- **Expediente Nº: EXP202104875**

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 1 de febrero de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***BANKINTER, S.A.*** (en adelante la parte reclamada). Notificado el acuerdo de inicio y tras analizar las alegaciones presentadas, con fecha 8 de septiembre de 2022 se emitió la propuesta de resolución que a continuación se transcribe:

<<
Expediente nº: EXP202104875

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: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 08/10/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BANKINTER, S.A. con NIF ***A28157360*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: que al acceder a su área personal en la web de la entidad reclamada, en el apartado correspondiente a extracto mensual, no solo figuran los movimientos de su cuenta sino también los movimientos de otra perteneciente a un tercero. Como consecuencia de ello, el 16/07/2021 presenta reclamación ante el Servicio de Atención al Cliente de dicha entidad y recibe respuesta el 22/07/2021, informando del inicio de las actuaciones oportunas sin que haya vuelto a recibir noticias al respecto, además de no haberse subsanado la incidencia.

Aporta impresión del documento *"extracto mensual"* que figura en el área personal del reclamante, correspondiente al mes de junio de 2017, así como e-mail de reclamación y respuesta ofrecida.

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.

No se ha recibido respuesta a este escrito.

TERCERO: Con fecha 29/12/2021 [la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 01/02/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado por la presunta infracción de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del citado Reglamento.

QUINTO: Notificado el acuerdo de inicio el reclamado solicito el 09/02/2022 ampliación del plazo para contestar y el 14/02/2022 copia del expediente; ampliación que fue concedida y copia que le fue trasladada el 11/02/2022 y 14/02/2022 respectivamente.

El reclamado presentó escrito de alegaciones el 25/02/2022 manifestando, en síntesis: que no es cierto como se afirma en el acuerdo de inicio que no respondiera a los requerimientos de la AEPD, puesto que la contestación se produjo el 27/12/2021; que la incidencia fue provocada por un error a la hora de gestionar el cambio de titularidad de la otra cuenta de la que en el pasado fue cotitular, no actualizándose correctamente la información que aparecía en el documento de “extracto mensual” del reclamante, para excluir aquella relativa a la otra cuenta; la ausencia de dolo y culpa en la actuación del reclamado; la inexistencia de infracción del artículo 32.1del RGPD al tener el reclamado implantadas medidas técnicas y organizativas adecuadas; la existencia de concurso medial de infracciones; la desproporción en las sanciones propuestas y la necesaria aplicaciones de atenuantes y la ausencia de agravantes; el archivo del procedimiento y subsidiariamente la minoración de las sanciones propuestas.

SEXTO: Con fecha 29/03/2022, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios las reclamaciones interpuestas por los reclamantes y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que acompaña.

SEPTIMO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes hechos probados:

1. El 08/10/2021 tiene entrada en la AEPD escrito del reclamante manifestando que al acceder a la web de la reclamada, área personal apartado correspondiente a *extracto mensual*, no solo figuran los movimientos de su cuenta sino también los movimientos de otra cuenta perteneciente a un tercero; presentada reclamación ante el Servicio de

Atención al Cliente recibió respuesta informándole del inicio de las actuaciones oportunas, sin que haya vuelto a recibir noticias al respecto, además de no haberse subsanado la incidencia.

2. Consta copia del DNI del reclamante.

3. Consta aportada copia del *extracto integral mensual* de junio de 2021 relativo a los movimientos de la cuenta nº ***CUENTA.1* de la que es titular el reclamante, así como de los movimientos de la cuenta ***CUENTA.2* cuyo titular es una tercera persona.

4. Consta correo electrónico remitido por el reclamante al reclamado de fecha 16/07/2021, en el que se señala lo siguiente:

"En el día de ayer jueves 15 de julio, accedí a mi cuenta personal en la web de Bankinter con el objeto de consultar un pago realizado en el mes pasado. Estaba repasando los movimientos de mi cuenta cuando, cual es mi sorpresa al descubrir que figuran también los movimientos de otra cuenta de la que no soy titular. Esa otra cuenta, según figura. corresponde a una "cuenta corriente oro pensión".
(…)
De conformidad con lo expuesto, solicito procedan a la inmediata corrección de esta situación.
(…)"

5. Consta la respuesta al correo, de fecha 22/07/2021, señalando:

"Estimado cliente:
Pasamos a realizar las gestiones oportunas en base a la situación planteada".

6. El reclamado ha aportado escrito remitido al reclamante de fecha 19/08/2021 en el que se indica lo siguiente:

"En relación a la situación planteada por usted, le informamos de que hemos trasladado sus comentarios a los responsables comerciales de sus cuentas para tratar este asunto.
Agradeciendo como siempre la confianza que ha depositado en Bankinter, seguimos a su disposición a través de Banca Telefónica, en bankinter.com o en cualquier punto de nuestra Red Comercial.
Asimismo, nos consta que han tratado de localizarle varias veces por teléfono sin éxito.
Para cualquier duda en relación con la reclamación, puede llamarnos al Servicio de Atención al Cliente (Telf. 900 802 081), facilitándonos el número de referencia".

7. El reclamado en escrito de fecha 25/02/2022 ha manifestado que: *"En realidad, la situación fue provocada por un error a la hora de gestionar el cambio de titularidad de la Otra Cuenta (tal como el propio Reclamante adelantaba en el Escrito). No se le había retirado completamente el acceso a la información de la Otra Cuenta (de la que él había sido cotitular) al producirse el cambio de titularidad de la misma, en la medida en que no se actualizó correctamente la información que aparecía en el documento de "extracto mensual" del Reclamante, para excluir aquella relativa a la Otra Cuenta".*

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

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

Los hechos denunciados se materializan en la visualización, cuando accede al *extracto mensual* de su cuenta en la web del reclamado, no solo a sus datos personales sino a los datos de una tercera persona (número de cuenta y movimientos de la misma), vulnerándose el deber de confidencialidad motivado por un incidente de seguridad por quebrantamiento de las medidas técnicas y organizativas.

El artículo 58 del RGPD, *Poderes*, señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)
b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
(…)"

En primer lugar, el artículo 5, *Principios relativos al tratamiento*, del RGPD establece que:

"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»).
(…)"

III

1. En primer lugar, el reclamado en escrito 25/02/2022 alegaba que el 27/12/2021, a través de la sede electrónica de la Agencia, dio contestación a los Traslados de Reclamación y Solicitud de Información, tal como se refleja en los en el propio Expediente en el que constan una copia de la respuesta ofrecida y que en el Acuerdo de Inicio, se indica que no ha recibido respuesta a los Traslados de Reclamación y Solicitud de Información.

Obviamente se trata de un error porque el reclamado es cierto que contestó, tal y como consta en el expediente, aunque tal circunstancia en contra de lo alegado por el reclamado no hubiera supuesto la inadmisión de la reclamación ni incumplimiento de las normas que regulan el procedimiento a la luz de la información ofrecida por el mismo.

En segundo lugar, en escrito de 07/04/2022 alegaba que al reclamado no le constaba ningún expediente ni procedimiento con la AEPD que se corresponda con los números de referencia (PS/00634/2021 ni E/12527/2021) y solicitaba se confirmara la existencia de dicho error y, en particular, que la referencia a *"los documentos obtenidos y generados que forman parte del procedimiento E/12527/2021"* también fue errónea, no existiendo otro procedimiento ni documentos de los que Bankinter tenga constancia (de lo contrario, se solicita a la Agencia que proporcione a Bankinter esta información junto con el expediente administrativo completo); y *"se subsane formalmente dicho error, para que tal Acuerdo conste rectificado en el expediente".*

El 07/02/2022 le fue notificado al reclamado Acuerdo de Inicio de Procedimiento Sancionador, figurando en la cabecera del mismo la referencia al Expediente Nº: EXP202104875, es decir, la misma que consta en la Propuesta que se emite y numeración que produce el sistema interno.

Posteriormente el reclamado ha solicitado copia del expediente y habrá podido comprobar que los documentos que integran el expediente administrativo se corresponden con los aportados por el reclamante, los generados por la AEPD y los aportados por el reclamado.

Asimismo, el 29/03/2022 fue notificado la apertura del periodo de pruebas y al contrario que en el anterior escrito figura la referencia al procedimiento sancionador Expediente Nº PS/00634/2021 y en el segundo punto del ACUERDA, se señala exigencia que el propio reclamado indicaba en sus alegaciones al acuerdo de inicio; en cuanto a la referencia a los citados números tanto del procedimiento sancionador como del expediente son cifras que aporta el sistema aplicativo interno y que nada tienen que ver con expedientes distintos (así el número de procedimiento sancionador es un numero de código que aporta el sistema en relación con el expediente procedimental) pero que nada tienen que ver con expedientes o documentos distintos a los que el reclamado tiene en su poder y que forman parte del expediente administrativo, por lo que no existe ningún otro procedimiento ni otros documento de los que Bankinter no tenga constancia.

En resumen, el número de expediente único que aparece en el acuerdo de inicio engloba todos los números internos que identifican los trámites realizados con

anterioridad, que se refieren todos ellos a la misma reclamación; lo que ha podido comprobar al recibir la copia de todo el expediente

2. Como señalábamos en el fundamento anterior el artículo 5, *Principios relativos al tratamiento*, establece en su letra f) lo siguiente:

"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«)

(…)"

Lo que viene a señalar el RGPD es que las medidas técnicas y organizativas que se adopten deben ir orientadas a impedir el acceso o uso no autorizado de dichos datos y del equipo utilizado en el tratamiento.

En ese mismo sentido el Considerando 39 señala que *"…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".*

Se refuerza este principio en el considerando 49 del RGPD, al señalar que el tratamiento de datos personales se realizará *…"en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir, la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos (…)."*

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, *deber de confidencialidad*, al posibilitar la visualización en su extracto mensual bancario, no solo los movimientos propios de su cuenta, sino también los relativos a una tercera persona.

Como así figura en los hechos probados consta aportada copia del extracto integral mensual correspondiente a junio de 2021 en el que figuran los movimientos de la cuenta de la que es titular el reclamante, así como de los movimientos relativos a una segunda cuenta de la que es titular una tercera persona.

El deber de confidencialidad, con anterioridad deber de secreto, ha de entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

El deber de confidencialidad es una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional.

El propio reclamado en su escrito de 07/04/2022 ha manifestado que *"En realidad, la situación fue provocada por un error a la hora de gestionar el cambio de titularidad de la Otra Cuenta (tal como el propio Reclamante adelantaba en el Escrito).*

No se le había retirado completamente el acceso a la información de la Otra Cuenta (de la que él había sido cotitular) al producirse el cambio de titularidad de la misma, en la medida en que no se actualizó correctamente la información que aparecía en el documento de "extracto mensual" del Reclamante, para excluir aquella relativa a la Otra Cuenta" y, además, que *"cuando recibió los Traslados de Reclamación y Solicitud de Información, Bankinter pudo comprender exactamente lo sucedido, deshaciéndose el malentendido anterior y adoptó medidas para solventar la incidencia"* (el subrayado corresponde a la AEPD).

Por tanto, se estima que el reclamado es responsable de la infracción del artículo 5.1.f) del RGPD, infracción tipificada en su artículo 83.5.a) del citado reglamento.

IV

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, *"con multas administrativas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".*

La LOPDGDD en su artículo 72 indica: *"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.
(…)"

V

En segundo lugar, el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

VI

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.
(…)"

Por su parte, la LOPDGDD 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:*

(…)
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".
(…)"

Los hechos puestos de manifiesto en la presente reclamación se materializan además en el quebrantamiento de las medidas técnicas y organizativas vulnerando la confidencialidad de los datos.

VII

1. 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".*

En la documentación aportada al expediente se evidencia que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad al permitir el acceso al reclamante a los datos personales de un tercero, al visualizar en su área personal de la web de la entidad los movimientos de la cuenta de otra persona.

Hay que señalar que el RGPD en el citado precepto 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".

2. En el presente caso, el reclamado ha alegado que ha otorgado una especial relevancia a la protección de la confidencialidad de la información bajo su control, por lo que ha desarrollado códigos, políticas y procedimientos dirigidos a garantizar la protección de dicha información, enumerando a continuación una serie de medidas implantadas sorprendiéndole que la AEPD le impute una infracción del art. 32 RGPD.

No obstante, tal manifestación no puede ser aceptada; parece obvio que dicho incidente se ha producido, es decir, las medidas técnicas y organizativas implantadas fallaron existiendo un incidente de seguridad al permitir la visualización por el reclamante de los movimientos de la cuenta de un tercero en su área personal de la web de la entidad, vulnerando el principio de confidencialidad.

De conformidad con los hechos probados y la documentación que consta en el expediente, el reclamante se dirigió al reclamado remitiéndole e-mail el 16/07/2021, manifestándole que *"En el día de ayer…accedí a mi cuenta personal en la web de Bankinter con el objeto de consultar un pago realizado el mes pasado. Estaba repasando los movimientos de mi cuenta cuando, cual es mi sorpresa al descubrir que figuran también los movimientos de otra cuenta de la que no soy titular. Esa otra cuenta, según figura, corresponde a una cuenta "corriente oro pensión…*

Intuyo que la persona titular de esa cuenta oro pensión es la persona con quien compartir la titularidad de una cuenta nomina donde ingresábamos nuestras correspondientes nominas (mi expareja). Una posible explicación de estos hechos, la más previsible, es que durante las gestiones realizadas en su día por la oficina de Bankinter para que pudiéramos poner fin a la cotitularidad de la cuenta nómina y pasar a tener cada uno su propia cuenta nomina, se produjo algún despiste por parte de la oficina bancaria...

De conformidad con lo expuesto, solicito procedan a la inmediata corrección de esta situación".

Seis días más tarde, el 22/07/2021 el reclamado respondía señalando: *"Pasamos a realizar las gestiones oportunas en base a la situación planteada"*

Pues bien, a pesar de que la situación planteada por el reclamante era meridianamente clara no recibió respuesta alguna, señalando que *"La situación que expuse al banco sigue igual sin que la hayan corregido".*

Respuesta que tampoco difiere mucho de la llevada a cabo el 19/08/2021 por el reclamado al reclamante *"En relación con la situación planteada por usted, le informamos de que hemos trasladado sus comentarios a los responsables comerciales de sus cuentas para tratar este asunto",* y que fue aportada el 27/12/2021 en respuesta al requerimiento informativo de la AEPD al que nos referíamos en el punto 1, del FD III.

Por tanto, el reclamado no puede ampararse en que no fue hasta que recibió los Traslados de Reclamación y Solicitud de Información cuando pudo comprender

exactamente lo sucedido, adoptando medidas para solventar la incidencia porque ya el reclamante en su escrito de reclamación y en los extractos aportados lo dejaba claro: identificaba la clase de cuenta: *"Esa otra cuenta, según figura, corresponde a una cuenta "corriente oro pensión…"* y al titular de la misma *"Intuyo que la persona titular de esa cuenta oro pensión es la persona con quien compartir la titularidad de una cuenta nomina donde ingresábamos nuestras correspondientes nominas (mi expareja)..,".*

El Tribunal Supremo en sentencia de 15/02/2022 señala que: *"La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.*

En las obligaciones de resultado existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad.

En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".

La diferencia radica en la responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

En estas últimas, la suficiencia de las medidas de seguridad que el responsable ha de establecer ha de ponerse en relación con el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados, pero no se garantiza un resultado."

El Tribunal confirma que no resulta suficiente el diseño de los medios técnicos y organizativos necesarios, puesto que también resulta necesaria su correcta implantación y su utilización de forma apropiada.

Por tanto, la responsabilidad del reclamado viene determinada por el incidente de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. Sin embargo, de la documentación aportada se desprende que la entidad no solo ha incumplido esta obligación, sino que además se desconoce la adopción de medidas al respecto, pesar de haberle dado traslado de la reclamación presentada.

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

VIII

Alega el reclamado la existencia de un concurso medial de infracciones por concurrir el supuesto a que se refiere el art. 29.5 de la Ley 40/2015, de 1 de octubre, por lo que procedería la imposición de sólo una de las dos sanciones, en concreto, la referente a la infracción del artículo 5.1.f) de la RGPD.

El art. 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, 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".*

No obstante, tal argumentación no puede ser aceptada; la norma específica en materia de protección de datos, es decir el RGPD, establece en su artículo 83.3 que:

"3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

Ya señalábamos en el FD IV que el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del RGPD se considera como infracción muy grave, por lo que el único límite vendría establecido por el importe señalado en el artículo 83.5 del RGPD *"20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".*

IX

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

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

"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 transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción de multa a imponer en el presente caso por la infracción tipificada en el artículo 83.5.a) y artículo 5.1.f) del RGPD de la que se responsabiliza al reclamado, en una valoración inicial, se estiman concurrentes los siguientes factores:

Son circunstancias agravantes:

- La naturaleza, gravedad y duración de la infracción: los hechos considerados probados afectan gravemente a un principio básico en el tratamiento de los datos de

carácter personal, como es el de confidencialidad e integridad, y cuyo reproche es de mayor gravedad revelando los datos de la cuenta de un tercero, datos de tipo económico; los daños y perjuicios causados como consecuencia de la intromisión en la esfera de privacidad del reclamante pues no hay que olvidar que nos encontramos ante la infracción de un derecho fundamental a la protección de los datos personales y que el reclamante se ha visto obligado a presentar reclamación ante la AGPD ante la inacción del reclamado.

- La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros. En la actividad de la entidad reclamada es imprescindible el tratamiento de datos de carácter personal por lo que, dado el volumen de negocio de la misma la transcendencia de la conducta objeto de la presente reclamación es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

- Aunque no se puede sostener que el reclamado haya actuado intencionadamente, no cabe duda de que se observa una grave falta de diligencia en su actuación. Conectado 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. Si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...) el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto"* (artículo 83.2, b) del RGPD).

- El volumen de negocio del reclamado se trata de una de las entidades financieras líderes dentro del mercado español, por su objeto de negocio (artículo 83.2, k) del RGPD).

Se consideran circunstancias atenuantes:

- Solo se ha visto afectada una persona por la conducta infractora.

Con arreglo a los anteriores factores se estima adecuado imponer al reclamado por vulneración del artículo 5.1.f) del RGPD una sanción de 60.000 euros.

- De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de multa a imponer en el presente caso por la infracción tipificada en el

artículo 83.4.a) y artículo 32.1 del RGPD de la que se responsabiliza al reclamado, en una valoración inicial, se estiman concurrentes los siguientes factores:

Son circunstancias agravantes:

- La naturaleza, gravedad y duración de la infracción: los hechos considerados probados afectan a una cuestión básica en materia de protección de datos como es la seguridad de los mismos, permitiendo el acceso del reclamante a los datos de un tercero, su expareja, como consecuencia del incidente de seguridad y su ausencia de respuesta, en un principio, ante la reclamación interpuesta por el reclamante lo que motivó que tuviera que dirigirse a la AEPD (artículo 83.2, a) del RGPD).

- La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros. En la actividad de la entidad reclamada es imprescindible el tratamiento de datos de carácter personal por lo que, dado el volumen de negocio de la misma la transcendencia de la conducta objeto de la presente reclamación es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

- Aunque no se puede sostener que el reclamado haya actuado intencionadamente, no cabe duda de que se observa una grave falta de diligencia en su actuación. Conectado 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. Si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...) el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto"* (artículo 83.2, b) del RGPD).

- El volumen de negocio del reclamado se trata de una de las entidades financieras líderes dentro del mercado español, por su objeto de negocio (artículo 83.2, k) del RGPD).

Se consideran circunstancias atenuantes:

- Solo se ha visto afectada una persona por la conducta infractora.

Con arreglo a los anteriores factores se estima adecuado imponer al reclamado por vulneración del artículo 32.1 del RGPD una sanción de 40.000 euros.

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

PROPUESTA DE RESOLUCIÓN

PRIMERO. Que por la Directora de la Agencia Española de Protección de Datos se sancione a BANKINTER, S.A., con NIF ***A28157360***, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5, a) del RGPD, con una multa de 60.000 € (sesenta mil euros).

SEGUNDO. Que por la Directora de la Agencia Española de Protección de Datos se sancione a BANKINTER, S.A., con NIF ***A28157360***, por una infracción del artículo 32.1.del RGPD, tipificada en el artículo 83.4, a) del RGPD, con una multa de 40.000 € (cuarenta 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 total quedaría establecida en 80.000 € (ochenta mil euros) y su pago implicará la terminación del procedimiento. 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 ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa, 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.

De conformidad con lo establecido en el artículo 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

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.

R.R.R.
INSPECTOR/INSTRUCTOR

ANEXO

Índice del expediente EXP202104875
08/10/2021 Reclamación de A.A.A.
11/10/2021 Reclamación de A.A.A.
24/11/2021 Traslado reclamación a BANKINTER, S.A.
25/11/2021 Traslado reclamación 2 a BANKINTER, S.A.
27/12/2021 Alegaciones de BANKINTER, S.A.
29/12/2021 Admisión a trámite a A.A.A.
02/02/2022 A. apertura a BANKINTER, S.A.
07/02/2022 Info. Reclamante a A.A.A.
09/02/2022 Solicitud de ampliación de plazo de BANKINTER S.A
09/02/2022 Solicitud de ampliación de plazo de BANKINTER.S. A
11/02/2022 Amp. Plazo a BANKINTER, S.A.
14/02/2022 Solicitud de copia del expediente de BANKINTER.S. A
14/02/2022 Traslado a BANKINTER, S.A.
25/02/2022 Alegaciones de BANKINTER.S. A
29/03/2022 Notificación periodo de pruebas
>>

SEGUNDO: En fecha 22 de septiembre de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **80000 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.

FUNDAMENTOS DE DERECHO

I

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

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 **EXP202104875**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***BANKINTER, 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.

968-230822

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