- Expediente N.º: EXP202203206

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Con fecha 16 de febrero de 2022, se presentó reclamación ante la Agencia Española de Protección de Datos contra el BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF A48265169 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

En fecha 17 de enero de 2022, a través de la banca online de la parte reclamada, un tercero, usurpando la identidad del reclamante realizó varias compras fraudulentas con cargo a su tarjeta de crédito, sin que la parte reclamada hubiese verificado su identidad, además de no haber recibido la reclamante ningún código de seguridad, ni habérsele solicitado ninguna firma digital para ello.

Tras lo ocurrido, en fecha 21 de enero de 2022, la parte reclamante presentó denuncia ante la Policía y, asimismo, presentó escrito de reclamación ante la entidad reclamada.

Documentación relevante aportada por la parte reclamante:

- Email enviado por la parte reclamada desde la dirección ******EMAIL.1*** a la parte reclamante (******EMAIL.2***) en el que se indica que "*se ha iniciado sesión en* ***XXXX*** *desde un nuevo dispositivo*". En el cuerpo del mensaje, se señala que el dispositivo móvil es un Alcatel 1SE el día 17/01/2022 a las 20:14h (hora peninsular). Este email lo reconoce como enviado la parte reclamada y ha aportado la acreditación documental correspondiente.

- Email donde se indica "*Hemos detectado una actividad sospechosa reciente y por tu seguridad, se ha bloqueado de forma temporal tu usuario de acceso a tu banca digital*". Aunque en el pantallazo aportado por la parte reclamante no figura ni la dirección del remitente, ni la del destinatario, ni la fecha, ni la hora de recepción del mismo, la parte reclamada reconoce haber envido este email y ha aportado la acreditación documental correspondiente.

- Email donde se indica que se ha inhabilitado la tarjeta a través de la que se han realizado las operaciones reclamadas por motivos de seguridad. En el cuerpo del mensaje se indica

  "*Tarjeta inhabilitada provisionalmente.*

  Hola ***A.A.A.***, *En* ***XXXX*** *hemos detectado un movimiento sospechoso en tu tarjeta terminada en *1519* y, para garantizar tu seguridad e impedir que pueda ser utilizada, hemos suspendido provisionalmente su uso*".

Asimismo, se adjunta imagen de una tarjeta donde sólo se puede observar el número de dicha tarjeta (***TARJETA.1**), la fecha de validez 12/20 y el titular **B.B.B.**.

En el pantallazo aportado por la parte reclamante no figura ni la dirección de correo electrónico del remitente ni la del destinatario, tampoco la fecha ni la hora. Por otro lado, la parte reclamada, como veremos también más adelante, señala que se podría tratar de *phishing*.

- Fotografías del terminal móvil de la parte reclamante donde se observa la marca HUAWEI y el modelo (P20 Lite) con el objetivo de señalar que se trata de un dispositivo móvil distinto al utilizado para llevar a cabo las operaciones reclamadas (como se verá más adelante, un móvil modelo Alcatel 1SE).

- Dos denuncias presentadas por la parte reclamante ante la Dirección General de la Policía (en adelante, DGP).

La primera denuncia se presentó el día 21 de enero de 2022 donde, entre otros, se indica:

*"Que es cliente de la entidad bancaria **XXXX**, en la que es titular de una tarjeta de crédito número *****TARJETA.2**, asociada a la cuenta corriente número *****CUENTA.1**.*

Que, en la fecha arriba indicada, persona/s desconocida/s han realizado sin su consentimiento una serie de seis operaciones con cargo a la tarjeta anteriormente reseñada, por un VALOR TOTAL de 2880 euros, por lo que como quiera que no ha llevado a cabo estas operaciones, ni ha autorizado a nadie para hacerlas y por lo tanto, no reconoce como propias, entiende que son operaciones fraudulentas.

*Que dichas seis operaciones se realizaron todas el día 17/01/2022 con concepto "Revolut**2732*LITUANIA", en la localidad "***LOCALIDAD.1" siendo el importe de cada una de 480 euros.*

Que NO ha procedido todavía a la cancelación de la tarjeta.

Que nunca ha extraviado o perdido la mencionada tarjeta y siempre la ha tenido consigo.

Que en este acto hace entrega a esta Instrucción de un certificado bancario en el que se reflejan los movimientos no autorizados, por lo que se adjunta a la presente."

La segunda denuncia se presentó el día 1 de febrero de 2022 donde, entre otros, se indica:

*"Que las presentes son ampliatorias al Atestado ***ATESTADO.1 de fecha 21 de enero de 2022 de la Comisaría de Distrito de Madrid-Arganzuela, donde denunciada un fraude informático.*

Que quiere dejar constancia de que el número correcto de tarjeta es ******TARJETA.3****, de la entidad bancaria* ***XXXX****.*

Que así mismo manifiesta que no ha consentido en ningún momento dichos cargos y desconoce su procedencia, no habiéndolos autorizado en ningún momento, ni habiendo recibido ningún mensaje por parte del banco para poder autorizarlos, como acostumbran a hacer para verificar la identidad del titular de la tarjeta en cada compra."

- Por último, se adjunta un certificado sellado por una sucursal de la parte reclamada donde se observan seis cargos realizados por importe de 480 euros cada uno de ellos en la tarjeta terminada en 1519 el día 17/01/2022.

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/ALIAS, 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 17 de marzo de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 26 de abril de 2022 se recibe en esta Agencia escrito de respuesta indicando, en síntesis, que se informó a la reclamante que se han abonado en la cuenta de su titularidad las cantidades reclamadas por un importe total de 2.880 €.

XXXX envío diferentes alertas de la operativa que se estaba llevando a cabo desde su usuario tanto a través de e-mail y SMS, y además procedió al bloqueo del usuario y de tarjetas de manera preventiva.

TERCERO: Con fecha 3 de mayo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

El día 17 de mayo de 2022, se envió un requerimiento de información a VODAFONE ESPAÑA S.A.U., (en adelante, VODAFONE).

En este requerimiento de información, se solicitaba a VODAFONE copia de las solicitudes de duplicado de tarjeta SIM correspondientes al número de teléfono móvil de la parte reclamante (******TELÉFONO.1***) realizadas durante el mes de enero de 2022,

mes en el que se produjeron los hechos reclamados, por si las operaciones reclamadas se hubieran podido realizar a través de una SIM duplicada correspondiente al número de teléfono de la parte reclamante.

La contestación de ***V***ODAFONE fue la siguiente:

"Incluyendo los movimientos historificados, no tiene ningún cambio de sim. No hay ninguna orden de trabajo, ni anulada, ni tramitada para cambio de sim, ni en 2022, ni en todos los movimientos de la clienta".

También el día 17 de mayo de 2022, se envió un requerimiento de información a la parte reclamada. En este requerimiento se solicitaba a la parte reclamada la siguiente información:

1. Copia de logs registrados en sus sistemas relativos a acciones realizadas por la parte reclamante en los datos de su perfil de cliente una semana antes y después del día de los hechos. En concreto, los que tengan que ver con cambios de contraseña, número de móvil de contacto, dirección de correo electrónico, acceso biométrico y otros que hubiera realizado la parte reclamante durante ese tiempo.

En la contestación a este punto, la parte reclamada hace referencia a un pantallazo de sus sistemas donde figuran los datos de contacto de la parte reclamante, en concreto, su número de teléfono móvil (******TELÉFONO.1***), mismo que el número indicado por ésta en su denuncia ante la DGP, y dirección de correo electrónico (******EMAIL.2***), donde no figura ningún cambio realizado entre los días 10/01/2022 y 24/01/2022.

2. Copia del procedimiento establecido para operaciones y acciones llevadas a cabo por los clientes en la banca online, indicando en qué casos se requiere doble factor de autentificación y cómo aplica en cada una de las operaciones llevadas a cabo por la parte reclamante una semana antes y después del día de los hechos.

Sobre este punto, la parte reclamada indica lo siguiente:

"La autenticación reforzada del cliente, conocida como SCA (Strong Customer Authentication), procedimiento para comprobar la autenticidad de los clientes mediante el uso de 2 factores que pertenezcan a alguna de las siguientes categorías:

Algo que solo el cliente sabe, por ejemplo, la contraseña.
Algo que solo el cliente tiene, por ejemplo, su teléfono móvil.
Algo que solo el cliente es, por ejemplo, su huella dactilar.

Este procedimiento de doble autentificación es obligatorio cada vez que el cliente:

- *Acceda a sus cuentas online (tanto por web como por app).*
- *Inicie transacciones de pago electrónicas (una transferencia, un pago en comercio online, etc).*

- *Y/o realice alguna acción a través de canales remotos que puedan suponer un riesgo de fraude.*

Existen casos en los que no será necesario aplicar SCA, por ejemplo, si se trata de pagos con tarjeta regalo o si las compras son de baja cuantía."

1. Copia de todas las comunicaciones (emails, SMS, notificaciones push, etc.) mantenidas con la parte reclamante una semana antes y después del día de los hechos, donde se pueda verificar, entre otros, los datos del remitente, destinatario, contenido de la comunicación, fecha y hora.

En relación a este punto, la parte reclamada contesta haciendo referencia a tres documentos que adjunta en su contestación, pantallazos de los sistemas de la parte reclamada con las comunicaciones enviadas a la parte reclamante, documento titulado "*GF-11312 Análisis de evidencias de operaciones en Banca a Distancia*" fechado el día 19 de mayo de 2022 y la traza de operaciones bancarias realizadas por la parte reclamante desde el día 10 de enero de 2022 hasta el 24 de enero de 2022.

Sobre los pantallazos de las comunicaciones, figura un correo electrónico enviado a la dirección de correo electrónico de la parte reclamante (******EMAIL.2***) el día 17 de enero de 2022 a las 20:14h y un mensaje PUSH-MOOM a la aplicación móvil de la parte reclamante, alertando de que se había accedido a la aplicación móvil desde un dispositivo móvil distinto al habitual. En este sentido, hay que indicar que la parte reclamada adjunta pantallazo de sus sistemas de comunicaciones con información del correo electrónico donde se observa lo siguiente:

"*Dispositivo: Alcatel 1SE*

Fecha y hora: 17/01/2022 20:14 (Hora peninsular)

Si has sido tú, puedes ignorar este mensaje. Si no has sido tú y crees que alguien puede haber accedido a tu cuenta, te recomendamos que, por precaución, cambies tu clave de acceso de la web o app ***XXXX***"

Respecto al mensaje PUSH_MOOM, en el mismo se indica lo siguiente:

Nuevo inicio de sesión. Se ha iniciado sesión en tu cuenta ***XXXX*** *desde un nuevo dispositivo, ¿has sido tú? […]*".

Una comunicación se envió a la dirección de correo electrónico de la parte reclamante (******EMAIL.2***) el día 17 de enero de 2022 a las 20:26:46 correspondiente a la modificación del límite de la tarjeta de crédito. En la contestación dada por la parte reclamada al traslado de la reclamación (Anexo 4), ésta indica que se incrementó el límite de la tarjeta terminada en 1519 de 1.000 euros a 5.000 euros.

Otra comunicación, mediante mensaje PUSH-MOOM enviado a la aplicación móvil de la parte reclamante el día 17 de enero de 2022 a las 20:22:43, fue la relativa a una compra denegada donde se indica:

"*Has iniciado una compra en **revolut****LOCALIDAD.1 con tu tarjeta terminada en 1519 que no se ha completado. Nos gustaría que respondieras a unas preguntas para que podamos mejorar tu experiencia y ofrecerte un mejor servicio, ¿nos ayudas?*".

Otra de las comunicaciones enviadas a la dirección de correo electrónico de la parte reclamante (***EMAIL.2**) es la información contractual relativa a la contratación de dos tarjetas con número de contrato ***CONTRATO.1** y ***CONTRATO.2**. En este sentido, hay que indicar que la parte reclamada adjunta pantallazos de sus sistemas de comunicaciones con información de los correos electrónicos enviados a la parte reclamante el día 17 de enero de 2022 a las 20:26:42 y 20:37:41.

La última notificación enviada por la parte reclamada mediante correo electrónico y mensaje PUSH-MOOM a la parte reclamante fue la relativa al bloqueo del usuario multicanal. La parte reclamada adjunta pantallazo de sus sistemas donde se observa el siguiente texto:

"*A pesar de que tu acceso a la App, al área privada de XXXX.es y a operar con tus claves en los cajeros no es posible actualmente, podrás seguir utilizando tu/s tarjeta/s tanto en nuestros cajeros, como en compras online o físicas.*

*Para la reactivación de tu usuario necesitamos identificarte, por lo que es necesario que acudas a cualquier oficina de **XXXX** con tu DNI/pasaporte u otro documento identificativo o contactando con Línea **XXXX** a través del número de teléfono ***TELÉFONO.2**.*".

La parte reclamada también adjunta a la contestación un informe de trazabilidad, documento titulado "GF-11312 Análisis de evidencias de operaciones en Banca a Distancia" fechado el día 19 de mayo de 2022, sobre las operaciones bancarias realizadas por la parte reclamante. Según se indica en este informe, existe la siguiente tipología de transacciones u operaciones:

- *getCardSecurityData*: Servicio que obtiene los datos seguros de una tarjeta a partir del identificador de ésta. Estos datos son: el nombre impreso, la fecha de caducidad y el código de seguridad de una tarjeta (CVV).

- *createTransfers*: Servicio que permite ejecutar transferencias tanto nacionales como internacionales.

- *finalizeDeviceBiometricEnrollm*: Servicio que permite al usuario finalizar el registro en FIDO[1].

- *certifyCard*: Servicio que realizará la firma y la puesta en vigor (si procede) de un contrato de una tarjeta con evidencias digitales en Backend de Firma y Riesgo para uno o varios titulares.

- *modifyCardLimits*: Servicio de modificación de límites de una tarjeta.

1

- *modifyCustomerOperative*: Servicio que permite realizar la modificación del bloqueo de cliente y el tipo de operativa de pre-activado a operativo.

Nada se dice sobre las transacciones del tipo *solicitarTicketConsumoAPI.* En contestación a un posterior requerimiento de información (tercero), la parte reclamada señala que este tipo de transacciones se corresponden con el acceso a la app/web de la parte reclamada.

Tampoco se indica nada sobre las transacciones de tipo *createCardV2*. En este sentido, también como parte de la contestación a un requerimiento de información posterior (tercero), la parte reclamada señala que este tipo de transacciones se corresponde con el proceso del alta de una tarjeta, proceso que finaliza mediante la transacción *certifyCard*, transacción que se ha descrito anteriormente.

En cuanto a los medios de autenticación, en dicho informe se hace referencia a dos:

- 02 (Autenticación con usuario y password personales).

- 119 (MA/CE FIDOTransparente). FIDO almacena información de identificación personal, como datos de autenticación biométrica.

Por último, la parte reclamada adjunta un listado con la traza de operaciones bancarias realizadas el día de los hechos (17 de enero de 2022) por el usuario ******USUARIO.1***, usuario correspondiente a la parte reclamante, a través de la Banca Móvil Android (acceso a la Banca a Distancia a través de la aplicación móvil para dispositivos Android).

El día de los hechos, entre otras, varias operaciones fueron realizadas desde la dirección IP ******IP.1*** mediante un dispositivo móvil Alcatel 1SE, dispositivo distinto al indicado por la parte reclamante. Por otro lado, ese mismo día hay una operación realizada desde la IP ******IP.2*** mediante un dispositivo móvil Huawei P20 Lite (dispositivo de la parte reclamante, según indicó la propia parte reclamante en su reclamación presentada en esta Agencia en la que adjuntó fotografía de su propio dispositivo móvil).

A continuación, se analiza el listado de transacciones remitido a esta Agencia por la parte reclamada, donde se puede observar la fecha y hora, el tipo de transacción, el medio de autenticación (FIDO o autenticación mediante usuario y password personales) y el tipo de firma empleado para su validación (password personales, autenticación mediante OTP/SMS, no aplica):

Transacción de acceso a la app/web (*solicitarTicketConsumoAPI*) autentificada mediante usuario y contraseña personales realizada desde la dirección IP ******IP.1*** a través de un dispositivo móvil Alcatel 1SE (dispositivo distinto al de la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:14:35 GMT+1	solicitarTicketConsumoAPI	02 (Autenticación con usuario y password personales)	No aplica

Transacción *EAHDT00201ES* realizada desde la dirección IP ******IP.3***:

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:14:36 GMT+1	EAHDT00201ES	-	-

En contestación al tercer requerimiento de información realizado a la parte reclamada, ésta aclara que esta transacción genera un evento que se corresponde con la notificación de seguridad que fue enviada a la parte reclamante, a modo informativo, alertando que se había accedido desde un dispositivo móvil distinto del habitual.

Transacción de activación de acceso biométrico (*finalizeDeviceBiometricEnrollm*) autentificada mediante usuario y contraseña personales realizada desde la dirección IP ******IP.1*** a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:15:33 GMT+1	finalizeDeviceBiometricEnro-llm	02 (Autenticación con usuario y password personales)	Autenticación mediante OTP/SMS

Según acredita la parte reclamada mediante pantallazo de sus sistemas, para la activación del acceso biométrico se envió un mensaje SMS con clave OTP (*One Time Password*) al número de teléfono ******TELÉFONO.1*** (mismo número de teléfono que indica la parte reclamante en su denuncia ante la DGP). En dicho mensaje si indica lo siguiente:

"*La clave para activar tu acceso biométrico es XXXXXX. Si no lo has solicitado tú, llama ahora al* ******TELÉFONO.3***"

Una vez se activó el acceso biométrico, el resto de transacciones reclamadas que se realizaron el día de los hechos se autentificaron biométricamente mediante FIDO.

Transacción de acceso a la app/web (*solicitarTicketConsumoAPI*) autentificada mediante FIDO y realizada desde la dirección IP ******IP.1*** a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:15:48 GMT+1	solicitarTicketConsumoAPI	119 (MA/CE FIDOTransparente)	No aplica

Transacciones (*getCardSecurityData*) autentificadas mediante FIDO con las que se obtienen los datos seguros de una tarjeta a partir del identificador de ésta (nombre impreso, fecha de caducidad y el código de seguridad de una tarjeta, CVV) realizadas desde la dirección IP ******IP.1***a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:16:19	getCardSecurityData	119 (MA/CE FIDOTransparente)	Password personales

GMT+1			
20:17:52 GMT+1	getCardSecurityData	119 (MA/CE FIDOTransparente)	Password personales
20:27:38 GMT+1	getCardSecurityData	119 (MA/CE FIDOTransparente)	Password personales
20:32:45 GMT+1	getCardSecurityData	119 (MA/CE FIDOTransparente)	Password personales
20:36:01 GMT+1	getCardSecurityData	119 (MA/CE FIDOTransparente)	Password personales

Transacción de acceso a la app/web (*solicitarTicketConsumoAPI*) autentificada mediante usuario y contraseña personales realizada desde la dirección IP ******IP.2*** a través de un dispositivo móvil Huawei P20 Lite (marca y modelo del dispositivo de la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:19:26 GMT+1	solicitarTicketConsumoAPI	02 (Autenticación con usuario y password personales)	No aplica

Transacción de modificación de límites de una tarjeta (*modifyCardLimits*) autentificada mediante FIDO y realizada desde la dirección IP ******IP.1*** a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:21:37 GMT+1	modifyCardLimits	119 (MA/CE FIDOTransparente)	Password personales

Transacciones de acceso a la app/web (*solicitarTicketConsumoAPI*) autentificadas mediante FIDO y realizadas desde la dirección IP ******IP.1***a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante):

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:22:54 GMT+1	solicitarTicketConsumoAPI	119 (MA/CE FIDOTransparente)	No aplica
20:23:49 GMT+1	solicitarTicketConsumoAPI	119 (MA/CE FIDOTransparente)	No aplica
20:24:45 GMT+1	solicitarTicketConsumoAPI	119 (MA/CE FIDOTransparente)	No aplica
20:25:15 GMT+1	solicitarTicketConsumoAPI	119 (MA/CE FIDOTransparente)	No aplica

Transacciones (*createCardV2* y *certifyCard*) autentificadas mediante FIDO con las que se lleva a cabo la contratación de una tarjeta bancaria. Estas operaciones fueron realizadas desde la dirección IP ******IP.1*** a través de un dispositivo móvil Alcatel 1SE (distinto al correspondiente a la parte reclamante). Estas transacciones se corresponden con la contratación de las tarjetas con número de contrato ******CONTRATO.1*** y ******CONTRATO.2***:

GMT	Tipo de transacción	Medio de autenticación	Tipo de firma
20:26:37 GMT+1	createCardV2	119 (MA/CE FIDOTransparente)	Password personales
20:27:01 GMT+1	certifyCard	119 (MA/CE FIDOTransparente)	Password personales
20:37:35 GMT+1	createCardV2	119 (MA/CE FIDOTransparente)	Password personales
20:38:13 GMT+1	certifyCard	119 (MA/CE FIDOTransparente)	Password personales

El día 15 de junio de 2022, se envió un segundo requerimiento de información a la parte reclamada. Además, el día 5 de julio de 2022 se recibió otra entrada en esta Agencia relativo a este requerimiento de información, que contenía una carta dirigida a esta Agencia por parte del Servicio de Atención al Cliente de la parte reclamada. En esta carta, se indica lo siguiente:

"*Hemos recibido el escrito que nos ha enviado, trasladándonos algunos aspectos de la relación de D/Dª.* ***A.A.A.*** *con la entidad.*

La solicitud se está gestionando con el número de referencia 9071865, indicando este número podrá realizar cualquier consulta al respecto.

[…]"

En este segundo requerimiento se solicitaba la siguiente información:

- Especificación del procedimiento establecido para obtener la aceptación por la parte reclamante de las siguientes operaciones:

Activación del acceso biométrico FIDO (transacción *finalizeDeviceBiometricEnrollm* correspondiente al día 17/01/2022).

Operaciones de acceso a los datos seguros de las tarjetas (transacciones *getCardSecurityData* correspondientes a los días 10/01/2022 y 17/01/2022).

Cargos realizados en las tarjetas (transacciones *solicitarTicketConsumoAPI*), con especial detalle de las operaciones correspondientes a los seis pagos fraudulentos denunciados por la parte reclamante.

Modificación del límite de la tarjeta de crédito (transacción *modifyCardLimits* correspondiente al día 17/01/2022).

Contratación de dos nuevas tarjetas de crédito con número de contrato ***CONTRATO.1 y ***CONTRATO.2 (transacciones *createCardV2* y *certifyCard* correspondientes al día 17/01/2022).

- Documentación que acredite la aceptación de todas las operaciones anteriores por la parte reclamante.

- El día de los hechos, se envió un correo electrónico a la parte reclamante indicando "Has iniciado una compra en ***revolut*******LOCALIDAD.1 con tu tarjeta terminada en 1519 que no se ha completado". Indique a qué registro del informe de trazabilidad (Documento_n_4.pdf) remitido a esta Agencia se corresponde este mensaje y los motivos por los que esa compra no se completó.

- Según escrito remitido por el defensor del cliente de la parte reclamada a la parte reclamante, se enviaron seis mensajes mediante el sistema PUSH-MOOM a la parte reclamante confirmando los pagos efectuados en ***REVOLUT***. Estos mensajes no figuran entre los reportados a esta Agencia como

contestación al anterior requerimiento, por lo que se solicita información sobre estos mensajes y los datos que permitan identificar al destinatario de los mismos.

Sobre el punto 1, la parte reclamada, en relación a la activación del acceso biométrico, indica lo siguiente:

"*El procedimiento para activar el acceso biométrico es un SMS con la clave OTP, se alerta a la Sra.* ***A.A.A.*** *de que si no ha solicitado dicho acceso contacte con la Línea* ***XXXX*** *en el* ******TELÉFONO.3.***
[…]"

La parte reclamada adjunta pantallazo de sus sistemas donde se ve el detalle del texto enviado a la parte reclamante mediante mensaje SMS enviado al número de teléfono móvil ***0034***TELÉFONO.1*** (mismo número de teléfono que indica la parte reclamante en su denuncia ante la DGP):

"La clave para activar tu acceso biométrico es: XXXXXX. Si no lo has solicitado tú, llama ahora al ******TELÉFONO.3****."*

En contestación a este mismo punto 1, en relación a los seis cargos reclamados, la parte reclamada comenta:

"*Para realizar la operativa "el cliente" accedió a la app por biometría (algo que eres) y las operaciones se firman con clave de acceso multicanal (algo que sabes).*

Se acompañan como documentos del nº 1 al 6 los informes de Redsys.

La contratación de las dos tarjetas de crédito con números ******CONTRATO.1*** *y* ******CONTRATO.2*** *se ha realizado desde la app de particulares de* ***XXXX.es*** *y han sido firmadas telemáticamente mediante segundo factor de autenticación, en este caso a través de clave de usuario multicanal. Para poder firmar operaciones con clave de usuario multicanal es necesario tener previamente activado el acceso biométrico a la app y el acceso biométrico a la app fue activado mediante segundo factor de autenticación, en este caso a través de OTP-SMS enviado al móvil validado del cliente el 17/01/2022 a las 19:15:02 como se evidencia en la captura de pantalla anterior.*".

Sobre el punto 3, la parte reclamada, en su contestación remitida a esta Agencia, no contesta específicamente a este punto.

Sobre el punto 4, la parte reclamada contesta:

"*Las notificaciones Push-Moom aparecen en la propia app de* ***XXXX****. Hay varios tipos de notificaciones. Las de seguridad que no son configurables y que se envían siempre que se produce el evento que lo desencadena (alerta nuevo dispositivo, activación firma biométrica, cambio de móvil validado, ubicación anómala, transferencia de alto importe, etc). Luego están las notificaciones de alerta operativa que se tiene que configurar el propio cliente (transferencias emitidas o recibidas a partir del importe que el cliente determine, cargo de recibos domiciliados a partir del*

importe que el cliente determine, reintegros de efectivo o compras con tarjeta a partir del importe que el cliente determine, etc). Concretamente a la Sra ***A.A.A.*** *se le enviaron ambos tipos de comunicaciones (vía push-moom y vía correo electrónico al email validado en* ***XXXX****): Las de seguridad por alerta de nuevo dispositivo y bloqueo de usuario multicanal (al detectar nuestras herramientas de monitorización que se estaba realizando una operativa sospechosa que no se correspondía con los patrones habituales de la cliente) y las comerciales y operativas con información contractual de las tarjetas contratadas y de denegación de compras (esto último es lo que tenía configurado la Sra.* ***A.A.A.****).*".

Sobre ello, la parte reclamada adjunta pantallazos a modo de evidencia que ya habían sido enviados con motivo del primer requerimiento y que han sido analizados previamente en este informe.

La parte reclamada añade, en su contestación, un punto adicional en el que indica:

"*Acompaña la Sra.* ***A.A.A.*** *junto con la documentación de su reclamación un correo phishing que recibió vía e-mail al buzón* ******EMAIL.2*** *informando de que se ha inhabilitado provisionalmente la tarjeta de crédito* ******TARJETA.3****. Cómo se puede apreciar el correo es fraudulento ya que la tarjeta ni siguiera es titularidad de la Sra.* ***A.A.A.*** *y está caducada. Además, posteriormente indican que la tarjeta termina en "1519". Copio a continuación captura y acompaño como documento nº 7*.

Es decir, la Sra. ***A.A.A.*** *acompaña con su reclamación un e-mail sin percatarse de que se trata de un phishing, por lo que cabe la posibilidad de que en el convencimiento de que se trataba de un e-mail del banco interactuara con una web fraudulenta desvelando sus credenciales*."

Por último, la parte reclamada en su contestación adjunta seis documentos proporcionados por Redsys Servicios de Procesamiento, S.L., (en adelante, Redsys) correspondientes a las seis operaciones reclamadas que se realizaron el día de los hechos (17 de enero de2022) con la tarjeta terminada en 1519 donde se puede observar todo el detalle de las mismas. Estas operaciones están autentificadas mediante el proceso 3D Secure que requiere que la entidad emisora del pago verifique la autenticidad del titular que realiza la operación correspondiente mediante mensaje OTP o biometría, entre otros. El día 06/07/2022 se accedió a la página web https://pagosonline.redsys.es/funcionalidades-autenticacion3DS.html donde se hace referencia a este proceso de autentificación. Asimismo, el día 08/07/2022 se accedió a las páginas web ******URL.1*** y ******URL.2*** donde se hace referencia a las operaciones de pago que requieren autentificación reforzada que es la combinación de dos de tres factores de autentificación, en concreto, algo que sabes (PIN o password), algo que tienes (un teléfono, la tarjeta, un token...) y algo que eres (huella dactilar, voz, etc.). Dado el valor de las seis operaciones reclamadas (480 euros), estos pagos requerían de un segundo factor de autentificación al no estar sujetas a las exenciones previstas sobre la doble autentificación establecidas según la normativa vigente de servicios de pago (PSD2).

El día 6 de julio de 2022 se envió un requerimiento de información a la parte reclamante, con fecha de acuse de recibo de ese mismo día 06/07/2022, a fin de

recabar algunos datos y comunicaciones mantenidas entre ella y la parte reclamada, entre otros, los motivos por los que cambió el número de tarjeta bancaria en su segunda denuncia ante la DGP, detalle de los mensajes SMS que recibió en su terminal móvil el día de los hechos, si tuvo algún problema con su terminal móvil que pudiera indicar que se llevó a cabo un duplicado de tarjeta SIM no autorizado y el detalle del correo electrónico que aportó en su reclamación que contenía el texto "Tarjeta inhabilitada provisionalmente" por si pudiera haber sido el medio (*phishing*) por el que los ciberdelincuentes accedieron a la banca online de la parte reclamante de cara a realizar las operaciones fraudulentas. Por desgracia, este requerimiento no ha sido contestado por la parte reclamante a fecha del presente informe.

El día 21 de septiembre de 2022 se envió un tercer requerimiento de información a la parte reclamada de cara a tener más detalle sobre algunas informaciones que previamente había remitido a esta Agencia. En la contestación a este requerimiento la parte reclamada adjunta un documento (documento_n_1) donde Redsys certifica lo siguiente:

"*Que según los datos que obran en sus registros, con fecha 17 de enero de 2022 la información sobre la operativa relativa a la tarjeta número* ******TARJETA.2*** *es la que se detalla en el documento que se adjunta como Anexo 1 a este certificado.*

Que, según figura en los registros, las citadas operaciones fueron autorizadas, registradas con exactitud y contabilizadas y no se vieron afectadas por un fallo técnico o cualquier otra deficiencia.

Que así mismo, las operaciones fueron de comercio electrónico y el cliente fue autenticado mediante 3d secure en comercio electrónico."

En dicho certificado se muestra un listado de operaciones de pago por importe de 480 euros, en concreto doce operaciones realizadas en el comercio ***Revolut***. En este listado figuran siete operaciones de compra como aprobadas (en negrita) y cinco como canceladas:

Banco Emisor Autent.		**Tarjeta Autent.**	**Fecha/Hora Operación**	**Nombre Comercio**	**Método Autent.**	**Estado Autent.**	**Teléfono OTP**
182	***XXXX***	******TARJETA.2***	17/01/2022 20:16	Revolut	OoB	**OPERACION APROBADA**	
			17/01/2022 20:20	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	
			17/01/2022 20:21	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	
			17/01/2022 20:22	revolut****LOCALIDAD.1	OoB	OPERACIÓN CANCELADA	
			17/01/2022 20:22	revolut****LOCALIDAD.1	OoB	OPERACIÓN CANCELADA	
			17/01/2022 20:22	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	
			17/01/2022 20:23	revolut****LOCALIDAD.1	OoB	OPERACIÓN CANCELADA	
			17/01/2022 20:23	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	
			17/01/2022 20:23	revolut****LOCALIDAD.1	OoB	OPERACIÓN CANCELADA	
			17/01/2022 20:24	revolut****LOCALIDAD.1	OoB	OPERACIÓN CANCELADA	
			17/01/2022 20:24	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	

		17/01/2022 20:25	revolut****LOCALIDAD.1	OoB	**OPERACION APROBADA**	

Asimismo, la parte reclamada señala:

"***XXXX*** *comprueba que las mismas fueron firmadas con "out of band" (accediendo a la app con biometría y autorizando la compra) y a continuación firmando la compra con su clave de acceso.*"

En el certificado de Redsys también figura un listado, a continuación del anterior, en el que figura seis operaciones de compra como autorizadas en el comercio ***Revolut*****2732* y con modo de autenticación mediante 3D Secure en comercio electrónico por importe de 480 euros cada una de ellas:

Fecha Operación (del TPV)	Hora Operación (del TPV)	Fecha Autorización	Hora Autorización	Código Operación	Respuesta Autorización Operación
1/17/2022	19:17:07	1/17/2022	20:17:07	Compra	AUTORIZADA
1/17/2022	19:20:44	1/17/2022	20:20:44	Compra	AUTORIZADA
1/17/2022	19:22:01	1/17/2022	20:22:01	Compra	AUTORIZADA
1/17/2022	19:23:09	1/17/2022	20:23:09	Compra	AUTORIZADA
1/17/2022	19:24:06	1/17/2022	20:24:05	Compra	AUTORIZADA
1/17/2022	19:24:59	1/17/2022	20:24:59	Compra	AUTORIZADA

El día 14 de octubre de 2022 se accede a la página web ******URL.3*** diseno.pdf donde se explica la aplicación de fuera de banda (*Out Of Band, OoB*) más el uso de biometría como solución para la autenticación SCA (*Strong Customer Authentication*).

Asimismo, adjunta un segundo documento (documento_n_2) donde vuelven a enviar la traza de transacciones realizadas correspondientes al día de los hechos reclamados (17 de enero de 2022) donde se aporta una breve descripción del tipo de transacción (ya analizado previamente en este informe), el medio de autenticación (FIDO o autenticación mediante usuario y password personales) y el tipo de firma de cada transacción (password personales, autenticación mediante OTP/SMS, no aplica). Como ya se ha analizado previamente, las transacciones que requieren, según la información aportada por la parte reclamada, password personales son las del tipo *certifyCard, createCardV2, getCardSecurityData* y *modifyCardLimits.* Las transacciones con autentificación mediante OTP/SMS son las correspondientes al tipo *finalizeDeviceBiometricEnrollm.* Por último, en las transacciones de tipo *solicitarTicketConsumoAPI* se indica en la columna "Tipo de firma" que "no aplica".

En este tercer requerimiento se le indicaba a la parte reclamada que en la documentación que había remitido previamente a esta Agencia se señalaba que se envió un correo electrónico el día 17 de enero de2022 a las 20:23:43 señalando que una operación realizada con la tarjeta terminada en 1519 no se había completado (esta pregunta ya se había planteado a la parte reclamada en el segundo requerimiento, pero no fue contestada explícitamente). De este modo, se solicitaba a la parte reclamada el detalle de por qué no se completó esta operación y con qué traza se correspondía con respecto al listado de trazas de transacciones enviado a esta

Agencia por la parte reclamada. A este punto la parte reclamada contesta lo siguiente y adjunta un pantallazo de sus sistemas:

"*La tarjeta* ******TARJETA.2*** *la única operación que tiene denegada fue el 17/01/2022 20:25:29, la cual se rechazada, debido a que la tarjeta a las 20:24:59 se procedió a bloquear de manera automática por ráfaga de operaciones en el mismo comercio y mismo importe, tras autenticarse la operación anterior*"

Rango de fechas consultadas: 17/1/2022 - 17/1/2022

	Modo de Operar	Tipo Operación/Resultado	Cod.Acción Adq/Resolutor/Regla Lynx	Fecha y Hora	Tipo Mensaje	Cod. Proceso	Importe/Moneda	FUC	Número Tarjeta	Cod. Autorización
	@	Compra Autorizada	000/000	17/01/2022 19:17:07	1100	000000	480,00 / 978 EURO	000000000	455223******1519	170768
	@	Compra Autorizada	000/000	17/01/2022 19:20:44	1100	000000	480,00 / 978 EURO	117531866	455223******1519	204568
	@	Compra Autorizada	000/000	17/01/2022 19:22:01	1100	000000	480,00 / 978 EURO	117531866	455223******1519	220168
	@	Compra Autorizada	000/000	17/01/2022 19:23:09	1100	000000	480,00 / 978 EURO	117531866	455223******1519	230968
	@	Compra Autorizada	000/000	17/01/2022 19:24:06	1100	000000	480,00 / 978 EURO	117531866	455223******1519	240668
	@	Compra Autorizada	000/000	17/01/2022 19:24:59	1100	000000	480,00 / 978 EURO	117531866	455223******1519	245968
	@	Compra Denegada	000/190 80030 TARJETA EN EXCEPCIONES.	17/01/2022 19:25:29	1100	000000	480,00 / 978 EURO	117531866	455223******1519	

Asimismo, en contestación al tercer punto del tercer requerimiento, la parte reclamada señala que:

"*Como se ha indicado previamente se trata de operaciones realizadas en comercios con tarjetas, es por ello que se aporta el informe de Redsys para acreditar la operación (numeración, cvv y fecha de caducidad) y segundo factor de la página de* ***Revolut*** *es ajena a la entidad.*"

Respecto al cuarto punto del tercer requerimiento de información en el que se solicitaba la justificación de por qué se procedió al bloqueo del usuario multicanal y si ello también supuso el bloqueo de la tarjeta terminada en 1519, la parte reclamada indica:

"*El 17/01/2022 20:38:22 tras la 2ª contratación de la tarjeta y la multitud de consultas de CVV se procedió a bloquear los SSTT del cliente de modo preventivo, informándole a través de notificaciones push/mail.*"

Como ya se ha analizado previamente en este informe, las notificaciones push/ mail fueron ya acreditadas previamente por la parte reclamada donde le informaba a la parte reclamante de lo siguiente:

"*A pesar de que tu acceso a la App, al área privada de XXXX.es y a operar con tus claves en los cajeros no es posible actualmente, podrás seguir utilizando tu/s tarjeta/s tanto en nuestros cajeros, como en compras online o físicas. Para la reactivación de tu usuario necesitamos identificarte, por lo que es necesario que acudas a cualquier oficina de* ***XXXX*** *con tu DNI/pasaporte u otro documento identificativo o contactando con Línea* ***XXXX*** *a través del número de teléfono* ******TELÉFONO.2***.".

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto 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 lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación 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
Seguridad del tratamiento

El artículo 32 del RGPD estipula 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

Principios relativos al tratamiento

La letra f) del artículo 5.1 del RGPD propugna:

"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»)."

IV

Hechos objeto de reclamación

La parte reclamante indica que, en fecha 17 de enero de 2022, a través de la banca online de la parte reclamada, un tercero, usurpando su identidad realizó varias compras fraudulentas con cargo a su tarjeta de crédito, sin que la parte reclamada hubiese verificado su identidad, además de no haber recibido la reclamante ningún código de seguridad, ni habérsele solicitado ninguna firma digital para ello.

Durante las actuaciones previas de investigación, en primer lugar, se requirió a VODAFONE si se había solicitado duplicado de tarjeta SIM correspondientes al número de teléfono móvil de la parte reclamante (******TELÉFONO.1***) s durante el mes de enero de 2022, mes en el que se produjeron los hechos reclamados. La contestación de VODAFONE fue que no se había realizado ninguna operación de cambio de tarjeta SIM y que tampoco había ninguna orden de trabajo, ni anulada ni

tramitada para cambio de tarjeta SIM, ni en el año 2022 ni en todo el histórico de movimientos de la parte reclamante.

Por otro lado, la parte reclamada para acreditar las medidas de seguridad desplegadas en el momento de realizarse las operaciones con la tarjeta de la parte reclamante ha enviado pantallazos de las comunicaciones mantenidas entre ella y la parte reclamante. Entre otras, figura un correo electrónico enviado por la parte reclamada a la dirección de correo electrónico de la parte reclamante (******EMAIL.2***) el día 17 de enero de 2022 a las 20:14h y un mensaje PUSH-MOOM enviado a la aplicación móvil de la parte reclamante, alertando de que se había accedido a la aplicación móvil desde un dispositivo móvil distinto al habitual, en concreto, un dispositivo móvil Alcatel 1SE, dispositivo distinto al de la parte reclamante, tal y como señala ésta en su reclamación presentada en esta Agencia. Asimismo, la parte reclamada también acredita el envío de dos correos electrónicos con información relativa a la contratación de dos tarjetas bancarias a la dirección de correo electrónico de la parte reclamante (******EMAIL.2***) el día 17 de enero de 2022. Por último, también es significativo destacar el mensaje PUSH-MOOM enviado a la aplicación móvil de la parte reclamante ese mismo día indicando que se había iniciado una compra en ***Revolut*** con la tarjeta terminada en 1519 que no se completó.

Sobre las seis operaciones reclamadas por importe de 480 euros cada una de ellas, Redsys ha certificado que fueron autentificadas mediante 3D Secure que requiere que la entidad emisora del pago verifique la autenticidad del titular que realiza la operación correspondiente mediante mensaje OTP o biometría, entre otros. De hecho, dichas seis operaciones reclamadas fueron autentificadas biométricamente mediante FIDO (*Fast Identity Online*). Para ello, previamente fue necesaria la activación de este servicio de autentificación biométrica de operaciones en línea (FIDO). Como ha acreditado la parte reclamada, para su activación se envió un mensaje SMS-OTP al número de teléfono móvil de la parte reclamante (******TELÉFONO.1***). Asimismo, es importante señalar que otras operaciones llevadas a cabo el día 17/01/2022, en concreto, la contratación de dos tarjetas bancarias, la modificación del límite de las mismas y el acceso a los datos de seguridad de las tarjetas, también se validaron mediante FIDO, tal y como ha acreditado la parte reclamada.

El día 6 de julio de 2022, el Inspector de datos responsable de las actuaciones previas envió un requerimiento de información a la parte reclamante, con fecha de acuse de recibo de ese mismo día, a fin de recabar algunos datos y comunicaciones mantenidas entre ella y la parte reclamada, entre otros, los motivos por los que cambió el número de tarjeta bancaria en su segunda denuncia ante la DGP, detalle de los mensajes SMS que recibió en su terminal móvil el día de los hechos (17 de enero de 2022), si tuvo algún problema con su terminal móvil que pudiera indicar que se llevó a cabo un duplicado de tarjeta SIM no autorizado y el detalle del correo electrónico que aportó en su reclamación que contenía el texto “Tarjeta inhabilitada provisionalmente” por si pudiera haber sido el medio (*phishing*) por el que los ciberdelincuentes accedieron a la banca online de la parte reclamante de cara a realizar las operaciones reclamadas. Este requerimiento no ha sido contestado por la parte reclamante.

V
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos, al entenderse que la parte reclamada tenía medidas de seguridad adecuadas para alertar a la parte reclamante de los movimientos realizados con su tarjeta.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al BANCO BILBAO VIZCAYA ARGENTARIA, S.A. y a la parte reclamante.

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.

940-091222

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