constados determinan la comisión de dos infracciones distintas, sin que la falta de aplicación de las medidas a las que se refiere el artículo 32 del RGPD, tal y como asevera BBVA, sea el medio necesario por el que se produce la infracción del 5.1.f) del RGPD.

## IV
## Integridad y confidencialidad

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, con fecha 12/05/2021, un empleado del BBVA emitió una “Consulta de Movimientos Económicos de Planes de Pensiones” relativa a un producto financiero de titularidad privativa de la parte reclamante a favor de su expareja; permitiendo el acceso indebido por un tercero no autorizado a datos personales como

su nombre y apellidos, DNI; y datos financieros como cuenta contrato, tipo y movimientos del plan de pensiones y saldo.

Además, en su escrito de alegaciones al acuerdo de inicio de 13/06/2023, BBVA reconoce que se produjo un *"resultado indeseado y que dicho resultado trae causa en una actuación indebida de un empleado que tenía conocimientos suficientes en materia de protección de datos para entender que ese tratamiento no era adecuado"*.

Atendiendo a lo señalado, BBVA reconoce que la confidencialidad de los datos personales de la parte reclamante vinculados a su Plan de Pensiones se vio afectada, toda vez que se pusieron a disposición de un tercero no autorizado. En este momento, se produjo el acceso indebido.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de propuesta de resolución de 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 a BBVA, por vulneración del artículo 5.1.f) del RGPD.

V

Tipificación y calificación 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 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. (…)"*

VI

Propuesta de 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 propuesta de resolución de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como circunstancias agravantes:

- Toda infracción anterior cometida por el responsable o el encargado del tratamiento (apartado e): en esta Agencia constan dos procedimientos sancionadores (PS/00419/2022 y PS/00429/2022) en los que se adoptaron decisiones de resolución en fecha 28/09/2022 y 11/11/2022. En ambos casos, se le imputa a BBVA la infracción del artículo 5.1.f).

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 circunstancias agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): BBVA es una entidad que realiza tratamientos de datos personales y financieros de manera sistemática y continua y que debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite proponer una sanción de 50.000 euros (cincuenta mil euros).

## VII
## Seguridad del tratamiento

El artículo 32 del RGPD, *"Seguridad del tratamiento",* 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;*

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

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

c) *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 supuesto, en el momento de producirse la violación de seguridad, BBVA no adoptó las medidas de seguridad de índole técnico y organizativo suficientes para impedir que un empleado divulgara información de sus clientes a un tercero no autorizado, exponiendo así los datos personales y financieros de estos.

Si bien es cierto que BBVA disponía de algunas medidas dirigidas a los empleados en relación con la protección de datos personales, como proporcionar información y formación; resulta evidente que son insuficientes las medidas para evitar un incidente parecido a la cuestión que dio origen al presente procedimiento. Además, tampoco es suficiente con que BBVA, como responsable del tratamiento, implante medidas de seguridad, sino que también, debe asegurar su cumplimiento.

Por todo ello, de conformidad con las evidencias de las que se dispone en este momento de propuesta de resolución 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.

## VIII
## 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 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
Propuesta de 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 propuesta de resolución de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como circunstancias agravantes:

- Toda infracción anterior cometida por el responsable o el encargado del tratamiento (apartado e): en esta Agencia constan dos procedimientos sancionadores (PS/00419/2022 y PS/00429/2022) en los que se adoptaron decisiones de resolución en fecha 28/09/2022 y 11/11/2022. En ambos casos, se le imputan a BBVA la infracción del artículo 32 del RGPD.

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 circunstancias agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): BBVA, entidad financiera, y el elevado número de clientes con el que cuenta, conlleva el manejo de un gran número de datos personales. Ello implica que tienen experiencia suficiente y deberían contar con el adecuado conocimiento para el tratamiento de dichos datos.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite proponer una sanción de 20.000 € (veinte mil euros).

IX
Adopción de medidas

De confirmarse la infracción, 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 la resolución que se adopte, se podrá requerir a BBVA para que en el plazo de seis meses notifique a esta Agencia la adopción de las siguientes medidas, sin perjuicio de otras que pudieran derivarse de la instrucción del procedimiento:

- Acreditar en el plazo de seis meses la aplicación efectiva de las medidas de seguridad técnicas y organizativas adecuadas, no solo para cumplir con la normativa, sino para demostrar su cumplimiento antes las autoridades de control e interesados.

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 la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá 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.

A la vista de lo expuesto se procede a emitir la siguiente

PROPUESTA DE RESOLUCIÓN

Que por la Directora de la Agencia Española de Protección de Datos se sancione 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 del RGPD, con multa administrativa de cuantía 50.000€ (cincuenta mil euros).

- Por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, con una multa de 20.000€ (veinte mil euros).

Asimismo, de conformidad con lo establecido en el artículo 85.2 de la LPACAP, se le informa de que podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá una reducción de un 20% del importe de la misma. Con la aplicación de esta reducción, la sanción quedaría establecida en 56.000€ (cincuenta y seis mil euros) y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de

las medidas correspondientes. La efectividad de esta reducción 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 la cantidad especificada anteriormente, de acuerdo con lo previsto en el artículo 85.2 citado, deberá hacerla efectiva mediante su ingreso 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., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa, por pago voluntario, de reducción del importe de la sanción. Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para proceder a cerrar el expediente.

En su virtud se le notifica cuanto antecede, y se le pone de manifiesto el procedimiento a fin de que en el plazo de DIEZ DÍAS pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP.

926-070623

***C.C.C.***
INSPECTOR/INSTRUCTOR

ANEXO

Índice del expediente EXP202213406
21/10/2022 Reclamación de ***A.A.A.***
16/12/2022 Traslado reclamación a BANCO BILBAO VIZCAYA ARGENTARIA, S.A.
21/01/2023 Comunicación a ***A.A.A.***
24/01/2023 Solicitud de ampliación de plazo de BANCO BILBAO VIZCAYA ARGENTARIA SA
30/01/2023 Respuesta requerimiento de BANCO BILBAO VIZCAYA ARGENTARIA SA
05/05/2023 Acuerdo de inicio a BANCO BILBAO VIZCAYA ARGENTARIA, S.A.
08/05/2023 Info. Reclamante a ***A.A.A.***
17/05/2023 Escrito de BANCO BILBAO VIZCAYA ARGENTARIA SA
13/06/2023 Alegaciones de BANCO BILBAO VIZCAYA ARGENTARIA SA
17/11/2023 Escrito 2 a BANCO BILBAO VIZCAYA ARGENTARIA, S.A.

>>

SEGUNDO: En fecha 3 de enero de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **56000 euros** haciendo uso de la reducción prevista en la propuesta de resolución transcrita anteriormente.

TERCERO: El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere la propuesta de resolución.

CUARTO: En fecha 9 de enero de 2024, BBVA presentó escrito de alegaciones a la propuesta de resolución ante esta Agencia.

## 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 **EXP202213406**, 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.

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