- **Expediente Nº: PS/00556/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 21 de octubre de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra **WIZINK BANK, S.A.** con NIF A81831067 (en adelante, la parte reclamada).

El motivo en que basa su reclamación es el tratamiento de sus datos personales por parte de la entidad reclamada para la contratación de una tarjeta de crédito, sin su consentimiento.

La reclamante, al pedir una financiación se entera que está incluido en ficheros de solvencia patrimonial por HOIST FINANCE.

La parte reclamante solicita información y le envían una copia del contrato, comprobando que excepto su nombre, apellidos y DNI, los demás datos son falsos (dirección, profesión, hijos, ingresos, mail, teléfono, cuenta bancaria...).

Se adjunta a su escrito de reclamación entre otros documentos denuncia ante la Dirección General de la Policía por posible estafa y suplantación de identidad con fecha de 16 de octubre de 2020.

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.

Con fecha 16 de diciembre de 2020 se recibe en esta Agencia escrito de respuesta de la entidad reclamada afirmando que no tiene ninguna relación contractual con el reclamado y por lo tanto no es responsable del tratamiento de los datos personales del reclamante, fundamentando su afirmación en la cesión de la deuda del reclamante a la entidad HOIST FINANCE, hecho que comunicó al reclamante por escrito al interesado.

Tales hechos quedan constatados mediante copia de la comunicación remitida al reclamante en la que le informan del origen de la deuda, la cesión de ésta en diciembre de 2018 a la entidad HOIST FINANCE.

TERCERO: Con fecha 4 de enero de 2021 la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Solicitada información a WIZINK sobre el procedimiento de la acreditación de identidad en la contratación de las tarjetas de crédito, con fecha de 10 de junio de 2021 se recibe en esta Agencia, escrito de alegaciones informando de que para la contratación de la tarjeta de crédito que nos ocupa, el solicitante eligió el procedimiento online siguiendo el siguiente procedimiento:

Cumplimentación de formulario introduciendo:

- nombre y apellidos, DNI, edad y teléfono.
- Y para continuar con el proceso, el solicitante eligió “COMPLETAR LOS DATOS Y CONTRATAR SIN LLAMADA”

En el siguiente paso, se requirieron los siguientes datos:

- Datos personales y de contacto: fecha de nacimiento, nacionalidad, teléfonos de contacto, dirección postal, dirección de correo electrónico, tipo de vivienda y régimen de tenencia, estado civil y número de hijos.
- Datos bancarios: titular de la cuenta e IBAN.

En el siguiente paso, se requirieron los siguientes datos:

- Datos sobre el empleo: Situación laboral.
- Datos económicos: Ingresos anuales no recurrentes.
- Datos profesionales: Datos de la empresa.

Quedando la solicitud retenida a la espera de su aprobación definitiva, procediendo a la firma y remisión de los documentos necesarios para la contratación.

Para la remisión de la documentación, el solicitante recibió un mail con un enlace, a través del cual el solicitante accedió a una web donde se le guio mediante 5 sencillos pasos, que se detallan a continuación, para completar el procedimiento de firma electrónica avanzada y adjuntar los documentos requeridos (DNI y nómina).

El solicitante envió copia del DNI por ambas caras y copia de su última nómina.

Para el proceso de firma avanzada, categoría de firma empleada según manifestaciones de WIZINK, se valió de un tercero de confianza (LLEIDANETWORKS SERVEIS TELEMATICS, S.A.) que remitió un SMS con un código al número móvil facilitado por el propio solicitante que este tuvo que introducir en el último paso del

proceso de contratación en la web de WIZINK. Adjuntan SMS certificado por ***URL.1*** y certificado de ***URL.1*** de validez de la firma

Posteriormente a este proceso, WIZINK realizó un análisis pormenorizado de la solicitud concluyendo que dicha solicitud debía ser aprobada.

Este análisis se basó prácticamente en el examen de la fotocopia del DNI.

Como la reclamada manifiesta, "*WIZINK es un banco digital que comercializa sus productos a través de medios de comunicación a distancia, y que ha puesto especial énfasis en adoptar las medidas necesarias para cumplir en todo momento con las obligaciones impuestas por la normativa que le es de aplicación a la hora de identificar a sus clientes*. Añaden que el proceso de identificación de los clientes *es resultado de la aplicación de la normativa sobre la Ley de Prevención del Blanqueo de Capitales y la Financiación al terrorismo, Ley 10/2010 de 28 de abril (en adelante, LPBC)".*

Para esta identificación realiza las siguientes actuaciones:

1 Vincular al solicitante de manera única:

WIZINK identificó al Solicitante por medio de un tercero de confianza, ***URL.1***, a través de la firma electrónica avanzada, que permitió cumplir con la obligación de diligencia debida impuesta por la normativa de la LPBC. Además, citan el artículo 12 de la LPBC, y su Reglamento de desarrollo, en su artículo 21, donde se reconoce la firma electrónica como uno de los requisitos válidos y reconocidos para emplear en el proceso de contratación a través de medios telefónicos, electrónicos o telemáticos.

Sostienen que esta interacción con ***URL.1*** permitió que el solicitante quedara identificado de forma unívoca en el inicio del proceso y a medida que avanzaba en el flujo de contratación.

2 Identificar al solicitante, en base a la recogida de una serie de evidencias, como dirección de correo electrónico

3 Facilitar que la firma se realizó por medios que el firmante podía mantener bajo su exclusivo control, su teléfono móvil.

QUINTO: Con fecha 22 de diciembre de 2021**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 6 del RGPD y artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

SEXTO: Notificado el citado acuerdo de inicio, a requerimiento de la entidad reclamada se le da acceso al expediente completo, así como ampliación del plazo para presentar alegaciones.

SEPTIMO: La parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que al datar la solicitud de la tarjeta de septiembre de 2017 y ser la fecha de notificación del acuerdo de inicio de diciembre de 2021, tales hechos se encuentran prescritos.

Además manifiesta que en relación a los requerimientos relativos al incumplimiento de blanqueo de capitales, el reclamado alega que la Agencia Española de Protección de Datos no es competente para observar las vulneraciones que en relación con dicha materia se pudieran llegar a cometer, dado que, estas funciones las tiene asignadas la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, dependiente de la Secretaría de Estado de Economía.

Señala que no es posible determinar que, tanto bajo la plena observancia de la normativa aplicable en el momento en la fecha de solicitud de la tarjeta, así como de la normativa vigente y aplicable en el momento de notificación del presente Acuerdo, haya incurrido en un incumplimiento en relación con las medidas de seguridad aplicadas y esto es derivado de la inexistencia de precepto legal que obligue a la identificación, ya que considera que el RGPD no le es de aplicación, sino la LOPD 15/1999.

OCTAVO: Con fecha 9 de marzo de 2022, se remite propuesta de resolución proponiendo que la Directora de la Agencia Española de Protección de Datos sancione a **WIZINK BANK, S.A.** con NIF A81831067**,** por:

- una infracción del artículo 6 del RGPD tipificada en el artículo 83.5.a) del RGPD y a efectos de prescripción, por el artículo 72.1 b) de la LOPDGDD con una multa de 100.000€ (cien mil euros).

- una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 a) del RGPD y a efectos de prescripción, por el artículo 73 g) de la LOPDGDD con una multa de 50.000€ (cincuenta mil euros).

NOVENO: Con fecha 23 de marzo de 2022, la parte reclamada presenta alegaciones a la propuesta de resolución reiterando las ya presentadas tras el acuerdo de inicio relativas a que los hechos objeto del presente procedimiento sancionador se encuentran prescritos, al datar la solicitud de la tarjeta de septiembre de 2017 y ser la fecha de notificación del acuerdo de inicio de diciembre de 2021.

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

HECHOS PROBADOS

PRIMERO: Se denuncia un tratamiento de datos personales del reclamante por parte de la entidad reclamada, sin su consentimiento.

La reclamante, al pedir una financiación se entera que está incluido en ficheros de solvencia patrimonial por HOIST FINANCE.

A través de dos reclamaciones formuladas a través de la OMIC tiene conocimiento que la deuda fue comprada a WIZINK BANK entidad con la que supuestamente había suscrito un contrato de tarjeta de crédito.

Le envían una copia del contrato y excepto su nombre y apellidos y DNI, los demás son falsos (dirección, profesión, hijos, ingresos, mail, teléfono, cuenta bancaria...), por lo que presenta denuncia ante la policía con fecha de 16 de octubre de 2020.

SEGUNDO: La entidad reclamada alega que los hechos objeto de esta reclamación se encuentran prescritos pues la solicitud de la tarjeta data de septiembre de 2017, y la falta de competencia de este Agencia, como autoridad de control.

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 y 48.1 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 6 del RGPD, establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

Por su parte, el artículo 32 del RGPD establece lo siguiente:

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

***a)** la seudonimización y el cifrado de datos personales;*

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

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

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

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

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

***4.** El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones*

del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

III

En el presente caso, la reclamante denuncia el tratamiento de sus datos personales sin su consentimiento por parte de la entidad reclamada para la contratación de una tarjeta de crédito, lo cual generó la inclusión de sus datos personales en ficheros de solvencia.

En su defensa, dicha entidad indica cual es el procedimiento utilizado para la acreditación de identidad en la contratación de las tarjetas de crédito indicado en el hecho cuarto.

Pese a dicho procedimiento, de las actuaciones de investigación realizadas por esta Agencia, se desprende que dada la existencia de esta reclamación, en la que se han comprobado que la mayoría de los datos aportados por el solicitante no corresponden al titular del DNI, es decir, que el solicitante no es el titular del DIN facilitado, se desprende que la aplicación de la normativa a la que se hace referencia no fue la correcta o no fue aplicada con la exigencia suficiente en base a lo establecido en el artículo 12. Epígrafe 1.a) de la Ley 10/2010, de 28 de abril, de prevención del banqueo de capitales y de la financiación del terrorismo, en adelante LPBC, (texto original publicado el 29 de abril de 2010 vigente en el momento de la contratación), al que se sujeta la reclamada, y que hace referencia al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 (en adelante, Reglamento eIDAS).

Todo ello nos lleva a considerar que no puede presumirse el consentimiento del reclamante en la celebración del contrato, ni la adopción de las medidas de seguridad adecuadas lo cual podría suponer una infracción del artículo 6 y otra del artículo 32 ambos del RGPD.

III

El artículo 72.1 b) de la LOPDGDD señala que *"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:*

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento en el artículo 6 del Reglamento (UE) 2016/679."

A su vez, el artículo 73.g) de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves dispone:

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

IV

Tras un estudio pormenorizado de los documentos obrantes en este procedimiento sancionador, se considera que al ser la fecha de entrada de la reclamación de octubre de 2020 y la fecha de contratación de la tarjeta de crédito, objeto del presente procedimiento sancionador, de septiembre de 2017, estos hechos se encuentran prescritos de conformidad con la legislación vigente, al haber transcurrido más de 3 años.

Por lo tanto, tras tener conocimiento de estos hechos, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al reclamante y reclamado.

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, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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