Procedimiento N.º: PS/00001/2021

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos (en lo sucesivo, AEPD) y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante uno), en fecha 2 de septiembre de 2019, interpone una reclamación ante la AEPD dirigida contra **VODAFONE ESPAÑA, S.A.U.** con CIF A80907397 (en adelante, VODAFONE o VDF), por los siguientes motivos:

"El día 5 de Agosto sobre las 21:00 horas de la noche compruebo que mi terminal con línea de su compañía ******TELÉFONO.1*** *se queda sin la red y no puedo efectuar ni recibir llamadas, por lo que llamo al Servicio de Atención al Cliente y tras 2 minutos de espera me dicen que la línea está bien y que acuda a un Distribuidor (tienda de Vodafone) para ver si se puede tratar de algún problema en la tarjeta SIM, que pueda estar dañada y que se soluciona con un cambio de la misma.*

Al día siguiente día 6 de agosto, dado que trabajo en una localidad a 70 kms de mi domicilio y allí no hay tienda, no puedo hacerlo hasta las 18:30 horas de la tarde y acudo a la tienda Vodafone que se encuentra en la calle Ancha nº 26 donde además de facilitarme una nueva SIM con coste de 5 euros, me contratan una oferta de algunos canales más a mi Tv del paquete que tengo contratado.

En el momento de recuperar el teléfono, sobre las 19:04 horas y una vez restablecida normalmente mi línea, recibo entrada de nuevos mensajes y en uno de ellos, una Alerta del Banco de Santander, me dice que estoy realizando una transferencia desde mi banca On line y que, si no es así, me ponga en contacto con el número ******TELÉFONO*** *en horario de 9:00 a 19:00 horas lo cual no hago, pues lo recibo a las 19:04 horas.*

Al llegar a mi domicilio, intento entrar en la Banca Digital pero no puedo acceder con mis contraseñas para comprobar si ha habido algún movimiento extraño en mi cuenta, lo cual pospongo para el día siguiente 7 de Agosto en la Sucursal del Banco de Santander en ******LOCALIDAD.1****, lugar donde trabajo; Es en la sucursal cuando un empleado me saca un extracto donde me comunican que tengo concedido y contratado un Préstamo, y una vez concedido ha habido 25 operaciones de gastos, compras de tarjetas de crédito, transferencias, y pagos a otras entidades, que yo no he realizado, por lo que acudo a formular una denuncia ante la Guardia Civil, porque alguna persona o personas, ha utilizado mis contraseñas y mi acceso a Banca On Line del Santander, para hacer todas esas operaciones de manera fraudulenta.*

Es obvio que utilizaron mi línea telefónica secuestrada durante 1 día y medio,

fecha en que acudo a hacer personalmente un duplicado de mi tarjeta.

*A posteriori de la Denuncia, y en llamada a Vodafone interesándome por lo que había pasado en aquellos dos días, un agente de la Compañía me informa que el día 5 a las 20:39 horas de la tarde, alguna persona o personas, han hecho un duplicado de mi tarjeta en la Tienda Vodafone del Centro Comercial "*****CENTRO.1**" de *****LOCALIDAD.3** (Cornellá) que yo no he realizado y por lo tanto DENUNCIO por suplantación de identidad, o por negligencia de quien o quienes permitieron ese cambio con mis datos, estando yo a 800 kms de distancia.*

Esto provoca el posterior delito o delitos de estafa, celebrando un contrato irregular de un Préstamo a mi nombre y la compra de tarjetas de crédito con saldos, además de un Seguro y varios movimientos con ese dinero conseguido, que yo no he autorizado".

Junto a la reclamación aporta la denuncia presentada ante la Guardia Civil de ******LOCALIDAD.1*** (******PROVINCIA.1***), en fecha 7 de agosto de 2019, con número de atestado ******ATESTADO.1***` y la factura número ******FACTURA.1*** emitida por VDF en esa misma fecha, que contiene el cargo correspondiente a la emisión de una tarjeta SIM ((Subscriber Identity Module – Modulo de Identidad del Abonado), donde especifica como dirección de entrega un Centro Comercial ubicado en el municipio de ******LOCALIDAD.2***, cuando el RECLAMANTE UNO tiene su residencia habitual en el municipio de ******PROVINCIA.1***.

De acuerdo con lo previsto en 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 lo sucesivo, LOPDGDD), que consiste en dar traslado de las mismas a los Delegados de Protección de Datos designados por los responsables o encargados del tratamiento, o a éstos cuando no los hubieren designado, y con la finalidad señalada en el referido artículo, en fecha 21 de octubre de 2019, se dio traslado de la reclamación a VDF, para que procediera a su análisis y diera respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

*"Tras analizar la denuncia presentada por el Sr. **A.A.A.** y realizar las investigaciones internas oportunas hemos verificado que con fecha 5 de agosto de 2019, se realiza un cambio de tarjeta SIM en la Tienda de Vodafone sita en el Centro Comercial *****CENTRO.1**, para la línea *****TELÉFONO.1** asociada a D. **A.A.A.**, con domicilio en C/ *****DIRECCIÓN.1, ***PROVINCIA.1**.*

*En su reclamación, el Sr. **A.A.A.** expone que, con fecha 7 de agosto de 2019, acudió a la Guardia Civil de *****LOCALIDAD.1** (*****PROVINCIA.1**) denunciando la posibilidad de que le hubieran suplantado la identidad y hubiesen realizado un duplicado de su tarjeta SIM sin su consentimiento, asociándolo a una serie de operaciones bancarias realizadas en su nombre con un préstamo bancario del Banco Santander no reconocido. Al día siguiente remite una carta por correo electrónico a mi representada, sobre los mismos hechos.*

Al llevar a cabo las investigaciones internas oportunas sobre el duplicado de

*tarjeta SIM que se reclama, Vodafone procedió a **(…).***

*Asimismo, y de conformidad con la política de seguridad de Vodafone, la tramitación de un duplicado de tarjeta SIM únicamente podrá tramitarse si **(…)**. Las políticas de seguridad de Vodafone se ponen a disposición de todos nuestros colaboradores y proveedores, siendo el cumplimiento de sus disposiciones obligatorio por todos sus empleados. No obstante, pueden existir casos en los terceros anteriormente referidos, por razones no relacionadas con Vodafone y fuera de su control puesto que son resultado de la toma de decisiones de una persona, no cumplan con la totalidad de lo dispuesto en dicha política.*

En cualquier caso, desde Vodafone se procedió a tomar las acciones necesarias para garantizar la seguridad de la cuenta. A tal efecto, la tarjeta SIM duplicada objeto de reclamación ha quedado debidamente bloqueada.

Sin perjuicio de lo anterior, desde mi representada no ha sido posible averiguar la identidad del responsable de la autorización al cambio de tarjeta SIM realizado el pasado 5 de agosto. (…)

Es importante en este caso poner de manifiesto que el hecho de hacer un duplicado de SIM, no implica más que acceso a la línea de teléfono, no sería posible acceder a contraseñas, datos bancarios y otra información del titular de la cuenta salvo que el tercero disponga de otra serie de datos personales del titular porque hubiera tenido acceso a los mismos o se los hubiera robado previamente. Pedir un crédito al banco o hacer transacciones solo por duplicado de SIM es altamente improbable como decimos sin disponer de otro tipo de información de la persona. (…)".

Sobre dicha reclamación recayó resolución de ARCHIVO DE ACTUACIONES de fecha 2 de diciembre de 2019, en el expediente con núm. de referencia E/10004/2019.

SEGUNDO: ***B.B.B.*** (en adelante, la parte reclamante dos), en fecha 20 de noviembre de 2019, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

"Mi compañía telefónica por unas medidas de seguridad malas en materia de protección de datos, ha permitido duplicar mi tarjeta SIM de mi teléfono, hasta en tres ocasiones (2, 3 y 12 de noviembre de 2019) a personas ajenas, accediendo así a todos mis datos y como consecuencia de esto han defraudado mis cuentas bancarias reintegrando todo su contenido, así como solicitar préstamos y abrir cuentas suplantando mi identidad".

Junto a la reclamación aporta tres denuncias con número de atestado ******ATESTADO.2*** de fecha 4 de noviembre de 2019; ******ATESTADO.3*** de fecha 5 de noviembre de 2019; y, ******ATESTADO.4*** de fecha 12 de noviembre de 2019; todas ellas, presentadas ante la Dirección General de la Policía Nacional (en adelante, DGPN) en las dependencias de Madrid-San Blas, denunciando estos hechos.

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 2 de enero de 2020, en el expediente con núm. de referencia E/12065/2019.

TERCERO: Con fecha 27 de noviembre de 2019, la directora de la AEPD, ante las

noticias aparecidas en medios de comunicación relativas a la utilización de prácticas fraudulentas basadas en la generación de duplicados de tarjetas SIM sin el consentimiento de sus legítimos titulares con objeto de acceder a información confidencial con fines delictivos (conocidas como “SIM Swapping”), insta a la Subdirección General de Inspección de Datos (en lo sucesivo, SGID) a iniciar de oficio las Actuaciones Previas de Investigación tendentes a analizar estas prácticas y las medidas de seguridad existentes para su prevención.

A saber:

Vodafone: "Duplicaron mi SIM y me robaron **XXXX**€": el fraude del 'SIM swapping' vuelve a España (elconfidencial.com)

https://www.elconfidencial.com/tecnologia/2019-09-10/sim-swapping-timo-duplicado-tarjeta-estafa_2216863/

El timo de la SIM duplicada: si su teléfono hace cosas raras, revise la cuenta bancaria | Economía | EL PAÍS (elpais.com)

https://elpais.com/economia/2019/05/21/actualidad/1558455806_935422.html

La peligrosa estafa de moda: Duplicar tu número de móvil para vaciarte la cuenta del banco | Tecnología (elmundo.es)

https://www.elmundo.es/tecnologia/2020/10/15/5f8700b321efa0c9118b462c.html

CUARTO: ***C.C.C***. en nombre y representación de ***D.D.D.*** (en adelante, la parte reclamante tres), en fecha 28 de noviembre de 2019, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

> *“El pasado 28 de septiembre Vodafone dio de paso un duplicado de SIM fraudulento (SIM swapping) en la tarjeta de mi marido (**D.D.D.**), ingresado en el hospital por aquel entonces, aquejado de una grave enfermedad.*
>
> *Tras muchas llamadas para intentar parar el proceso fraudulento, Vodafone hizo caso omiso y le entregó la copia de la SIM al estafador. Con esto le dio la llave de acceso a nuestras cuentas bancarias y consiguieron robarnos dinero, pedir préstamos a nombre de mi marido, pagos a casas de apuestas, pagos Bizum, venta de acciones y sustracción del dinero, retiradas de efectivo en cajeros...*
>
> *Quiero aclarar que no estamos reclamando ninguna deuda ni la inclusión en ningún fichero de morosos, sino la negligencia de Vodafone al entregar los datos privados y financieros de un cliente a un estafador, dándole la herramienta para acceder a las cuentas bancarias y robar a sus anchas.*
>
> *Posteriormente y con fecha 2 de noviembre mi marido falleció, por lo que no es posible que haga la reclamación él mismo”.*

Junto a la reclamación aporta dos denuncias con número de atestado ******ATESTADO.5***, de fecha 24 de octubre de 2019 y ******ATESTADO.6***, de fecha 4 de noviembre de 2019. Ambas presentadas por la hija de ambos -***E.E.E.***- ante la DGPN en las dependencias de ******LOCALIDAD***.

En fecha 22 de octubre de 2019, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

> *"(…) la persona infractora que suplantó la identidad del Sr.* ***D.D.D.*** *a fin de conseguir realizar el cambio o duplicado de la tarjeta SIM, (…). A estos efectos, el infractor conocía previamente la información personal del Sr.* ***D.D.D.****, en concreto, nombre, apellidos, NIF y cuenta de domiciliación.*
>
> *Por ello, en tanto todos los datos fueron facilitados de manera correcta a través del (…), para mi representada la persona que estaba solicitando el cambio de SIM era el correcto titular, el Sr.* ***D.D.D.,*** *no pudiendo de ningún modo advertir de que dicha persona no se trataba del Sr.* ***D.D.D.****, sino de un infractor que estaba suplantando su identidad.*
>
> *En cualquier caso, quiere mi representada recalcar que, un cambio o duplicado de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, y de ningún modo ofrece la posibilidad de que la operadora facilite los datos bancarios del titular.*
>
> *De este modo, de ningún modo es posible afirmar que exista una responsabilidad de Vodafone por las acciones ocurridas en las cuentas bancarias de ING y Banco Santander del Sr.* ***D.D.D.****, a lo cual se hará referencia más adelante.*
>
> *Tras realizar las investigaciones oportunas, se comprobó que, en fecha 28 de septiembre de 2019, tras recibir las llamadas a las que hace referencia la Sra.* ***C.C.C.*** *en su reclamación,* ***(…).***
>
> ***(…).***

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 25 de febrero de 2020, en el expediente con núm. de referencia E/00557/2020.

QUINTO: ***F.F.F.*** (en adelante, la parte reclamante cuatro), en fecha 28 de noviembre de 2019, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

> *"El pasado martes 12 y 14 de noviembre me realizaron de modo fraudulento una copia SIM de dos de mis tres líneas que tengo contratadas en Vodafone, concretamente los números* ******TELÉFONO.2*** *y* ******TELÉFONO.3****. Al preguntar en el servicio de atención al cliente y en las oficinas me confirman que se realizaron por vía telefónica, sin pedir físicamente el DNI en ninguna oficina. Nadie me ha explicado a día de hoy en Vodafone cómo es posible que cualquier persona que de mi número de DNI por teléfono pueda recibir una copia SIM de mis líneas".*

En fecha 22 de enero de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo si-

guiente:

“

- La “SIM Original” en el momento del alta del servicio tenía asignada la numeración ******SIM.1.***

- El 12/11/2018 se solicita duplicado vía telefónica de la SIM Original que pasa a ser la “(…)” con numeración ******SIM.2.***

- El 14/11/2018 tras la activación de la “SIM Bis” se solicita su duplicado presencial y pasa a ser la “(…)” con numeración ******SIM.3.***

De otro lado, en lo que respecta a la línea de la cual también es titular el Sr. ***F.F.F.****,* ******TELÉFONO.2****, en fecha 14 de noviembre de 2019, se comprobó que se produjo desde la tienda* ******TIENDA.1*** *de Majadahonda un cambio de tarjeta SIM, pasando del número inicial* ******SIM.4*** *al número* ******SIM.5****, “(…)”.*

De igual forma, el Sr. ***F.F.F.*** *contactó con Vodafone ese mismo día, con el fin de informar de la realización de un duplicado de tarjeta SIM que él no había solicitado. Por tanto, nos encontramos ante la circunstancia de que se solicitaron dos cambios de tarjetas SIM (…) de los dos servicios del Sr.* ***F.F.F.****, una el día 12 de noviembre de 2019, y otra el 14 de noviembre de 2019, motivo por el cual el reclamante contactó con Vodafone al percibir que se quedaba sin servicio. Vodafone, ante semejantes circunstancias actuó con máxima celeridad y con carácter preventivo bloqueando ambas tarjetas SIM y evitando posibles actuaciones fraudulentas que pudieran beneficiarse de las pasarelas de seguridad utilizados por los medios de pago a través del envío de SMS.*

Vodafone procedió a restablecer el servicio del Sr. ***F.F.F.*** *en sus tarjetas SIM originales ese mismo día 14 de noviembre de 2019 quedando la incidencia resuelta. De esta manera, a fecha de la presente reclamación el Sr.* ***F.F.F.*** *dispone de tarjetas SIM activas y operativas, habiendo quedado automáticamente anuladas los duplicados realizados de forma fraudulenta. (…)*

Quiere mi representada resaltar la idea de que Vodafone no es la causante del fraude económico ocasionado al reclamante, en tanto en ningún momento ha proporcionado o facilitado la información relativa a la cuenta bancaria al tercero que solicitó el cambio de tarjeta SIM y que, no olvidemos, consiguió superar las medidas de seguridad de Vodafone porque ya tenía y conocía los datos personales del reclamante. En este sentido, señalar que mi representada desconoce cómo el infractor pudo tener acceso a los datos personales del reclamante para hacer uso de los mismos. Vodafone al igual que el reclamante, ha sido engañada por un tercero, quien, conocedor de los mecanismos de seguridad con que cuentan las entidades bancarias, sabía que el paso previo era obtener un duplicado de la SIM para poder recibir vía SMS las claves para acceder a la información bancaria del reclamante, utilizando como paso previo y mero instrumento para lograr su objetivo final a Vodafone. Mi representada es, por tanto, una víctima y perjudicada más en

todo este artificio fraudulento, viéndose altamente comprometida y dañada tanto su imagen de marca como la confianza que depositan en ella los clientes".

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 11 de marzo de 2020, en el expediente con núm. de referencia E/00558/2020.

SEXTO: ***G.G.G.*** (en adelante, la parte reclamante cinco), en fecha 4 de diciembre de 2019, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

"Como Clienta de la compañía telefónica Vodafone con numero de terminal ******TELÉFONO.4****.*

Me dirijo a este departamento para comunicarles que en julio de 2019 fui víctima de un fraude la cual la responsable fue dicha compañía telefónica. Debido a la insuficiente política de Seguridad que aplica la empresa para sus Clientes.

Hechos

Que en fecha 4 de agosto de 2019, contactó conmigo el Sr. ***H.H.H.*** *del departamento de transferencias fraudulentas de mi banco EVO BANC. El Señor* ***H.H.H.*** *me informó que en la madrugada del pasado día 29 de julio se efectuaron una serie de transferencias por valor de 15.000 € de las cuales el sistema de seguridad solo pudo anular las últimas, ascendiendo a la suma de 4889 euros.*

Tras mantener una conversación telefónica con el Señor ***H.H.H.****, el mismo me preguntó si recientemente había tenido algún tipo de incidencia con el dispositivo móvil. A lo que le indiqué, que efectivamente el pasado 29 de julio sobre las 20:00 el terminal había dejado de funcionar. En concreto, la SIM de mi número* ******TELÉFONO.4****, se encontraba totalmente inoperativa.*

Dada la hora en la que sucedieron los acontecimientos relatados, y dado que las tiendas físicas de Vodafone se encontraban cerradas al público, me personé al día siguiente sobre las 10.30h a efectos de poder conocer qué sucedía. La empleada de la tienda me indicó que debía de hacer una copia de la tarjeta dado que la SIM no funcionaba. Para poder completar este proceso, me solicitó el DNI y procedió a la venta y activación de la nueva tarjeta SIM, todo ello, sin verificar los datos correspondientes, dado que no se me hizo firmar ningún tipo de documentación.

Tal y como adelantaba, el Sr. ***H.H.H.*** *me aconsejó que llamará a mi compañía telefónica para averiguar el motivo por el que la tarjeta SIM de mi terminal, dejó de funcionar. Tras efectuar la correspondiente llamada gestión telefónica, me confirmaron que efectivamente se había hecho una copia de la misma el 29 de julio 2019 desde* ***(…).***

Tras localizar los datos de la referida tienda física, procedí a ponerme en contacto con el encargado Sr. ***I.I.I.****, que me confirmó que efectivamente en la fecha indicada se procedió a efectuar un duplicado de mi tarjeta SIM para lo que se presentó el correspondiente DNI que consta en los archivos de la*

tienda.

*Dada la imposibilidad material de haberse efectuado esta gestión por mi propia persona, le solicité que, por favor, me remitiera el supuesto documento de identificación personal presentado. El Señor **I.I.I.** me indicó que como consecuencia de la normativa referente a la protección de datos no podía facilitarme la documentación.*

A la vista de lo expuesto, no habiendo autorizado en ningún momento la expedición del duplicado de la tarjeta SIM, rogaría se me remita la información correspondiente acerca de cómo ha podido ser autorizada tal actuación.

*A la vista de lo expuesto, y dado que se realizó una transacción sin la correspondiente autorización y que ascendía al importe de **XXXX** €, tras ser conocedora de la anterior situación, procedí a interponer la denuncia correspondiente ante las dependencias policiales a fin de que el banco me pudiera reintegrar el importe retirado sin el correspondiente consentimiento otorgado por mi parte.*

La entidad bancaria tras interponer la denuncia me comunicó que por seguridad se procedería a bloquear todas las cuentas de las que soy titular.

Asimismo, he intentado en reiteradas ocasiones el contacto con el departamento de atención al cliente de Vodafone, habiendo resultado todos los intentos de conseguir solucionar esta situación infructuosa".

Junto a la reclamación aporta la denuncia presentada por estos hechos, en fecha 5 de agosto de 2019, con número de diligencia: ******DILIGENCIA.1*** ante los Mossos d'Esquadra, OAC de ******LOCALIDAD*** (Girona); certificado bancario expedido en esa misma fecha que informa sobre dos transferencias realizadas en fecha 29 de julio de 2019 desde su cuenta corriente a favor de un tercero -***J.J.J.-*** por un importe de 2.175'00 euros y 2.713'00 euros.

También aporta un CD-R que contiene la grabación de la conversación telefónica mantenida con la operadora de Vodafone, demandando una política de seguridad que evite la reproducción de estos hechos y una copia de la reclamación presentada ante la Secretaría de Estado para el Avance Digital, con registro de entrada de fecha 12 de septiembre de 2019.

En fecha 22 de enero de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

*"Tras analizar la reclamación e investigar lo sucedido, mi representada ha podido comprobar que, con fecha 29 de julio de 2019 se realizó, desde una tienda física de un distribuidor, en concreto, en Santa Cruz de Tenerife, un cambio de la tarjeta SIM correspondiente a la línea *****TELÉFONO.4***, *cuyo titular es la Sra. **G.G.G.***

En concreto, consta el cambio de numeración de la tarjeta SIM original

*"*****SIM.6**" al número "*****SIM.7**" ("(…)").*

*Asimismo, se comprobó que en fecha 30 de julio de 2019, figura la gestión de otro cambio de SIM vinculada a la misma línea móvil, realizado, en la misma tienda física de Vodafone. En particular, figura el cambio de la SIM Bis a la numeración "*****SIM.8**" ("(…)").*

*Como consecuencia de ello, en fecha 11 de octubre de 2019, la Sra. **G.G.G.** interpuso reclamación ante la SETSI, mediante la cual ponía de manifiesto la realización de un cambio de la SIM Original solicitando a Vodafone: (i) la baja de los servicios, y (ii) la indemnización por daños y perjuicios derivados del fraude, en concreto, la cantidad de **XXXX** € que detectó que habían sido transferidos desde su cuenta bancaria.*

*Mi representada respondió a dicha reclamación, en fecha 16 de octubre de 2019, informando de que el cambio de SIM Original asociado a su línea de teléfono *****TELÉFONO.4** tiene su origen en dos solicitudes creadas en un distribuidor de Vodafone, con fecha 29 y 30 de julio del 2019. Asimismo, se puso en conocimiento de la reclamante la política de seguridad de Vodafone, en virtud de la cual se debe presentar un documento que avale la identidad del solicitante para poder gestionar los duplicados de tarjetas SIM.*

Con respecto a la baja de los servicios que solicitó la reclamante, mi representada procedió a informarle de que, en tanto dichos servicios no contaban con compromiso de permanencia alguno, gestionar la baja supondría para ella perder la numeración salvo que solicitara una portabilidad de sus líneas a otro operador y causar el menor perjuicio posible. (…)

*De hecho, y tras comprobaciones realizadas en sistemas, mi representada ha verificado que la Sra. **G.G.G.** ha portado sin ningún tipo de cargo por compromiso de permanencia a la compañía Orange sus líneas móviles *****TELÉFONO.5** en fecha 11 de febrero de 2020 y *****TELÉFONO.6** en fecha 7 de febrero de 2020.*

*Con posterioridad, en fecha 29 de noviembre de 2019, la reclamante interpuso una segunda reclamación ante la SETSI, mediante la cual volvía a señalar que, debido a las transferencias realizadas desde su cuenta bancaria, solicitaba a Vodafone la indemnización del perjuicio económico causado. Mi representada respondió en fecha 11 de diciembre de 2019, indicando que, tras verificar la ausencia de consentimiento en el cambio de SIM, gracias a la denuncia adjunta interpuesta por la Sra. **G.G.G.** ante la Dirección General de la Policía y adjunta en la reclamación de la SETSI, el Departamento de Calidad de Vodafone ese mismo día contactó con la Sra. **G.G.G.**, a fin de explicarle los procesos de seguridad existentes en Vodafone que garantizan la seguridad de su cuenta cliente. Es importante indicar que fue al recibir esta segunda reclamación vía SETSI (29 de noviembre de 2019) cuando mi representada tuvo constancia del posible carácter fraudulento de la tramitación de los cambios de SIM realizados en los días 29 y 30 de julio de 2019. (…)*

En ese momento, el departamento de fraude de Vodafone estudió con

detenimiento lo ocurrido, y catalogó el cambio de SIM como ***(…).***

En cualquier caso, queda de todo modo probado que la compañía telefónica es un mero intermediario, a quien evidentemente, no puede serle repercutida la responsabilidad por la gestión con falta de diligencia efectuada por parte de la entidad bancaria en el seno de sus medidas de seguridad".

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 26 de febrero de 2020, en el expediente con núm. de referencia E/00559/2020.

SÉPTIMO: ***K.K.K.*** (en adelante, la parte reclamante seis), en fecha 17 de febrero de 2020, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

"Me pongo en contacto con ustedes para denunciar la grave situación en la que me encuentro desde que la compañía Vodafone facilitó mis datos personales y sensibles a un desconocido. Desde aquel día han ocurrido hechos muy graves y desconozco si en el futuro pueden acontecer otros similares.

Les adjunto varios documentos a mi escrito para que puedan verificar los hechos que voy a relatar a continuación.

El día 5 de enero de 2020, a las 18:23, una persona se hace pasar por mí llamando al servicio de atención al cliente de Vodafone y solicita que se envíe mi última factura de telefonía a un correo electrónico ajeno a mi y que ni siquiera consta en mis datos personales de cliente.

El servicio que tengo contratado con dicha Cía. es que para poder acceder a cualquier factura he de hacerlo a través de mi espacio como cliente que tuve activar con contraseñas personales y siempre online. Con mi área de cliente puedo descargar mis facturas y gestionarlas como considere ya que así lo contraté con ellos. En las facturas constan datos tan importantes como mi nombre completo, mi número de DNI, mi dirección de correo electrónico, la dirección de mi casa, todas las líneas que tengo contratadas, los extras contratados como TV y plataformas audiovisuales (en mi caso HBO y NETFLIX) y las cuatro últimas cifras de mi cuenta bancaria. No sólo es irregular que un operador de telefonía reenvíe una factura con dichos datos, sino que lo haga a un correo que no les consta en su base de datos. Yo entiendo que si alguien llama se le ha de remitir a su espacio personal, y como mucho reenviar una factura al correo electrónico que le consta a Vodafone en su base de datos.

A partir de este momento y en 13 llamadas efectuadas por esa persona durante la tarde del 05 de enero de 2020, intenta varios cambios de SIM (Vodafone dice que sólo puede hacerse en tienda física), solicitudes del número de PIN y PUK e intento de compra.

También me consta un intento acceso a HBO.

Dos días después, el día 07 de enero 2020, ocurre lo que Vodafone decía que era imposible. Me quedo sin línea sobre las 10:30 de la mañana. Esta persona realiza una llamada a Vodafone y dice tener una SIM por activar,

SIM que no sabemos ni si quiera de dónde sale. El operador que le atiende activa la SIM para mi línea de teléfono y yo dejo de tener conexión y no puedo llamar ni recibir llamadas.

Llamo a Vodafone ignorando lo sucedido y solicito que me activen la línea porque no funciona. El operador que me atiende en ningún momento me notifica que media hora antes se ha activado otra SIM, simplemente me pide que le facilita la numeración de mi tarjeta y al hacerlo me remite a tienda física para hacer un nuevo duplicado.

Dos horas después, en la tienda de Vodafone sita en el Corte Inglés de ******LOCALIDAD*** *tramitamos un cambio de SIM sin que me expliquen qué ha ocurrido con la línea y por qué ha fallado. Unas horas después, mi mujer (que es usuaria de una de las líneas), recibe un mensaje de texto en su teléfono de su entidad bancaria (ING Direct), donde le comunican que han bloqueado cuentas y tarjetas asociadas a* ***K.K.K.*** *y que comparte con él. Nos extrañamos porque yo soy beneficiario de sus cuentas, pero nunca he operado ni entrado en los Servicios de ING. No le dimos excesiva importancia hasta que bloquearon definitivamente todas sus tarjetas y cuentas (incluso las que no tenían relación conmigo). ING Direct detecta intento de entrada con mi identidad y mi línea telefónica. Desde el momento en que dispusieron de mi línea con el cambio de SIM, hasta que gestionamos nosotros en el Corte Ingles la nueva, han intentado operar en varios bancos solicitando el reenvío de contraseñas a mi línea de teléfono (que esa persona tenía activa).*

Afortunadamente, no hicieron intentos en mi entidad bancaria y lo hicieron en la de mi mujer, dónde consta mi DNI como beneficiario, pero no mi tlf porque nunca me he registrado. Suerte que los filtros de Seguridad de ING Direct han sido efectivos y han evitado una tragedia mayor para nosotros.

En una tienda de Vodafone situada en Barberà del Vallés, una trabajadora nos informa de todo lo acontecido en mis líneas. Me saca el listado de las operaciones realizadas por esa persona desconocida desde el día 5 de enero (les adjunto dicho documento).

Interponemos denuncia policial en comisaría de Mossos d'Esquadra (documento adjunto).

A partir de ahí, hemos pedido explicaciones a Vodafone en sucesivas llamadas solicitando medidas que garanticen que esto no acarree más consecuencias y sobre todo que no vuelva a ocurrir.

Me facilitaron una clave de Seguridad atención telefónica que no sirve para nada porque nunca la pide ningún operador.

No puedo anular estas líneas de teléfono porque hay una permanencia, y lo correcto es que estos números dejen de tener relación conmigo sabiendo que alguien dispone de tantos datos comprometidos.

La respuesta de Vodafone como empresa (me dirigí a oficinas en Barcelona de atención personal) es que nada se ha hecho mal y no me ofrecen ninguna

salida.

Finalmente he tenido que cancelar todos los Servicios (pagando casi 300 euros de permanencia por culpa de sus acciones) para asegurarme que no puedan seguir mi rastro a través de Vodafone".

Junto a la reclamación aporta la denuncia presentada por estos hechos, en fecha 9 de enero de 2020, con número de diligencia ******DILIGENCIA.2*** ante los Mossos d'Esquadra USC de ******LOCALIDAD*** (Barcelona); y, detalle facilitado por VDF de los movimientos efectuados por la persona que se hizo pasar por él.

En fecha 26 de marzo de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

"Tras analizar la reclamación e investigar lo sucedido, Vodafone ha podido comprobar que, con fecha 5 de enero de 2020, mi representada envió un duplicado de una factura a la dirección ******EMAIL.1****.*

Asimismo, en fecha 7 de enero de 2020, mi representada también pudo verificar que fue efectuado a través (…) un cambio de la tarjeta SIM correspondiente a la línea ******TELÉFONO.7,*** *asociada a la titularidad del reclamante, quien era cliente de Vodafone en dicha fecha.*

Quiere esta parte señalar que la efectiva gestión del envío de un duplicado de factura, así como la tramitación de un cambio de tarjeta SIM conlleva la superación de las políticas de seguridad que Vodafone tiene implementadas a fin de prevenir que se realicen prácticas fraudulentas sobre los datos personales de sus clientes. En este sentido, ha sido verificado que la realización de ambas gestiones se realizó superando dichas políticas de seguridad, por lo que mi representada entendió en todo momento que se trataban de gestiones lícitas, reales y veraces.

Sin embargo, en fecha 22 de enero de 2020, el reclamante interpuso una reclamación ante el servicio de atención al cliente de mi representada, alegando que se le había facilitado a un tercero un duplicado de su factura en Vodafone. Es en este momento cuando Vodafone tuvo constancia por primera vez de la supuesta suplantación de la identidad del reclamante, al entender previamente que las gestiones se habían realizado de forma lícita, veraz y leal, pues fueron superadas las Políticas en materia de seguridad.

A partir de este momento, mi representada realizó las investigaciones y gestiones oportunas, poniéndose en contacto con el reclamante en fecha 28 de enero de 2020, es decir, tan solo seis días después de tener constancia de la presunta suplantación de identidad que reclamaba el Sr. ***K.K.K.****, e informándole asimismo de las políticas de seguridad que tenía implementadas Vodafone.*

Adicionalmente, quiere mi representada señalar que ha sido verificado que ya en fecha 7 de enero de 2020, es decir, tan solo dos días después a que tuviera lugar el duplicado de la tarjeta SIM, mi representada procedió a ***(…)****.*

Dicha medida implica asimismo que (…). Asimismo, y fruto de la activación de dicho duplicado como fraude, se desactivó temporalmente la línea titularidad del Sr. ***K.K.K.*** *Mi representada, además, advirtió al reclamante que, en caso de haber tramitado un tercero dichas gestiones sin su conocimiento, era posible que tal tercero conociese de antemano los datos personales relativos a su persona.*

Sin embargo, y en vista de los hechos acontecidos, en fecha 4 de febrero de 2020, el Sr. ***K.K.K.*** *decidió de forma voluntaria desactivar la totalidad de los servicios que tenía asociados con Vodafone. De esta manera, en dicha fecha mi representada tramitó no solo la baja de la línea supuestamente afectada por la tramitación del cambio de SIM (****TELÉFONO.7****), sino la del resto de servicios asociados al reclamante (Fibra ONE 600Mb, Fijo* ****TELÉFONO.8****, y líneas móviles* ****TELÉFONO.9*** *y* ****TELÉFONO.10****) y sobre los cuales no se había gestionado un duplicado SIM.*

Por último, resulta oportuno indicar que el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, no a los datos bancarios del titular, por lo que no parece posible afirmar que exista una correlación entre las acciones efectuadas en relación con la tarjeta SIM del Sr. ***K.K.K.*** *y lo ocurrido con sus cuentas bancarias, en este caso, de la entidad ING".*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 16 de julio de 2020, en el expediente con núm. de referencia E/03065/2020.

OCTAVO: ***L.L.L.*** (en adelante, la parte reclamante siete), en fecha 17 de marzo de 2020, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

"Me suplantaron la identidad en una tienda física de VODAFONE en Girona y se apropiaron de las líneas contratadas por mí a VODAFONE. Por dichas acciones realizaron una duplicación de tarjeta SIM de la línea móvil, desembocando en un fraude económico y unas consecuencias administrativas que sigo reclamando".

Junto a la reclamación aporta la denuncia presentada por estos hechos ante la DGPN en las dependencias de ****LOCALIDAD***, con número de atestado ****ATESTADO.7*** en fecha 4 de enero de 2020; y, reclamación dirigida a VDF, de fecha 15 de enero de 2020, en la que solicita que *"(…) como quiera que en ningún momento he expresado mi consentimiento para cambiar la titularidad de mis servicios a otra persona, les requerimos para que procedan a dar explicaciones sobre los hechos relatados en el presente escrito, así como en todo caso, realicen los trámites y gestiones necesarias para hacer efectiva la activación inmediata de las líneas e indemnicen por la falta de suministro e interrupción del servicio, absteniéndose de cobrar cantidad alguna desde el pasado 4 de enero. 2º.- Que se proceda a informar a esta parte como se han producido el cambio de titularidad de mis líneas, poniendo a mi disposición la grabación de voz o documental asociada, a fin de efectuar las acciones legales oportunas. 3º.- Que se me abonen todos los gastos ocasionados por esta incidencia, para solventar los gastos injustos: compra SIM prepago y sus recargas hasta la recuperación de los servicios, uso de locutorio telefónico, reintegro del importe correspondiente en las facturas indebidamente cargadas en cuenta, e indemnización*

por los daños y perjuicios sufridos en esta VULNERACIÓN EN LA PROTECCIÓN DE DATOS Y SUPLANTACIÓN DE IDENTIDAD. (…)".

Asimismo, aporta extracto bancario de ING Direct de la cuenta corriente que comparte con su mujer donde se observa que en fecha 4 de enero de 2020 se efectúan 5 cargos fraudulentos que ascienden a un total de ***XXXX,XX*** euros y dos extractos de los cargos efectuados a través de la tarjeta de crédito que ascienden a ***XXXX,XX*** euros.

En fecha 2 de junio de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

> *"Tras analizar la reclamación e investigar lo sucedido, mi representada ha podido comprobar que, con fecha 4 de enero de 2020, se produjeron dos cambios de titularidad sobre el ID de cliente* ******ID.1****, titularidad del Sr.* ***L.L.L.*** *En primer lugar, se produjo un cambio de titularidad que asoció los datos de un tercero, D.* ***M.M.M.****, al ID* ******ID.1*** *del reclamante. Posteriormente, tuvo lugar un segundo cambio de titular que asoció el id de cliente anterior a los datos de otro tercero, D.* ***N.N.N.***
>
> *Asimismo, mi representada ha también podido verificar que en fecha 4 de enero de 2020, se tramitó un cambio de SIM sobre la línea* ******TELÉFONO.11****, asociada al ID* ******ID.1*** *anterior. Dicho cambio de SIM fue gestionado de forma presencial, a través de una tienda Vodafone ubicada en Gerona.*
>
> *Quiere esta parte señalar que la efectiva gestión de un cambio de titularidad, así como la tramitación de un cambio de tarjeta sim conllevan la superación de las políticas de seguridad que Vodafone tiene implementadas, a fin de prevenir que se realicen prácticas fraudulentas sobre los datos personales de sus clientes. En este sentido, y al haberse tramitado ambas gestiones sujetas a dicha política de seguridad, mi representada entendió en todo momento que se trataban de gestiones lícitas, reales y veraces.*
>
> *Sin embargo, y en vista de los hechos acontecidos, el mismo día 4 de enero de 2020, el Sr.* ***L.L.L.*** *se puso en contacto con mi representada, indicando que las gestiones anteriores se habían realizado, presuntamente, sin su autorización, siendo éste el primer momento en que Vodafone tuvo constancia de los hechos objeto de reclamación. Asimismo, en dicha interacción, el reclamante solicitó el bloqueo de las líneas asociadas al ID* ******ID.1*** *y puso en conocimiento de mi representada que estaba en proceso de tramitar una denuncia de los hechos ante la Policía.*
>
> *En vista de la denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado que indicaba el reclamante procedería a interponer, mi representada procedió a realizar las investigaciones y gestiones oportunas con el fin de resolver con la máxima celeridad posible la incidencia reportada por el Sr.* ***L.L.L.*** *De esta manera, en fecha 4 de enero de 2020, es decir, el mismo día en que se Vodafone fue notificada de los hechos, procedió a bloquear los servicios asociados al* ***ID ***ID.1****, restringiendo en este sentido, y como*

media primordial y principal ante un caso de duplicado de tarjeta sim, el uso de las líneas asociadas a tal id. tales bloqueos se efectuaron con el exclusivo fin de evitar que se pudiese producir un perjuicio posterior mayor al reclamante.

Asimismo, y tras efectuar los bloqueos anteriormente mencionados, el departamento de fraude de Vodafone procedió a realizar las investigaciones oportunas, a fin de verificar si lo sucedido podría tener el carácter de fraudulento y en caso afirmativo, tramitar el cambio de titularidad y de sim a favor del Sr. ***L.L.L.***

Finalmente, en fecha 22 de enero de 2020, mi representada, tras verificar que las anteriores gestiones se realizaron de forma fraudulenta, procedió a efectuar un cambio de titularidad sobre los servicios asociados al ID ******ID.1****, volviéndolos a asociar de manera exitosa al Sr.* ***L.L.L.*** *Asimismo, en fecha 23 de enero de 2020, mi representada efectuó a su vez un cambio de SIM sobre la línea* ******TELÉFONO.11*** *afectada, con el fin de invalidar la tarjeta SIM obtenida de forma fraudulenta y devolver el control de la línea al reclamante.*

Sin embargo, en fecha 23 de enero de 2020, y debido a que los servicios asociados al ID ******ID.1*** *habían sido bloqueados anteriormente por Vodafone, el cliente se puso en contacto con mi representada, manifestando que no podía realizar llamadas correctamente. En vista de lo anterior, en fecha 26 de enero de 2020, mi representada procedió, a petición del Sr.* ***L.L.L.****, a eliminar las restricciones en el uso de las líneas asociadas al ID* ******ID.1****, reestableciendo, por tanto, el uso sobre los servicios ya asociados al reclamante. (…).*

Por último, resulta asimismo oportuno indicar que el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, no a los datos bancarios del titular, por lo que no parece posible afirmar que exista una correlación entre las acciones efectuadas en relación con la tarjeta SIM del Sr. ***L.L.L.*** *y lo sucedido con sus cuentas bancarias, en este caso, pertenecientes a la entidad ING".*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 24 de julio de 2020, en el expediente con núm. de referencia E/03632/2020.

NOVENO: ***Ñ.Ñ.Ñ.*** (en adelante, la parte reclamante ocho), en fecha 30 de junio 2020, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

"El exponente, ***Ñ.Ñ.Ñ.****, con DNI* ******NIF.1****, reside en Sevilla. C/* ******DIRECCIÓN.2****. El día 2 de junio de 2020, sobre las 13 del mediodía notó que no tenía línea telefónica, cosa que no pudo solucionar hasta el día siguiente 3 de junio sobre la misma hora en que compra nueva tarjeta.*

De las averiguaciones y documentos que se acompañan se deduce:

1.- Unos desconocidos, sin estar debidamente acreditados, porque no se les exige el DNI, compran en Valencia una tarjeta telefónica a mi nombre, y celebran un contrato nuevo con Vodafone, también a mi nombre. En dicho

contrato Vodafone les proporciona mi cuenta bancaria de cargo en el Banco Santander.

2.- Con tales datos solicitan por teléfono al banco mi firma electrónica, mis datos de la tarjeta de crédito y desvalijan la cuenta titularidad del interesado en dicho banco".

Junto a su reclamación aporta una solicitud dirigida a VDF de fecha 8 de junio de 2020 en la que demanda que *"dichos hechos no se vuelvan a producir, guarden las cintas de videovigilancia de la tienda de Carrefour Valencia y, en su caso, las pongan a disposición de la policía para investigar los hechos y a indemnizar al interesado en la cantidad en la que este ha resultado perjudicado; 17.265,00 euros desaparecidos de la cuenta corriente (…)".*

Acompaña también otra reclamación dirigida a VDF vía email, en fecha 10 de junio de 2020, en la que reitera sus peticiones.

También aporta la factura emitida por VDF, de fecha 2 de junio de 2020, con el número ******FACTURA.2***, que contiene el cargo correspondiente a la emisión de una tarjeta SIM, donde especifica como dirección de entrega una sociedad denominada (…) ubicada en el municipio de******LOCALIDAD*** (Valencia), cuando el RECLAMANETE OCHO tiene su residencia habitual en el municipio de SEVILLA.

Acompaña también el Contrato de Servicio Móvil, Banda Ancha, Fijo y TV para Clientes Particulares que niega haber suscrito en el municipio de ******LOCALIDAD*** de fecha 2 de junio de 2020 y la reclamación de operaciones efectuadas mediante la tarjeta de crédito Visa/MasterCard a su nombre, dirigida al Banco Santander por las más de 20 transacciones efectuadas entre los días 2 y 4 de junio de 2020, que superan los ***XXXX,XX*** euros.

Añade, además, la queja presentada en fecha 12 de junio de 2020 ante una sucursal de VDF ubicada en Málaga por los hechos acontecidos.

En fecha 17 de julio de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

"Tras analizar la reclamación e investigar lo sucedido, Vodafone ha podido comprobar que, en fecha 2 de junio de 2020 se tramitó un cambio de SIM sobre la línea ******TELÉFONO.12****, asociada al ID de cliente* ******TELÉFONO.13****, del que es titular el reclamante. Dicho cambio de SIM fue gestionado de forma presencial, a través del Punto de Venta Vodafone operado por (…), ubicado en* ******LOCALIDAD****, Valencia.*

Quiere esta parte señalar que la efectiva tramitación de un cambio de tarjeta SIM conlleva la superación de las políticas de seguridad que Vodafone tiene implementadas a fin de prevenir que se realicen prácticas fraudulentas sobre los datos personales de sus clientes. En este sentido, y al haberse tramitado dicho cambio de SIM, tratándose dicha gestión de una operación sujeta a la superación de la política de seguridad de Vodafone, mi representada entendió en todo momento que se trataba de una gestión con la apariencia

lícita, real y veraz.

Sin perjuicio de lo anterior, en fecha 3 de junio de 2020, el reclamante se puso en contacto con mi representada, indicándole que no disponía de cobertura en su dispositivo asociada a la línea móvil ******TELÉFONO.12****, siendo este el primer momento en que Vodafone tuvo conocimiento de la incidencia objeto de reclamación. De esta manera, mi representada realizó las investigaciones y gestiones oportunas, pudiendo confirmar que la razón por la que no disponía de cobertura el reclamante se debía al cambio SIM tramitado el día anterior. En vista de lo anterior, mi representada procedió a tramitar un nuevo cambio de SIM, con el fin de anular el cambio realizado en fecha 2 de junio, restableciendo a tal efecto la línea y el control sobre la línea* ******TELÉFONO.12*** *al Sr.* ***Ñ.Ñ.Ñ.*** *en fecha 3 de junio de 2020, es decir, un día después de tener conocimiento de la incidencia objeto de reclamación y en todo caso, con anterioridad a la recepción del presente requerimiento por parte de la Agencia.*

Asimismo, mi representada también pudo verificar que, en también fecha de 2 junio de 2020, se tramitó una orden de modificación sobre los servicios asociados al ID de cliente anterior, a fin de modificar los servicios Vodafone One Fibra 50Mb + M + TV + Total + Fijo que disfrutaba el Sr. ***Ñ.Ñ.Ñ.*** *por la tarifa Vodafone One Ilimitada Total Fibra 1Gb. Además, dicha orden pretendía a su vez desactivar los servicios de Vodafone TV del reclamante. Dicha orden de modificación fue también gestionada de forma presencial, a través del Punto de Venta Vodafone operado por (…) ubicado en* ******LOCALIDAD****.*

Al igual que para la tramitación de un cambio SIM, la modificación de los servicios y tarifas activadas al ID de uno de los clientes de Vodafone conlleva la superación de las políticas de seguridad que Vodafone, a fin de prevenir que se realicen contrataciones fraudulentas sobre los datos personales de sus clientes que pudiesen originarle perjuicios económicos a los mismos por la contratación de servicios no reconocidos. En este sentido, y al haberse plasmado la orden de modificación de servicios bajo un contrato, la cual se aporta como Documento número 2, mi representada entendió en todo momento que estaba ante una gestión con la apariencia lícita, real y veraz.

Sin perjuicio de lo anterior, con motivo de la interacción entre el reclamante y mi representada de fecha 3 de junio de 2020, y debido a que la orden de modificación de servicios también se tramitó desde el mismo Punto de Venta sobre el cual se había tramitado el cambio de SIM fraudulento, mi representada procedió a interrumpir el proceso de activación de las tarifas contratadas, con el fin de evitar causarle cualquier perjuicio al Sr. ***Ñ.Ñ.Ñ.*** *(…)*

Por último, considera mi representada oportuno indicar que, el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, no a los datos bancarios del titular, por lo que no parece posible afirmar que exista una correlación entre las acciones efectuadas en relación con la tarjeta SIM del Sr. ***Ñ.Ñ.Ñ.*** *y lo ocurrido con sus cuentas bancarias".*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 28 de agosto de 2020, en el expediente con núm. de referencia E/05844/2020.

DÉCIMO: ***O.O.O.*** (en adelante, la parte reclamante nueve), en fecha 8 de junio 2020, interpone una reclamación ante la AEPD dirigida contra VDF, por los siguientes motivos:

> *"El día 7 de enero de 2020 mi terminal se queda sin línea, al estar en la oficina no le doy más importancia ya que sigo conectado al wifi, a continuación, me llega un mensaje de ING Direct para confirmar una operación que yo no he realizado, dicho mensaje lo veo cuando bajo a desayunar, por lo que al no tener línea no puedo denegar la operación. A través de otro móvil consigo contactar con Vodafone porque sospecho que me han duplicado la SIM y están haciendo operaciones fraudulentas en entidades bancarias.*
>
> *Al llamar a Vodafone me indican que yo no soy el titular de la línea, que se acaba de producir un cambio de titular (sin mi consentimiento). Les indico que es un fraude, lo marcan (o eso dicen) como tal y quedan en llamarme urgentemente. Dicha llamada nunca se produce, así que unas 8 horas después vuelvo a llamar y resulta que han vuelto a cambiar la titularidad de la cuenta a otra persona diferente...*
>
> *En resumen, sin mi consentimiento realizan un cambio de titular, me dejan sin línea 2 semanas y hacen duplicado de SIM que aprovechan para acceder a cuentas de ING Direct, pedir préstamo a mi nombre y sacar en efectivo 5 mil euros..."*

Junto a su reclamación aportó la denuncia presentada por estos hechos, en fecha 7 de enero de 2020, con número de atestado ******ATESTADO.8*** ante la DGPN en las dependencias de ******LOCALIDAD***.

Asimismo, aporta la factura número ******FACTURA.3*** emitida por VDF en esa misma fecha, que contiene el cargo correspondiente a la emisión de una tarjeta SIM, donde especifica como dirección de entrega ******DIRECCIÓN.3*** en el municipio de ******LOCALIDAD*** (GIRONA), cuando el RECLAMANTE NUEVE tiene su residencia habitual en el municipio de ******LOCALIDAD*** (LAS PALMAS).

También aporta la reclamación dirigida a VDF en fecha 8 de enero de 2020 solicitando una explicación a los dos cambios de titularidad producidos en su línea y la expedición de una tarjeta SIM, sin su consentimiento y los mensajes siguientes intercambiados con el Servicio de Atención al Cliente de VDF, en respuesta a su reclamación.

En fecha 23 de junio de 2020, se da traslado de la reclamación a VDF, para su análisis y respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, VDF manifiesta -entre otros argumentos- lo siguiente:

> *"Tras analizar la reclamación e investigar lo sucedido, Vodafone ha podido comprobar que,* ***(…).***
>
> *Asimismo, mi representada ha también podido verificar que en fecha 7 de enero de 2020 se tramitó un cambio de SIM sobre la línea* ******TELÉFONO.13****, asociada al ID* ******ID.2*** *anterior. Dicho cambio de SIM fue* ***(…)****.*

Quiere esta parte señalar que la efectiva gestión de un cambio de titularidad, así como la tramitación de un cambio de tarjeta SIM conllevan la superación de las políticas de seguridad que Vodafone tiene implementadas, a fin de prevenir que se realicen prácticas fraudulentas sobre los datos personales de sus clientes. En este sentido, y al haberse tramitado ambas gestiones sujetas a dicha política de seguridad, mi representada entendió en todo momento que se trataban de gestiones lícitas, reales y veraces.

Sin embargo, en vista de los hechos acontecidos, el mismo día 7 de enero de 2020, el reclamante se puso en contacto con mi representada, indicando que las gestiones anteriores se habían realizado supuestamente sin su autorización, siendo este el primer momento en que Vodafone tuvo conocimiento de los hechos objeto de reclamación. En este sentido, mi representada procedió a realizar las investigaciones y gestiones oportunas, a fin de resolver la incidencia acontecida y efectuar el cambio de titularidad y el cambio de SIM que devolvieran el control de tanto la línea como el ID afectado, al Sr. ***O.O.O.*** *Por ello, en fecha 9 de enero de 2020, es decir, tan solo dos días después de tener constancia de los hechos objeto de reclamación, y tras verificar que estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento, mi representada procedió a bloquear la cuenta del cliente, restringiendo el uso de los servicios asociados al ID* ******ID.2****. Tal bloqueo se efectuó con el exclusivo fin de evitar que se pudiese producir un perjuicio mayor al reclamante* ***O.O.O.*** *y desactivando a los anteriores terceros que constaron indebidamente como titular de la cuenta del reclamante. (…)*

Asimismo, en fecha 13 de enero de 2020, el reclamante efectuó, a su vez, de forma presencial en una tienda Vodafone, un cambio de SIM sobre la línea ******TELÉFONO.13*** *afectada, que permitió invalidar la anterior tarjeta SIM duplicada de forma fraudulenta, devolviendo de esta manera el control de la línea al reclamante. (…)*

Por tanto, mi representada logró solventar la incidencia objeto de reclamación de forma efectiva el 13 de enero de 2020, cuando tramitó el cambio de SIM sobre la línea móvil afectada que, junto con el cambio de titularidad efectuado el 9 de enero de 2020 sobre el ID ******ID.2****, devolvieron el control total de las líneas al Sr* ***O.O.O.*** *En este sentido, la incidencia quedó correctamente resuelta en sistemas internos de mi representada con notoria anterioridad a la recepción del presente requerimiento por parte de la Agencia.*

Por último, resulta oportuno indicar que el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, no a los datos bancarios del titular, por lo que no parece posible afirmar que exista una correlación entre las acciones efectuadas en relación con la tarjeta SIM del Sr. ***O.O.O.*** *y lo ocurrido con sus cuentas bancarias".*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 2 de septiembre de 2020, en el expediente con núm. de referencia E/05287/2020.

UNDÉCIMO: A la vista de los hechos denunciados en las distintas reclamaciones, de los documentos aportados por las partes reclamantes y de la Nota Interior acordada

por la directora de la Agencia, la SGID procede 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 57.1 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.

En el marco de las actuaciones previas de investigación se practicaron tres requerimientos de información dirigidos a VDF, en distintas fechas:

Requerimiento	Código Seguro de Verificación	Fecha requerimiento	Fecha notificación requerimiento
Primero	***CSV.1**	13/01/2020	16/01/2020
Segundo	***CSV.2**	12/06/2020	15/01/2020
Tercero	***CSV.3**	15/09/2020	16/09/2020

En el primero de los requerimientos, de fecha 13 de enero de 2020, se solicitaba la siguiente información:

1. Información sobre las vías de que disponen los clientes para solicitar un duplicado de tarjeta SIM. (Teléfono, Internet, tiendas, etc.).

2. Para cada una de las vías de que se disponga, se pide información detallada del procedimiento establecido para la atención de las solicitudes, incluyendo los controles para la verificación de la identidad del solicitante incluyendo los datos y documentos que se requieren al solicitante, así como el detalle de las verificaciones que se realizan sobre los mismos. En caso de envío de tarjeta SIM por correo, detalle de los controles y exigencias establecidas sobre la dirección de envío.

3. Instrucciones giradas al respecto al personal que atiende las solicitudes para la atención de las mismas. Documentación que acredite su difusión entre los empleados dedicados a dichas tareas, internos o externos a la entidad.

4. Información sobre si la realización de los controles para la verificación de la identidad queda reflejada, para cada solicitud atendida, en el Sistema de Información de la entidad. Documentación que lo acredite en su caso, tal como impresión de pantalla de los botones (check-box) u otra documentación según el método utilizado.

5. Motivos por los cuales ha sido posible en algunos casos la suplantación de la identidad de clientes para la emisión de duplicados de SIM. Razones por las cuales las medidas y controles de seguridad implementados no han surgido efecto.

6. Acciones emprendidas por la entidad cuando se detecta uno de estos casos. Información sobre la existencia de un procedimiento escrito y copia del mismo en caso afirmativo. Acciones emprendidas para evitar que casos de este tipo se vuelvan a producir, en concreto, cambios que se hayan podido realizar sobre el

procedimiento para mejorar la seguridad.

7. Número de casos de solicitudes fraudulentas de duplicados de SIM detectados durante todo el año 2019.

Número de clientes de telefonía móvil total de la entidad.

En el segundo de los requerimientos, de fecha 12 de junio de 2020, se solicitaba la siguiente información:

PUNTO 1. Se solicita aclaración sobre los siguientes aspectos con relación a la contestación de nuestro requerimiento de fecha 16 de enero de 2020, en el marco de este mismo expediente:

A). Al final de la manifestación PRIMERA de la contestación se menciona que únicamente es posible la tramitación (…) en tres supuestos *((…)).* Sin embargo, en el punto 2 de la manifestación TERCERA se menciona que *(…).*

Se pide copia del procedimiento por escrito donde consten todos los casos que se tramitan (…), incluyendo todos los supuestos.

Se pide copia de las instrucciones concretas dadas a los operadores con información detallada de cómo valora el operador todos los supuestos, incluyendo cómo valora o comprueba (…).

B). Con relación a los datos para la identificación del cliente que se piden durante una solicitud de duplicado (…). En la manifestación SEGUNDA se menciona que se pide "(…)", además (…). Sin embargo, en el punto 2.a) de la manifestación TERCERA se dice que se piden "(…)".

Se pide copia del procedimiento/política de seguridad donde consten claramente los datos que se solicitan según los diferentes casos, incluyendo todos los supuestos.

Se pide copia de las instrucciones concretas dadas a los operadores con información detallada de los datos que deben pedir en cada caso.

C) Sobre el proceso de solicitud (…). Copia del proceso que siguen los clientes, incluyendo los pasos que deben dar y los datos que aportan necesariamente.

D). Comprobaciones que se realizan en la entrega a domicilio de la tarjeta SIM para la identificación del destinatario. Copia de la documentación contractual con las empresas de logística/mensajería que realizan el reparto, donde consten las comprobaciones de identidad que debe realizar el repartidor.

E) Copia de los comunicados periódicos enviados a los puntos de venta, canal telefónico y al operador logístico sobre los riesgos y las políticas al respecto, mencionados en la manifestación CUARTA de su escrito de contestación.

PUNTO 2. Listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes. El listado incluirá los duplicados de SIM solicitados desde el 1 de enero de 2020, es decir, todos los reclamados que sucedieron a partir del 1 de enero, desde el primero, consecutivos hasta llegar a 20 *(se trata de casos que no han sido objeto de reclamación ante la AEPD).*

Se pide indicar en el listado la fecha, el número de línea y el canal de la solicitud.

PUNTO 3. Sobre casos presentados ante esta Agencia que se resumen en la tabla (que se da por íntegramente reproducida en este acto de trámite):

Se pide:

A. Motivo por el cual en el caso E/10004/2019 cuando el cliente llama indicando que no tiene línea no se le alerta que se le ha duplicado el SIM.

B. Motivo por el cual en los casos E/12065/2019 y E/00558/2020 no se han tenido en cuenta los recientes envíos de duplicados de SIM y se ha conseguido duplicar la SIM repetidas veces.

Procedimiento escrito o instrucciones que existan de cómo considerar posibles casos de suplantación de identidad futuros en un determinado cliente con precedentes.

C. En los casos de solicitud en tienda, copias de los DNI recabados en la solicitud de duplicado de SIM. Si no existe copia recabada, reflejo que conste en los sistemas de la solicitud y comprobación de la identidad del solicitante mediante exhibición de su DNI.

D. Para los casos de solicitud (…), información sobre si se tiene como requisito para la entrega que la ciudad donde se solicita la SIM sea la ciudad de residencia del cliente. Información sobre si existe algún control adicional en caso de ciudades distintas.

E. En los casos de solicitud (…), registro del caso (Aportando grabación de la llamada, e impresión del caso registrado en los sistemas de la entidad).

F. En los casos de solicitud (…), con envío de SIM a domicilio, justificación de los motivos por lo que se pudo entregar la SIM en una dirección diferente a la del cliente si no se permiten dichos canales con cambio de domicilio previo. Información sobre si se establecieron en las solicitudes de duplicados direcciones de entrega nuevas.

G. Acciones emprendidas por VODAFONE en cada caso, incluyendo acreditación documental de los siguientes aspectos:

- Si se ha marcado como víctima de fraude al cliente para evitar posibles intentos de suplantación de identidad futuros.
- Si se han realizado investigaciones internas para esclarecer los hechos ya sea con el punto de venta en caso de entrega en tienda, o internas en caso de canal on-line/telefónico.
- Si se ha contactado con el cliente para alertarle de lo sucedido y sobre la resolución de su caso.

En el tercero y último de los requerimientos, de fecha 15 de septiembre de 2020, se solicitaba la siguiente información:

PUNTO 1. Sobre el listado de 20 casos de duplicados de SIM denunciados/reclamados facilitados en la contestación anterior detallados (que se da por íntegramente reproducido en este acto de trámite):

Se pide, en los casos de solicitud presencial, copia de los DNIs o documentos

identificativos aportados por los solicitantes en el cambio de SIM.

En los casos de solicitudes telefónicas copia de la grabación de la conversación donde el solicitante supera la política de seguridad.

PUNTO 2. Sobre los casos presentados ante esta Agencia que se resumen en la tabla:

Se pide:

A) Caso E/3065/2020: Con relación a la llamada atendida el 5/1/2020 de una persona que solicita copia de una factura. Se pide copia de la grabación de la llamada donde se supera la política de seguridad por la persona llamante.

Copia de la factura remitida.

Copia del registro de la llamada con los comentarios del operador, así como el motivo por el cual se remite a una dirección de correo electrónico que no consta en los datos del cliente.

Copia del registro de los múltiples intentos de cambio de SIM realizados el 5/1/2020, solicitudes de PIN y PUK e intentos de compra.

Copia del registro de cambio/activación de SIM efectuado el 7/1/2020. Grabación de la llamada donde quede constancia de las comprobaciones de la identidad del solicitante (superación de la política de privacidad).

Motivo por el cual se produce el cambio de SIM después de múltiples intentos sospechosos de fraude. Motivo por el cual no se marca el cliente como fraude hasta el día 7/1/2020, y se permite el cambio de SIM.

Motivo por el cual no se alerta al cliente del cambio de SIM previo, cuando llama el 7/1/2020 al advertir que no tiene línea, indicándole por parte de VODAFONE que solicite un cambio de SIM de forma presencial.

Copia del registro de la llamada del cliente, de fecha 7/1/2020 donde el cliente comunica que se ha quedado sin línea.

B) Caso E/3632/2020: Con relación a los cambios de titularidad previos al cambio de SIM se pide copia de la grabación de las llamadas donde se supera la política de seguridad por la persona llamante.

Copia del registro de la llamada y las gestiones realizadas con los comentarios del operador para los cambios de titularidad del 4/1/2020.

Para el cambio de SIM presencial del 4/1/2020, se pide copia del DNI o documento identificativo recabado en la solicitud de duplicado de SIM.

C) Caso E/5844/2020: Para el nuevo contrato o cambio de contratación de telefonía del 2/6/2020, se pide copia del DNI o documento identificativo recabado en la contratación presencial.

Copia del nuevo contrato entregado al contratante.

Para el cambio de SIM presencial del 2/6/2020, se pide copia del DNI o documento identificativo recabado en la solicitud de duplicado de SIM.

D) Caso E/5287/2020: Con relación a los cambios de titularidad previos al cambio de SIM se pide copia de la grabación de las llamadas donde se supera la política de seguridad por la persona llamante.

Copia del registro de las llamadas y las gestiones realizadas con los comentarios del operador para los cambios de titularidad del 7/1/2020.

Copia de los registros de las llamadas realizadas por el cliente alertando de que no dispone de línea los comentarios del operador para los cambios de titularidad del 7/1/2020.

Se producen dos cambios de titularidad, llamando el cliente entre ambos dos alertando de no disponer de línea y posible cambio de SIM. Justificación que puedan aportar para que se produzca el segundo cambio de titular después de la alerta del cliente.

Motivo por el cual no se ha incluido una alerta para que no se produzcan más cambios supuestamente fraudulentos.

Para el cambio de SIM presencial del 7/1/2020, se pide copia del DNI o documento identificativo recabado en la solicitud de duplicado de SIM.

PUNTO 3. Sobre los casos en los cuales se entrega presencialmente un SIM en tienda y se activa vía telefónica, o se produce un robo de SIMs en tienda (ver casos E/12065/2019, E/00557/2020, E/00558/2020).

Se pide:

- Información sobre si es posible adquirir SIMs enviados a tienda por Vodafone sin asociarlos a ninguna línea o cliente. Causas por las que se permite que un cliente se lleve de una tienda un SIM sin activar y sin asociar a una línea determinada, y se permite posteriormente activar telefónicamente el SIM y asociar a una línea.
- Información sobre los casos, que no supongan un posible fraude de SIM swapping, en los cuales un cliente puede estar en posesión de un SIM sin haber sido asociado previamente en los sistemas de la entidad a una línea de su titularidad.
- Política de seguridad que se pasa al solicitante en la recogida del SIM cuando no se asocia a una línea o cliente durante su recogida.
- Causas por las que se permite en el procedimiento activar telefónicamente un SIM cualquiera para una línea determinada. (Caso de SIMs sustraídos en una tienda, que se encuentran sin asociar con cliente alguno o línea).

Sobre los cambios de titularidad vía telefónica se pide Política de seguridad que se pasa al solicitante. Copia de las instrucciones concretas que al respecto disponen los operadores.

DUODÉCIMO: Con fecha 23 de junio de 2020, VDF solicita una ampliación del plazo ante la imposibilidad de recabar y estructurar la información requerida en el plazo establecido.

Con fecha 29 de junio de 2020 la Subdirectora General de Inspección de Datos acuerda la ampliación del plazo por un periodo de cinco días.

DÉCIMO TERCERO: En respuesta a los tres requerimientos formulados, VDF aporta la siguiente información:

Respecto al primero de los requerimientos se especifica la información conforme a los

apartados requeridos según el orden de numeración:

1.- Información sobre las vías de que disponen los clientes:

(…).

2.- Información detallada del procedimiento:

(…).

3.- Instrucciones giradas al personal:

(…).

4.- Información sobre el registro de la información en el sistema:

(…).

5.- Motivos por los cuales ha sido posible la suplantación de la identidad de clientes:

(…).

6.- Información sobre la existencia de un procedimiento escrito:

(…).

> Con relación al procedimiento o las instrucciones existentes sobre cómo considerar posibles casos de suplantación de identidad futuros en un determinado cliente con precedentes, ***(…).*** Asimismo, ***(…)***. Han aportado copia de los comunicados enviados en el último año.

7.- Número de casos de solicitudes fraudulentas de duplicados de SIM detectados durante todo el año 2019.

(…).

Respecto al segundo de los requerimientos se especifica la información conforme a los puntos requeridos según el orden de numeración:

PUNTO 1:

A). Copia del procedimiento y de las instrucciones:

(…).

B). Copia del procedimiento o política de seguridad:

(…).

C). Sobre el proceso de solicitud vía web:

(…).

D). Copia de la documentación contractual con las empresas de logística/mensajería que realizan el reparto:

(…).

E). Copia de los comunicados periódicos enviados:

(…).

PUNTO 2: Listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes:

(…).

PUNTO 3: Sobre casos presentados ante esta Agencia:

- Expediente E/10004/2019:

  Manifiesta que tras analizar el motivo por el cual no se alertó al cliente del duplicado de la tarjeta SIM en el momento en el efectuó la llamada, han constatado que el duplicado fraudulento se realizó el día 05/08/2019 a las 20:38 horas, pero hasta las 23:08 horas el reclamante no llama a atención al cliente. ***(…).***

  Sin embargo, el reclamante ha manifestado sobre la llamada (no indica hora, pero posterior a las 21:00) que *"tras 2 minutos de espera me dicen que la línea está bien y que acuda a un distribuidor (tienda de Vodafone) para ver si se puede tratar de algún problema en la tarjeta SIM, que pueda estar dañada y que se soluciona con un cambio de la misma".* Indica así mismo que al día siguiente, dado que trabaja en una localidad en la que no hay tienda Vodafone, no pudo acudir a una tienda hasta las 18:30 horas y a las 19:04 al recuperar la línea recibe alerta de su banco de transferencia bancaria. El 07/08/2019 descubre en una sucursal de su entidad bancaria más de 25 operaciones de gasto fraudulentas.

  El duplicado se ha realizado en una tienda Vodafone en ciudad distinta a la de residencia del reclamante el día 05/08/2019 a las 20:39 horas.

  VDF indica que ***(…).***

  VDF no ha aportado ***(…).***

- Expediente E/12065/2019:

  - *El primer cambio de SIM se realiza con fecha 1/11/2019 a las 23:23:22 por canal telefónico. La petición del cambio de SIM se realiza a partir de llamada al servicio de atención al cliente desde número oculto.*

  - *El segundo con fecha 4/11/2019 6:30:23 por canal Web Mi Vodafone utilizando la tarjeta SIM* ******SIM.9****.*

  - *El tercero con fecha 12/11/2019 11:58:03 por canal Web Mi Vodafone, utilizando la tarjeta SIM* ***5***SIM.10****.*

  - ***(…).***

- Expediente E/00557/2020:

Indica que la realización de un cambio de SIM puede ser efectuado únicamente mediante la superación de las políticas de seguridad que tiene implementadas para prevenir que se realicen prácticas fraudulentas sobre los datos de sus clientes. Manifiesta que la persona infractora que suplantó la identidad del cliente a fin de conseguir realizar el cambio o duplicado de la tarjeta SIM, fue requerido ***(…).***

Indica que el infractor conocía previamente la información personal del cliente, en concreto, (…). Por ello, en tanto todos los datos fueron facilitados de manera correcta a través del Servicio de Atención al Cliente, para Vodafone la persona que estaba solicitando el cambio de SIM era el correcto titular, no pudiendo de ningún modo advertir de que dicha persona era un infractor que estaba suplantando su identidad.

También indica que, tras realizar las investigaciones oportunas, se comprobó que, en fecha 28 de septiembre de 2019, tras recibir las llamadas a las que hace referencia en la reclamación, desde el departamento de fraude de Vodafone se estudió con detenimiento lo ocurrido, y este caso ***(…).***

También indica sobre este caso que el 28/09/2019 21:03:16 desde el departamento de fraude se detecta el cambio de SIM y se aplica desactivación temporal a la línea a fin de que no pueda ser utilizada para realizar llamadas o transacciones. Se contacta con cliente con fecha 28/09/2019 donde se confirma que dicho cliente no ha realizado ninguna modificación, pero indica que no puede atender más la llamada.

(…).

De forma previa al cambio de SIM realizado vía telefónica, se envía a distribuidor.

(…).

- Expediente E/00558/2020:

Ha indicado que según la información que consta en sus sistemas se puede comprobar que los intentos de duplicados de SIM fueron cancelados y no tramitados al completo desde el momento en el que se tuvo constancia de la comisión del fraude. Aportan impresión de pantalla indicando que *"el día 12/11/2019 se lleva a cabo un duplicado fraudulento de tarjeta SIM y el día 14/11/2019 se produce un intento desde el canal On-line, pero las ordenes aparecen canceladas"* (se refieren a las órdenes del día 14/11/2019, que son dos). Vodafone ha indicado para otro caso que *"cuando una orden se completa el estado aparece como cerrada*". En el pantallazo aportado, la orden de 12/11/2019 aparece como cerrada, y las órdenes de fecha 14/11/2019 aparecen canceladas.

El cambio de SIM del día 12/11/2019 se realizó (…) y el del 14/11/2019 vía (…). Informa que *"dado que el primer cambio de SIM es realizado por (…) se traslada con fecha 19/11/2019 información a responsable de atención al cliente para que refuercen la política de seguridad y revisen las acciones con el agente/agencia."*

Asimismo, indica que con fecha 05/12/2019 a petición del departamento de fraude "*se cerró la opción de (…)".*

Informa que analizada la procedencia de las tarjetas SIM, las dos proceden del

mismo lote de 100 tarjetas remitidas a un distribuidor. Se solicitó información y la documentación al distribuidor en cuestión para que acreditara a quien se le había entregado la tarjeta SIM. El distribuidor confirma que no dispone de la documentación.

- Expediente E/00559/2020:

VDF no ha aportado copia del DNI del solicitante, alegando que se solicitó a la tienda el documento aportado para la recogida de la tarjeta SIM y que disponían de dicho documento, que estaba manipulado. Indican que no se penalizó al distribuidor ya que cumple con las directrices marcadas por Vodafone ante estos casos.

Respecto al tercero de los requerimientos se especifica la información conforme a los puntos requeridos según el orden de numeración:

PUNTO 1: *(se trata de casos que no han sido objeto de reclamación ante la AEPD).*

- Copia de los DNIs, respecto a lo cual se verifica lo siguiente:

  (…).

- En las solicitudes telefónicas, copia de las grabaciones de la conversación:

  (…).

PUNTO 2:

- Expediente E/03065/2020 respecto al cual manifiesta lo siguiente:

  Indican que la grabación de la llamada no se lleva a cabo en todas las interacciones que se realizan con llamantes clientes o personas interesadas en los productos de Vodafone, dado que no es estrictamente necesario para el buen desarrollo de la prestación de los servicios de atención al cliente, como sería el caso. Indican que (…).

  (…).

  Indican que estas interacciones no solamente se identificaban por el llamante como cambio de SIM, sino que se enmascaraban dentro de otras solicitudes de soporte, dificultando la determinación de dichas acciones como fraudulentas, máxime cuando el servicio de atención al cliente fue provisto por diferentes operadores.

  Indican que no es posible recabar las grabaciones de las llamadas efectuadas para el cambio de las tarjetas SIM dado que el plazo de conservación de esta ha expirado. Consta la interacción realizada por el llamante en la que se muestra la apreciación del operador de superación de la política de seguridad “pol. Ok cliente solicita cambio de SIM que ha recibido”.

  Han indicado que los diferentes intentos de obtener el cambio de SIM se identifican ante el servicio de atención al cliente bajo distintas incidencias, resultando la identificación de estas conductas fraudulentas más complejas, máxime cuan-

do el llamante supera la política de seguridad.

(…).

Manifiestan que en el momento en el que el cliente advierte que no tiene línea, su representada no tiene constancia de que se haya producido previamente una conducta fraudulenta ya que, cuando se efectúa el cambio de SIM, se supera la política de seguridad.

(…). Al persistir esta incidencia, se le indica al cliente que haga el duplicado de SIM. Es después de estas interacciones, el día 7 de enero de 2020, cuando el departamento de fraude de Vodafone identifica que el cliente es víctima de una conducta fraudulenta, momento en el manifiestan que se inicia todo el proceso pertinente para solventar esta situación.

También indican (el 9 de enero de 2020) que el propio cliente se pone en contacto con atención al cliente manifestando que quiere solicitar una doble clave de seguridad debido a que estaban intentando suplantar su identidad. En ese momento, VDF informa al cliente que no existe la posibilidad de una doble clave, por lo que se determina con el cliente modificar la que tiene. Manifiestan que esta interacción evidencia que VDF actuó con la máxima diligencia posible.

Respecto a la copia del registro de la llamada del cliente, se verifica que consta en la interacción con el cliente como solución a la incidencia *"se le indica hacer duplicado de la tarjeta".*

- Expediente E/03632/2020:

VDF no aporta dichas grabaciones manifestando que no es posible aportar la grabación de la llamada dadas las limitaciones de almacenaje de los sistemas al producirse millones de llamadas al servicio de atención al cliente que generarían un alto volumen de grabaciones a ser custodiadas, y que la superación de la política de seguridad es un procedimiento intrínseco al servicio de atención al cliente que todos los operadores pasan antes de proporcionar cualquier información.

Aportan impresión de las pantallas constando como notas del operador únicamente ***"(…)"*** para el primer cambio (se cambia dos veces consecutivas el mismo día, cancelando el primero) y *"confirmo cambio de titular de* ******TELÉFONO.11****"* para el segundo cambio.

Consta interacción por llamada del cliente del mismo día en la que el reclamante manifiesta que él no ha solicitado cambio de titular ni cambio de SIM.

VDF ha aportado copia del DNI aportado por el solicitante (el nuevo titular). La copia del DNI aportada se observa incompleta, estando el DNI troceado y faltando un pequeño trozo de este.

- Expediente E/05844/2020:

VDF manifiesta que no es posible aportar dicho documento al ser los puntos de venta los que realizan la verificación y copia de los DNI para llevar a cabo la contratación presencial. Son los propios puntos de venta quienes custodian las copias de los DNI y los ponen a disposición de VDF. En el presente caso, indican que han verificado que se gestionó en una tienda de ***(…).***

Aportan copia de un contrato en formato PDF sin firmar en el que constan los datos del reclamante y su número de DNI, de fecha el 02/06/2020, dando de baja determinados servicios. Constan los datos del nuevo cliente y una cuenta bancaria que coincide con la del reclamante. El documento se encuentra suscrito digitalmente por el nuevo cliente, pero no por el antiguo, la parte reclamante ocho.

Indican que no es posible aportar copia del DNI al ser los puntos de venta presenciales los que realizan la verificación y copia de los DNIs para llevar a cabo el duplicado de SIM. Son los propios puntos de venta quienes custodian las copias de los DNIs y los ponen a disposición de VDF. En el presente caso, indican que ***(…).***

Sí aportan impresiones de pantalla que reflejan la gestión en relación con el duplicado de SIM. Indican que las impresiones de pantalla muestran las diferentes interacciones efectuadas en las que se plasma la firma digital del solicitante y la orden de cambio de SIM. Se observa que en las pantallas aparece el nombre del nuevo titular.

- Expediente E/05287/2020:

VDF no aporta dichas grabaciones manifestando que no es posible aportar la grabación de la llamada dadas las limitaciones de almacenaje de los sistemas al producirse millones de llamadas al servicio de atención al cliente que generarían un alto volumen de grabaciones a ser custodiadas, y que la superación de la política de seguridad es un procedimiento intrínseco al servicio de atención al cliente que todos los operadores pasan antes de proporcionar cualquier información.

Los representantes de VODAFONE aportan impresiones de pantalla que reflejan interacciones que se listan por orden sucesivo en el tiempo (ver número interacción):

- Interacción ******INTERACCIÓN.1***: se realiza el cambio de titular.

- Interacción ******INTERACCIÓN.2***: se informa del cambio de titular producido.

- Interacción ******INTERACCIÓN.3***: el titular pregunta sobre el cambio producido y desea cancelarlo.

- Interacción ******INTERACCIÓN.4***: se ayuda al cliente a atender su petición.

- Interacción ******INTERACCIÓN.5***: el cliente llama informando sobre la presunta suplantación de identidad.

- Interacción ******INTERACCIÓN.6***: nueva solicitud de cambio de titular, modi-

ficación únicamente la persona titular.

- Interacción ******INTERACCIÓN.7***: se confirma el cambio de titular:
- Interacción ******INTERACCIÓN.8***: se abre la petición de fraude

Alega que después del primer cambio de titularidad, el cliente, se pone en contacto con atención al cliente para informar de que está teniendo problemas con su línea y, posteriormente, se identifica que puede ser una acción de fraude. Indican que durante el tiempo en que VDF llevó a cabo las acciones pertinentes para determinar la existencia de un supuesto de fraude, se producen diversas interacciones entre Vodafone y los distintos implicados, todas ellas con la apariencia de veraces que se les presume por pasar la política de seguridad.

En ninguna interacción se refleja que se haya pasado o no se haya pasado la política de seguridad.

Manifiestan que, durante el mismo día 7 de enero de 2020, VDF lleva a cabo las acciones pertinentes para proteger los intereses del cliente, bloqueando las líneas hasta que el departamento de fraude de Vodafone determinase las acciones a desarrollar. No se refleja en las pantallas.

(…).

Aporta copia del DNI aportado por el solicitante (del nuevo titular). La copia del DNI aportada se observa incompleta, estando el DNI troceado y faltando un trozo de este. Se observa también que es el mismo DNI que para la parte reclamante siete.

PUNTO 3

- Información sobre si es posible adquirir SIMs (…);

(…).

- Información sobre los casos (…):

(…).

- Política de seguridad que se pasa al solicitante en la recogida del SIM (…);

(…).

- Causas por las que se permite en el procedimiento activar telefónicamente un SIM ***(…)***:

(…).

- Sobre los cambios de titularidad vía telefónica ***(…)***:

(…).

DÉCIMO CUARTO: Con fecha 27 de agosto de 2020, se obtiene información de la Comisión Nacional de los Mercados y la Competencia sobre las líneas de telefonía móvil de voz por tipo de contrato y por segmento siendo los resultados:

OPERADOR	PREPAGO		POSPAGO	
	Residencial	Negocios	Residencial	Negocios
VODAFONE	2.066.349	0	6.867.903	3.487.812

DÉCIMO QUINTO: Con fecha 25 de enero de 2021, se obtiene información comercial sobre el volumen de ventas de VDF durante el año 2019 siendo los resultados de 3.635.853.000 euros. El capital social asciende a 439.110.908,20 euros.

DÉCIMO SEXTO: Con fecha 8 de febrero de 2021**,** la directora de la AEPD acuerda iniciar un procedimiento sancionador contra VDF, 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 presunta infracción del artículo 5.1.f) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1.a) de la LOPDGDD.

El Acuerdo de inicio se notifica a VDF, en fecha 10 de febrero de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

DÉCIMO SÉPTIMO: Con fecha 11 de febrero de 2021, VDF presenta un escrito a través del cual solicita la ampliación del plazo para aducir alegaciones y aportar documentos u otros elementos de juicio, y además, la remisión del expediente sancionador.

DÉCIMO OCTAVO: Con fecha 17 de febrero de 2021, el órgano instructor acuerda la ampliación de plazo instada hasta un máximo de cinco días, así como la remisión de la copia del expediente, de acuerdo con lo dispuesto en los artículos 32.1 y 53.1 a) de la LPACAP.

El Acuerdo de ampliación se notifica en fecha 22 de febrero de 2021.

DÉCIMO NOVENO: Con fecha 3 de marzo de 2021, se recibe en esta Agencia, en tiempo y forma, escrito del abogado y representante de VDF, por el que se procede a formular alegaciones y en el que, tras manifestar lo que a su derecho convenía, termina solicitando el sobreseimiento del expediente con el consiguiente archivo de las actuaciones al no haberse cometido ninguna de las infracciones imputadas y subsidiariamente, en caso de imponerse una sanción, la imposición de una cuantía mínima, a la luz de las circunstancias atenuantes alegadas.

En síntesis manifiesta que:

> 1.- VDF no había infringido los artículos 5.1.f) y 5.2 del RGPD, ya que había aplicado las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
>
> 2.- No existía culpa en las infracciones imputadas y en consecuencia, no podía

imponerse sanción alguna.

3.- En el caso de que se entendiera de que procedía imponer una sanción, deberían tenerse en cuenta las circunstancias atenuantes.

4.- Enumeraba las pruebas de las que pretender valerse.

VDF alegó los siguientes argumentos:

Primera.- La adopción de medidas técnicas y organizativas no es una obligación absoluta. VDF ha cumplido con el principio de integridad y confidencialidad y con la obligación de adoptar medidas técnicas y organizativas adecuadas.

I.- Invoca las Sentencias de la Audiencia Nacional (en lo sucesivo, SAN) (Sala de lo Contencioso Administrativo, en adelante, SCA) de 25 de febrero de 2010 [JUR 2010/82723] y de 10 de noviembre de 2017 [JUR 2018/3170]) (…). Así pues, el hecho de que un tercero haya superado dichas medidas no implica, per se, haber incumplido la obligación o, en su caso, el principio de integridad y confidencialidad. El responsable del tratamiento está sujeto a una obligación de medios, no a una obligación de resultado en el sentido de entender que todo incidente es un incumplimiento del deber de "garantizar un nivel de seguridad adecuado al riesgo" (artículo 32 del RGPD).

II.- VDF es responsable de adoptar medidas técnicas y organizativas dirigidas a que los duplicados de tarjetas SIM sean facilitados a los titulares de las líneas telefónicas. En este sentido, las siguientes conductas caen fuera de la esfera de control de VDF:

1.- Las conductas realizadas por el estafador o ciberdelincuente en un estadio anterior a la solicitud del duplicado de la tarjeta SIM:

(…).

2.- Las conductas realizadas por el estafador o ciberdelincuente en un estadio posterior a la solicitud del duplicado de la tarjeta SIM, como por ejemplo el acceso a las aplicaciones de banca online de las víctimas y la realización de operaciones fraudulentas a través de dichas aplicaciones.

Remite a los folios 291 y siguientes del expediente donde el BBVA pone de manifiesto que no es suficiente con introducir la clave única que BBVA remite a través de SMS al teléfono validado por el cliente, sino que además será necesario que el defraudador acceda a la aplicación de BBVA mediante un usuario y contraseña. Hace referencia a varias técnicas de phishing utilizadas por los defraudadores como el envío masivo de correos suplantando al BBVA, llamadas aleatorias, o enlaces a través de SMS. Solo cuando los estafadores consiguen el usuario y la clave para acceder a las cuentas de los clientes, entonces y sólo entonces, el defraudador, mediante el duplicado de la tarjeta SIM, puede tener acceso a las cuentas de los afectados. Por tanto, el duplicado frau-

dulento de la tarjeta SIM no es una actuación necesaria (hay entidades bancarias. que no envían SMS con sus claves únicas) ni suficiente (se requiere el acceso a otros datos y claves) para lograr acceder a las cuentas de los sujetos afectados.

Aclaran que con lo anterior VDF no quiere tratar de distraer responsabilidades o culpar a terceros, sino simplemente centrar el objeto de debate. A VDF podrán achacársele infracciones sólo respecto de aquellas medidas de seguridad de las que sea responsable, esto es, aquellas dirigidas a garantizar que el solicitante del duplicado de la tarjeta SIM es el titular de la línea; no están (ni pueden estar) dirigidas a evitar la suplantación de identidad (falsificación del DNI, por ejemplo) ni a evitar el acceso a las cuentas bancarias. a través de la aplicación de la entidad de crédito en cuestión.

III.- Medidas técnicas y organizativas adoptadas por VDF:

Diferencia dos supuestos:

(...).

En suma, alega que no sólo implementó las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sino que ha velado por que estas medidas se mantuvieran actualizadas en todo momento, saliendo el paso de las actividades delictivas realizadas por los estafadores y ciberdelincuentes y tratando de evitar que terceros obtengan duplicados de tarjetas SIM de forma fraudulenta.

V.- Las medidas técnicas y organizativas implementadas por VDF son efectivas y adecuadas para garantizar un nivel de seguridad adecuado al riesgo:

1. El porcentaje de clientes que se ha visto afectado por un cambio de tarjeta SIM fraudulento es de un ***X,XXX*** %; y

2. El porcentaje de cambios de tarjeta SIM fraudulentos comparado con la totalidad de cambios de tarjeta SIM realizado sobre el sector de clientes particulares es de un ***X,XXX*** %.

VI.- Estamos ante un tercero cuyo propósito es, mediante una actividad delictiva, superar dichas medidas de seguridad.

El acceso a los datos personales de los interesados (tarjeta SIM) se produce mediante una actividad delictiva debidamente organizada y planeada. No estamos ante un fallo o error del sistema implementado por VDF. Hay que tener en cuenta la capacidad de estas organizaciones criminales para adaptarse a las nuevas realidades e ir mejorando sus métodos para cometer los fraudes en cuestión. En este sentido, VDF ha ido modificando su política de seguridad para tratar de anticiparse a nuevos métodos criminales, si bien, dichas organizaciones van evolucionando e implementando nuevas formas de actuación con el fin de superar la seguridad de las operadoras, lo que hace que sea imposible una anticipa-

ción a la actividad criminal en todos los casos.

VII.- Sobre los supuestos aspectos que VDF no habría acreditado:

- Identidad de los solicitantes de los duplicados de las tarjetas SIM, en los cambios de titularidad de la línea o en los solicitantes de las copias de las facturas:

  VDF no ha probado la identidad de los estafadores y ciberdelincuentes porque precisamente estos sujetos han ocultado su verdadera identidad y se han hecho pasar por los clientes de VDF, superando mediante técnicas ilícitas las políticas de seguridad. Pretender que pruebe la identidad de los solicitantes supone una suerte de prueba diabólica que no se puede exigir a VDF.

- Las grabaciones de las llamadas telefónicas amparándose en que los plazos de conservación han expirado, cuando nos encontramos ante un total de ***XXX*** fraudulentos declarados en el ejercicio 2019:

- La Agencia no ha solicitado copia de las grabaciones de las llamadas telefónicas de los ***XXX*** casos fraudulentos declarados en 2019 por VDF, sino de los 9 casos que dieron lugar al Acuerdo de Inicio (folio 414 del expediente) y de los 20 casos reportados por VDF (folio 787 del expediente). Sentado lo anterior, no ha sido posible aportar las grabaciones de las llamadas pues, por motivos logísticos, el tiempo durante el cual se almacenan las grabaciones de dichas llamadas es de un mes, lo cual además es conforme con el principio de limitación del plazo de conservación (artículo 5.1 e) del RGPD).

- El motivo por el cual se ha remitido el duplicado de la tarjeta SIM a una ciudad distinta a la de la residencia de los abonados sin controles o garantías adicionales" (Reclamantes 1, 8 y 9):

  Para la parte reclamante uno, el cambio de tarjeta SIM se realizó en tienda por un comercial del distribuidor ***LOCALIDAD.3 CC Llobregat (folio 616 del expediente); y para la parte reclamante ocho, se realizó en una tienda de un distribuidor VDF ubicada en un centro Carrefour en Valencia (folio 878 del expediente). Por lo que se refiere a la parte reclamante nueve, tal y como se pone de manifiesto en los folios 881 y siguientes del expediente, no se llegó a remitir un duplicado de la tarjeta SIM al estafador.

- La efectividad del check "víctima de fraude":

  Para la parte reclamante dos, tal y como se desprende de los folios 603 y 604 de las actuaciones, se realizó un primer duplicado fraudulento de la tarjeta SIM el 1 de noviembre de 2019, resultando infructuosos los posteriores intentos de duplicado fraudulento (días 4 y 5 de noviembre de 2019) por haber sido marcado el cliente como "víctima de fraude.

  Para la parte reclamante cuatro, tal y como se desprende del folio 605 de las actuaciones, se realizó un primer duplicado fraudulento de la tar-

jeta SIM el 12 de noviembre de 2019, resultando infructuoso el posterior intento de duplicado fraudulento (de 14 de noviembre de 2019) por haber sido marcado como "víctima de fraude".

- La efectividad del procedimiento de activación telefónica después de la recogida de la tarjeta SIM de forma presencial:

  (…).

- La efectividad de la atención multicanal que establece la vía presencial como canal prioritario para la solicitud de los duplicados de SIM, indicando a los gestores que atienden las llamadas que deriven a tienda a los solicitantes que solicitan el duplicado vía telefónica ***(…)***:

  (…).

Segunda.- Subsidiariamente, y para el caso de que la Agencia entendiera que VDF ha infringido los artículos 5.1 f) y 5.2 del RGPD, no puede apreciarse la existencia de culpabilidad en las infracciones imputadas y, en consecuencia, no puede imponerse sanción alguna.

I.- VDF no ha actuado culposamente, por lo que no procede la imposición de sanción alguna.

El artículo 28.1 de la Ley 40/2015, de 1 de octubre, regula el principio de culpabilidad. Siguiendo con la interpretación realizada por el Tribunal Supremo, para la exculpación no bastará la invocación de la ausencia de culpa, sino que será preciso que se haya empleado la diligencia que era exigible por quien aduce su inexistencia (entre otras, la Sentencia del Tribunal Supremo de 23 de enero de 1998 [RJ 1998\601]).

Asimismo, la Audiencia Nacional ha entendido, en casos similares al presente, en los que un tercero ha accedido, mediante actividades delictivas, a datos de los interesados custodiados por un responsable del tratamiento, que imputar tales hechos al responsable del tratamiento podría conllevar la vulneración del principio de culpabilidad. A título de ejemplo, la SAN (SCA, Sección 1ª) de 25 de febrero de 2010 [JUR 2010/82723].

"Así, aun cuando el artículo 9 de la LOPD establece una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, tal obligación no es absoluta y no puede abarcar un supuesto como el analizado. En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www.portalatino.com, descargándose una copia de la misma. Y, tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad". (el subrayado es de VDF).

En ningún caso el duplicado de las tarjetas SIM de determinados clientes puede suponer la consideración de que VDF ha obrado culposamente. En efecto, todas las actuaciones de la misma han ido siempre dirigidas al establecimiento y supervisión de medidas técnicas y organizativas tendentes a garantizar la seguridad de los datos personales de sus clientes: diseño de políticas de seguridad que son seguidas por el servicio postventa y son apropiadas para garantizar un nivel de seguridad adecuado al riesgo" ya que "sólo" un ***X,XXX*** % de los clientes han sido víctimas de este tipo de actuación criminal; actualización de las medidas de seguridad -desde el 30 de mayo de 2019 fija la obligatoriedad de realizar y guardar una copia del DNI del solicitante- y ha enviado multitud de comunicados y alertas a sus tiendas; en aquellos casos en que la actividad del estafador consigue defraudar el sistema implementado por VDF, ha reaccionado dirigiendo sus acciones hacia 4 frentes:

.- el cliente: bloqueando la tarjeta SIM y restringiendo la recepción de SMS, contacto y abono de las llamadas operadas por el estafador

.- a los agentes y empleados: enviando comunicaciones periódicas con alertas y aplicando penalizaciones

.- con las Fuerzas y Cuerpos de Seguridad del Estado: colaborando en la lucha contra este fraude

.-a terceros: como entidades de crédito desarrollando futuras herramientas como ***(...).***

En consecuencia, ha actuado con la diligencia debida que es exigible y conforme dispone el derecho sancionador, no procede la imposición de sanción alguna.

II.- En cualquier caso, las suplantaciones de identidad de los afectados son debidas a la existencia de errores humanos, que son inevitables y sobre los que VDF no puede tener un control efectivo:

En estos supuestos (residuales), estaríamos ante errores humanos en los que el estafador o ciberdelincuente, valiéndose de artimañas y utilizando a su favor su experiencia criminal, ha logrado burlar las políticas de seguridad, provocando el error humano del servicio postventa.

La Agencia se ha pronunciado en numerosas ocasiones sobre los errores humanos, destacando que los mismos no pueden ser castigados. Por ejemplo, en el Procedimiento Sancionador PS/00210/2019 y en el Procedimiento E/ 02877/2019, en los que se citó la SAN (SCA, Sección 1ª) de 23 de diciembre de 2013 [JUR 2014\15015]: *"La cuestión, pues, ha de resolverse conforme a los principios propios del derecho punitivo dado que el mero error humano no puede dar lugar, por sí mismo (y sobre todo cuando se produce con carácter aislado), a la atribución de consecuencias sancionadoras; pues, de hacerse así, se incurriría en un sistema de responsabilidad objetiva vedado por nuestro orden constitucional".*

Tercera.- Subsidiariamente, y para el caso de que la Agencia entienda que ha exis-

tido infracción y deba imponerse una sanción, deberán tenerse en cuenta las siguientes circunstancias agravantes y atenuantes:

VDF discrepa respetuosamente de los agravantes listados en el Acuerdo de Inicio:

La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, el 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:

I. Naturaleza, gravedad y duración de la infracción:

El único dato personal sobre el que se pierde la disposición (de forma temporal, hasta que la nueva SIM es bloqueada) es la línea telefónica. La pérdida de disposición y control sobre otros datos personales (como el nombre, apellidos, DNI, dirección, datos bancarios) se produce:

(i) bien en un momento anterior a la participación de VDF (por ejemplo, relajación de la conducta humana en la facilitación de ciertos datos a desconocidos, que los obtienen mediante prácticas de phishing o "ingeniería social").

(ii) bien en un momento posterior a su participación (por ejemplo, utilización de SMS para el envío de claves de acceso a la banca electrónica), por lo que no se le pueden achacar.

Los hechos acontecen en un periodo inferior a un año, no superior como señala la Agencia.

La naturaleza de los hechos hace muy difícil -casi imposible- erradicar por completo estas prácticas, por lo que el elemento temporal no podrá ser tenido en cuenta como agravante, más aún cuando VDF ha implementado una política de seguridad dirigida a prevenir este tipo de conductas.

- Número de interesados afectados:

El porcentaje de clientes que se ha visto afectado por un cambio fraudulento de tarjeta SIM es de un ***X,XXX*** %, y que el porcentaje de cambios de tarjeta fraudulentos comparado con la totalidad de cambios de tarjeta SIM realizados sobre el sector de clientes particulares es de un ***X,XXX*** %, por lo que entendemos que el número de interesados afectados no es alto si lo comparamos con el número de potenciales afectados.

- Nivel de los daños y perjuicios sufridos:

La Agencia destaca que mediante el control de la línea del abonado se puede tener acceso a los "*SMS dirigidos al legítimo abonado para realizar operaciones on-line con entidades bancarias suplantando su identidad".* En este sentido, el sistema de verificación de identidad empleado por una entidad bancaria (por ejemplo, el envío de SMS con claves de acceso) responde a la voluntad de

la entidad de crédito y del usuario, no de VDF. En otras palabras, el riesgo viene generado por la entidad de crédito al utilizar este sistema de verificación de la identidad del interesado, no por VDF.

Asimismo, otro elemento a tener en cuenta es que la entidad bancaria reintegra los importes defraudados a la víctima del fraude, tal y como destaca el BBVA en la respuesta a la solicitud de información de la Agencia obrante en el folio 292 del expediente: *"[...] devolviéndole los importes de las operaciones fraudulentas así como las comisiones generadas".*

II. La intencionalidad o negligencia en la infracción:

Queda por completo descartada. VDF sí ha asegurado un procedimiento que garantice la protección de los datos personales de sus clientes (esto es, su tarjeta SIM). Buena muestra de ello es que sólo un ***X,XXX*** % de los clientes se han visto afectados por esta estafa y además, ha llevado a cabo acciones tendentes a mantener dicha política de seguridad actualizada.

III. Cualquier medida tomada por el responsable del tratamiento para paliar los daños y perjuicios sufridos por los interesados:

(…).

IV. El grado de responsabilidad, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32 del RGP: ha implementado medidas técnicas y organizativas adecuadas para el riesgo generado, esto es, tendentes a asegurar que quien solicita el duplicado o cambio de una tarjeta SIM es el titular de la línea.

V. Toda infracción anterior cometida por el responsable del tratamiento: Hasta la fecha, VDF no sido sancionada por infracción de los artículos 5.1 f) y 5.2 del RGPD en relación con hechos similares, circunstancia que también deberá ser tenida en cuenta para modular la sanción a la baja.

VI. 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: el grado de cooperación con la Agencia ha sido alto.

VII. Las categorías de los datos personales afectados por la infracción: Alegan que los datos personales afectados no pueden ser considerados como circunstancia agravante. La Agencia incurre en un error de apreciación, en la medida en que la suplantación de identidad es previa a la expedición del duplicado de tarjeta SIM. La superación de las políticas de seguridad, puede ser un medio usado junto a otros, para burlar los controles de identidad implementados por otros operadores económicos, pero nada tiene que ver con la actividad respecto de la que es exigible a VDF en la adopción de medidas de seguridad adecuadas. De hecho, dependerá de los sistemas de seguridad implementados por las entidades bancarias. el hecho de que el defraudador pueda o no acceder a las cuentas del afectado, no pudiendo responsabilizarse a VDF de la falta de robustez del sistema de seguridad de un tercero (la entidad bancaria).

VIII. Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción: La actividad criminal también ha supuesto un perjuicio reputacional para VDF y una defraudación de sus políticas de seguridad.

IX. El carácter continuado de la infracción: Se postula a favor del criterio de la Agencia que considera que estas infracciones no tienen carácter continuado.

Cuarta.- Prueba que esta parte estima conveniente proponer:

(…).

VIGÉSIMO: Con fecha 14 de abril de 2021, tras comprobarse que no constaba adjunta parte de la documentación que señalaba haber aportado, se requiere a VDF para que en el plazo de 10 días a partir del siguiente a su notificación, aportase los siguientes documentos:

(…).

Dicho requerimiento fue notificado en fecha 19 de abril de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

VIGÉSIMO PRIMERO: En respuesta a dicho requerimiento de información, con fecha 29 de abril de 2021, VDF remite la documentación solicitada.

VIGÉSIMO SEGUNDO: Con fecha 30 de abril de 2021, la instructora del procedimiento acuerda la apertura de un período de práctica de pruebas en los siguientes términos:

*"Se dan por reproducidas a efectos probatorios las reclamaciones interpuestas por **A.A.A.; B.B.B.; C.C.C.; F.F.F.; G.G.G.; K.K.K.; L.L.L.; Ñ.Ñ.Ñ.;** y **O.O.O.**, y su documentación. Los documentos obtenidos y generados por los Servicios de Inspección ante VODAFONE ESPAÑA, S.A.U, y el Informe de actuaciones previas de Inspección que forman parte del expediente E/11418/2019. 2. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio PS/ 00001/2021 presentadas por VODAFONE ESPAÑA, S.A.U., en fecha 3 de marzo de 2021 y 29 de abril de 2021 y la documentación que a ellas acompaña:*

- *Documento 1, (…).*
- *Documento 2, (…).*
- *Documento 3, (…).*
- *Documento 4, (…).*
- *Documento 5, (…).*
- *Documento 6, (…).*

· *Documento 7, (…).”*

VIGÉSIMO TERCERO: Con fecha 28 julio de 2021, la instructora del procedimiento formula Propuesta de Resolución, en la que propone que por la directora de la AEPD se sancione a **VODAFONE ESPAÑA, S.A.U.**, con CIF A80907397, por infracción del artículo 5.1.f) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1.a) de la LOPDGDD, con una multa administrativa de 4.000.000’00 (cuatro millones de euros).

Con fecha 2 de agosto de 2021 a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, se notifica la Propuesta de Resolución.

VIGÉSIMO CUARTO: Con fecha 5 de agosto de 2021, VDF solicita la ampliación del plazo para formular alegaciones a la Propuesta de resolución.

VIGÉSIMO QUINTO: Con fecha 9 de agosto de 2021, la Agencia concede la ampliación instada.

VIGÉSIMO SEXTO: Con fecha 23 de agosto de 2021, se recibe en esta Agencia, en tiempo y forma, escrito del abogado y representante de VDF, por el que se procede a formular alegaciones a la Propuesta de Resolución y en el que, tras manifestar lo que a su derecho convenía, termina solicitando, como hacía en las alegaciones al Acuerdo de inicio, el sobreseimiento del expediente con el consiguiente archivo de las actuaciones al no haberse cometido ninguna de las infracciones imputadas y subsidiariamente, en caso de imponerse una sanción, la imposición de una cuantía mínima, a la luz de las circunstancias atenuantes alegadas.

Como alegación previa VDF señala que la Propuesta de Resolución propone la imposición de una multa de 4.000.000’00 a VDF por una presunta infracción de los artículo 5.1.f) y 5.2 del RGPD, infracción tipificada como muy grave el artículo 83.5.a) del RGPD y por el artículo 72.1 de la LOPDGDD, porque VDF habría vulnerado los principios de integridad y confidencialidad y de responsabilidad proactiva, al facilitar duplicados de tarjeta SIM a personas que no son las titulares de las líneas móviles, tras la superación por estos terceros de las políticas de seguridad implementadas por VDF.

Asimismo, manifiesta que el expediente sancionador tiene su origen en nueve reclamaciones presentadas ante la Agencia, si bien ésta no sólo ha tenido en cuenta los hechos concretos y especificidades acaecidos en esos casos, sino que ha enjuiciado las medidas de seguridad adoptadas por VDF con carácter general.

A continuación, y, sin perjuicio de que VDF se remite en su integridad a las alegaciones presentadas en fecha 3 de marzo de 2021 al Acuerdo de inicio, manifiesta que:

1). El objeto del presente procedimiento debe limitarse a determinar si VDF ha adoptado las medidas de técnicas y organizativas adecuadas para evitar, en la medida de lo posible, que se expidan duplicados de tarjetas SIM a sujetos que no son los titulares de las líneas móviles. El enjuiciamiento no puede extenderse a las actuaciones anteriores y posteriores llevadas a cabo por los ciberdelincuentes. A esta cuestión de-

dica la alegación primera.

VDF enfatiza que el presente procedimiento debe dirigirse única y exclusivamente a analizar si las medidas técnicas y organizativas adoptadas por VDF son apropiadas para asegurarse (en la medida de lo posible) que los duplicados de tarjetas SIM sean facilitados a los titulares de las líneas telefónicas y que la adecuación o no de las medidas adoptadas por VDF no puede hacerse depender de un hecho futuro que no depende de su mandante, esto es, que el ciberdelincuente consiga acceder a la banca online de la persona afectada.

2). Argumenta VDF que sí ha cumplido con los principios de confidencialidad e integridad y responsabilidad proactiva, así como con la obligación de adoptar las medidas técnicas y organizativas adecuadas: las medidas de seguridad adoptadas por Vodafone no tienen carácter estático, sino que las mismas se han ido revisando y actualizando a lo largo del tiempo. A esta cuestión se dedica la alegación segunda.

3). La adopción de medidas técnicas y organizativas no es una obligación absoluta: las cifras obrantes en el expediente son un indicio relevante de que VDF ha cumplido con el principio de integridad y confidencialidad. A esta cuestión dedica la alegación tercera.

En apoyo de esta alegación VDF indica que las cifras obrantes en el expediente demuestran que ha cumplido con el principio de integridad y confidencialidad; esgrimiendo como argumentos que VDF ha procedido a la implementación de medidas objetivamente idóneas para proteger la integridad y confidencialidad de los datos personales de los clientes teniendo en cuenta el número de casos en los que dichas medidas de seguridad se han visto superadas, tomando como referencia el periodo temporal en el que se enmarcan los hechos objeto de las presentes actuaciones, esto es, desde el 29 de julio de 2019 (caso del Reclamante 5, folio 109 del expediente) hasta el 2 de junio de 2020 (caso del Reclamante 8, folio 450 del expediente), vemos que Vodafone ha rechazado un total de ***XXXX*** solicitudes de duplicados de tarjetas SIM, evitando potenciales problemas de fraude y se han materializado ***XXX*** casos, lo que demostraría que las medidas de seguridad implementadas funcionan, según VDF.

4). Subsidiariamente, para el caso de que se entendiera que sí ha habido infracción, son varios los factores que hacen llegar a la conclusión de que la actuación de VDF no ha sido negligente y, en consecuencia, no puede imponerse a la misma sanción alguna. A esta cuestión dedica la alegación cuarta.

Aduciendo en su defensa que en el presente procedimiento sancionador se han evaluado las circunstancias de nueve casos concretos; que las cifras obrantes en el expediente (que no han sido discutidas por la Agencia) ponen de manifiesto que estamos ante casos aislados, de lo que se puede inferir que la actuación de VDF no ha sido negligente; por todas las medidas adoptadas por VDF para prevenir el duplicado fraudulento de tarjetas; la realización de actividades delictivas de terceros para acceder a determinados datos personales de los afectados; y por último la existencia de errores humanos que han llevado a la emisión de los duplicados fraudulentos.

5). Manifiesta VDF que subsidiariamente al punto 4) anterior, para el caso de que se entendiera que sí puede imponérsele una sanción, deberán tenerse en cuenta las circunstancias identificadas en la alegación quinta para disminuir el importe de la sanción.

Manifestando en esta alegación que subsidiariamente, para el supuesto de que la Agencia entendiera que sí que ha existido infracción y que asimismo procediera la im-

posición de una sanción a Vodafone, su mandante considera que, al ser la misma desproporcionada (se propone una sanción de aproximadamente ***XXX.XXX*** euros por cada caso), deberá modularse a la baja atendiendo a las circunstancias que se exponen en su alegación.

Esas circunstancias son los agravantes tenidos en cuenta por la AEPD, y que son los siguientes:

Naturaleza, gravedad y duración de la infracción (artículo 83.2 a) del RGPD): manifiesta con relación al periodo temporal respecto al que acontecen los hechos, que la Agencia alega que con posterioridad al 2 de junio de 2020 (fecha en la que se produjo la última de las nueve reclamaciones que han dado lugar al presente expediente) se habrían registrado tres reclamaciones adicionales denunciando hechos similares que no han sido objeto de acumulación al presente procedimiento sancionador y que no deberían ser tenidos en cuenta como agravantes.

Número de interesados afectados (artículo 83.2 a) del RGPD): manifiesta que, los ***XXX*** casos no pueden ser tenidos en cuenta sin ponerlos en su debido contexto alegando una serie de circunstancias, en relación con el total de clientes de VDF, con el total de solicitudes de duplicado de tarjetas SIM y con el número de solicitudes de tarjetas SIM denegadas.

Nivel de los daños y perjuicios sufridos (artículo 83.2 a) del RGPD el grado de responsabilidad que, en su caso, pueda achacarse a VDF, no puede hacerse depender de una actuación de un tercero que escapa al control de mi mandante, esto es: las medidas de seguridad implementadas por una u otra entidad bancaria o incluso el hecho de que el afectado disponga o no de banca electrónica.

Intencionalidad o negligencia en la infracción (artículo 83.2 b) del RGPD): Manifiesta VDF que a fin de evitar reiteraciones innecesarias, se remite a la Alegación Cuarta en lo relativo a la ausencia de negligencia. Y añade además, su disconformidad con la siguiente afirmación de la Agencia: "Igualmente, el hecho de que VDF haya implementado posteriormente modificaciones en las medidas técnicas u organizativas existentes, corrobora que aquellas otras no proporcionaban la seguridad adecuada" y que no se puede convertir en perjudicial para VDF el hecho de cumplir con el RGPD, que impone una evaluación continua y sistemática de las medidas de seguridad para ir adaptándolas a los riesgos cambiantes, cuestión que ha sido tratada en la Alegación Segunda de este escrito. Si la sanción se impone por la falta de la, a juicio de la Agencia, debida diligencia, la negligencia que constituye precisamente el hecho infractor no puede, a su vez, ser valorada como agravante.

Sobre las medidas tomadas por el responsable (artículo 83.2 c) del RGPD): Argumenta VDF que la Agencia se refiere a la adopción de un listado de medidas (el listado de medidas son las expresamente manifestadas por VDF en el apartado III de la Alegación Tercera de su escrito de alegaciones al Acuerdo de inicio del presente procedimiento, esta alegación al igual que el resto de alegaciones al citado Acuerdo fueron debidamente contestadas en el Fundamento Jurídico Cuarto de la Propuesta de Resolución, respecto del que realiza dos precisiones:

La primera precisión relativa a que VDF ha adoptado, además, otras muchas medidas.

La segunda precisión, se admite las medidas posteriores adoptadas tengan la consideración de mínimos.

Grado de responsabilidad del responsable (artículo 83.2 d) del RGPD): Señala VDF que tal y como ha expuesto en las Alegaciones Segunda y Tercera de este escrito, VDF ha implementado medidas técnicas y organizativas adecuadas para el riesgo generado por mi mandante, esto es, tendentes a asegurar que quien solicita el duplicado o cambio de una tarjeta SIM es el titular de la línea. Nos remitimos a dichas Alegaciones para evitar reiteraciones innecesarias.

Infracciones anteriores al Acuerdo de iniciación cometidas por VDF (artículo 83.2 e) del RGPD): Aduce VDF que este punto no fue incluido por la Agencia como circunstancia agravante en el Acuerdo de Inicio del procedimiento sancionador de 8 de febrero de 2021 (el "Acuerdo de Inicio") mostrando su disconformidad con este hecho porque se incluyó como agravante cuando Vodafone incluyó en su Escrito de Alegaciones de 3 de marzo una referencia a que Vodafone no había sido sancionada por infracción de los artículos 5.1 f) y 5.2 del RGPD en relación con hechos similares a los tratados en el presente expediente y que las infracciones y porque ninguna de las once resoluciones sancionadoras citadas por la Agencia en su Propuesta de Resolución se refiere a infracciones de los artículos 5.1 f) y 5.2 del RGPD en relación con hechos similares a los tratados en el presente expediente.

Categorías de datos personales afectados (artículo 83.2 g) del RGPD): Según VDF la Agencia entiende que la infracción en cuestión "posibilita la suplantación de identidad". Además, en su defensa VDF hace referencia a las alegaciones contenidas en su escrito de alegaciones de 3 de marzo de 2021.

Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal (artículo 76.2 b) de la LOPD): la Agencia se refiere a que el "número de líneas de telefonía móvil [...] posiciona a VDF como una de las operadoras de telecomunicaciones más grandes de nuestro país.

6). Finalmente, manifiesta que en la Alegación Sexta enumera las nuevas pruebas de las que se pretende valer; solicita la prueba que estima conveniente proponer, que se tengan por presentadas como documentos acreditativos de la falta de culpabilidad, o, en su caso, se module a la baja la sanción propuesta por la Agencia, documentos 1 y 2 aportados: Documento 1 copia del correo electrónico enviado por VDF a los responsables de las agencias el 7 de junio de 2019 relativo a los duplicados de tarjeta SIM por vía telefónico y Documento 2 copia de la carta de la Brigada Provincial de Policía Judicial de Valladolid (Grupo de Investigación Tecnológica), en las que puede observarse que las Fuerzas y Cuerpos de Seguridad del Estado han felicitado a VDF por su colaboración en distintas ocasiones.

Estas Alegaciones serán objeto de respuesta en los Fundamentos de Derecho de la presente Resolución.

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

HECHOS PROBADOS

PRIMERO: VDF es la responsable de los tratamientos de datos referidos en la presente Propuesta de Resolución, toda vez que conforme a la definición del artículo 4.7 del RGPD es quién determina la finalidad y medios de los tratamientos realizados con las finalidades señaladas en su Política de Privacidad: ofrecer servicio (procesar pedidos y

proporcionar productos y servicios, facturación y atención al cliente, mensaje de información de servicios, proporcionar servicios de roaming); mejorar el servicio (innovar productos y servicios, gestionar sus redes y comprender el uso de la red); marketing y adaptación de su servicio a las necesidades de los clientes (publicidad on line, investigación y análisis); o generación de perfiles (análisis de crédito y verificación de identidad, prevención del fraude y seguridad).

SEGUNDO: VDF cuenta con una Política de Seguridad específica para el cambio de SIM que efectúa a través de ***(…).***

La solicitud de un duplicado por parte del cliente puede realizarse:

(…).

TERCERO: VDF ha definido en los ***(…)*** las siguientes cláusulas contractuales:

(…).

CUARTO: VDF envió hasta ***(…).***

QUINTO: VDF envió ***(…).***

SEXTO: Con fecha 2 de septiembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante uno (expediente con núm. de referencia E/10004/2019), dirigida contra VDF, tras quedarse sin red en la línea ******TELÉFONO.1,*** en fecha 5 de agosto de 2019***,*** sin poder recibir ni efectuar llamadas.

VDF, en fecha 5 de agosto de 2019, realizó un duplicado de la tarjeta SIM correspondiente a la línea ******TELÉFONO.1*** a las 20:39 horas, que fue entregado a una tercera persona en la tienda VDF del centro comercial de ******CENTRO.1*** (Barcelona).

Consta factura número ******FACTURA.1*** emitida en fecha 7 de agosto de 2019, que contiene el cargo correspondiente a la emisión de la tarjeta SIM, donde especifica como dirección de entrega un Centro Comercial ubicado en el municipio de ******LOCALIDAD.2***, cuando la parte reclamante uno tiene su residencia habitual en el municipio de ******PROVINCIA.1.***

Por estos hechos, la parte reclamante uno presentó una denuncia ante la Guardia Civil de ******LOCALIDAD.1*** (***PROVINCIA.1), en fecha 7 de agosto de 2019, con número de atestado ******ATESTADO.1*** en la que manifiesta que en fecha 6 de agosto, tras conseguir un duplicado de la tarjeta SIM, recibió una serie de SMS del Banco Santander informándole sobre la realización de una transferencia desde la banca online. Al acudir a su banco le informaron de la realización de un total de 25 operaciones de gastos, entre ellas: un préstamo por importe de 5.690,76 euros, la disposición de dos tarjetas de crédito con un saldo de 5.000,00 y 1.000,00 euros respectivamente, y la suscripción de un seguro vinculado al préstamo por importe de 806,66 euros.

En relación con esta reclamación, VDF informó a esta Agencia que, en fecha 5 de agosto de 2019, se realizó un cambio de tarjeta SIM en tienda por un comercial del

distribuidor ***LOCALIDAD.3 CC Llobregat y que tramitó el expediente como un servicio fraudulento, bloqueando la tarjeta SIM duplicada objeto de reclamación en fecha 6 de agosto de 2019.

Indica que previo a la solicitud de cambio de SIM hay una llamada al departamento de atención al cliente, donde tras pasar política de seguridad, se solicita el duplicado de dos facturas, se confirma que el número que origina la llamada es una línea móvil que no pertenece al cliente y que se encuentra alojado en la red de otro operador.

VDF no ha aportado copia del DNI de solicitante del duplicado, indicando que se solicitó la documentación al distribuidor a fin de confirmar si había seguido el proceso de custodia de documentación. ***(…).***

SÉPTIMO: Con fecha 20 de noviembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante dos (expediente con núm. de referencia E/12065/2019), dirigida contra VDF, tras quedarse sin servicio en la línea ***XXXXXXX-XX*** en fechas 4 y 12 de noviembre de 2019, y, expedirse tres duplicados de su tarjeta SIM a favor de terceras personas, sin su consentimiento.

Por estos hechos, la parte reclamante dos, presentó tres denuncias con número de atestado ******ATESTADO.2*** de fecha 4 de noviembre de 2019; ******ATESTADO.3*** de fecha 5 de noviembre de 2019; y, ******ATESTADO.4*** de fecha 12 de noviembre de 2019; todas ellas, presentadas ante la DGPN en las dependencias de Madrid-San Blas. Manifiesta que pudo comprobar a través de su ordenador portátil que en la cuenta de la entidad ING en la que figuraba como autorizado, habían devuelto cuatro recibos y habían realizado una disposición de cajero de 890,00 euros.

Personado en una tienda de VDF le informaron que, en fecha 4 de noviembre de 2019, una persona desconocida había solicitado un duplicado de su tarjeta SIM on line a través del correo electrónico ******EMAIL.3.*** En fecha 5 de noviembre de 2019, comprueba una serie de cobros no autorizados a través de una tarjeta Visa de crédito de BANKIA, así como tres transferencias recibidas en la cuenta de ING en la que figura como autorizado, por importes de 3.000,00, 6.000,00 y 2.500,00 euros. En fecha 12 de noviembre de 2019, de nuevo, se queda sin servicio en su dispositivo móvil. Contacta con VDF y le informan que, personas desconocidas habían anulado su tarjeta SIM y habían hecho un duplicado vía on line.

En relación con esta reclamación, VDF informó a esta Agencia que se realizaron tres duplicados de la tarjeta SIM:

- El primero, con fecha 1/11/2019 a las 23:23:22 ***(…)***. La petición del cambio de SIM se realiza a partir de llamada al servicio de atención al cliente desde número oculto.
- El segundo, con fecha 4/11/2019 6:30:23 por ***(…)*** utilizando la tarjeta SIM ******SIM.9***.
- El tercero con fecha 12/11/2019 11:58:03 por ***(…)***, utilizando la tarjeta SIM ***5***SIM.10***.

Manifiesta que el segundo y tercer duplicado resultaron infructuosos por haber sido marcado el cliente como "víctima de fraude". ***(…).***

OCTAVO: Con fecha 28 de noviembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la representante de la parte reclamante tres (expediente con núm. de referencia E/00557/2020), dirigida contra VDF, tras solicitarse por un tercero y expedirse a su favor, con fecha 28 de septiembre de 2019, un duplicado de la tarjeta SIM de la línea número ******TELÉFONO.14*** de la que era titular su marido.

Por estos hechos, la hija de la parte reclamante tres, presentó dos denuncias con número de atestado ******ATESTADO.5***, de fecha 24 de octubre de 2019 y ******ATESTADO.6***, de fecha 4 de noviembre de 2019 ante la DGPN en las dependencias de ******LOCALIDAD***. Manifiesta en las denuncias, que en la cuenta bancaria de ING de la que eran titulares sus progenitores, se solicitaron dos préstamos personales por valor de 23.000,00 y 3.000,00 euros y se realizaron dos extracciones en cajero por valor de 2.000,00 y 3.000,00 euros. También se transfirieron 5.000,00 euros a una cuenta del Banco Santander de la que es titular la parte reclamante tres. En la cuenta de destino se realizaron v varias retiradas de efectivo mediante Bizum, así como compras con Wallet Santander, movimientos con la tarjeta y venta de acciones. También se vendió un fondo de inversión por valor de 5.000,00 euros reembolsándose el dinero en la cuenta de su padre.

En relación con esta reclamación, VDF informó a esta Agencia que ***(…).***

NOVENO: Con fecha 28 de noviembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante cuatro (expediente con núm. de referencia E/00558/2020), dirigida contra VDF, tras expedirse en fecha 12 y 14 de noviembre de 2019 dos duplicados de la tarjeta SIM de las líneas ******TELÉFONO.15*** y ******TELÉFONO.3*** vía telefónica, a favor de un tercero distinto al titular de las líneas.

En fecha 12 de noviembre de 2019, desde su cuenta corriente y a través de la banca a distancia, se realizaron cuatro transferencias, sin su consentimiento:

Concepto	Fecha	Importe
Retirada de efectivo sin soporte	12-11-2019	300,00
Transferencias XXXXXX	12-11-2019	900,90
Transferencias XXXXXX	12-11-2019	779,90
Transferencias XXXXXX	12-11-2019	810,90

Consta acreditado que el BBVA le reintegró el total de las cantidades sustraídas.

Por estos hechos, la esposa de la parte reclamante cuatro, presentó una denuncia con número de atestado ******ATESTADO.6***, en fecha 13 de noviembre de 2019, ante la Comandancia de la Guardia Civil de Madrid Compañía de ******LOCALIDAD.***

En relación con esta reclamación, VDF informó a esta Agencia que se realizó un primer duplicado fraudulento de la tarjeta SIM el 12 de noviembre de 2019, resultando infructuoso el posterior intento de 14 de noviembre de 2019, por haber sido marcado el cliente como "víctima de fraude".

VDF informó que ***(…).***

DÉCIMO: Con fecha 4 de diciembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante cinco (expediente con núm. de referencia E/ 00559/2020), dirigida contra VDF, tras quedarse sin servicio en la línea ******TELÉFONO.4,*** en fecha 29 de julio de 2019.

En esta última fecha, se expidió a favor de una tercera persona distinta a la titular de la línea, un duplicado de la tarjeta SIM en la tienda sita en la Avd. Suecia de Santa Cruz de Tenerife, cuando la parte reclamante cinco tiene su domicilio en Barcelona.

En fecha 29 de julio de 2019, desde su cuenta corriente, se realizaron dos transferencias a favor de ***J.J.J.***, sin su consentimiento:

Concepto	Fecha	Importe
Orden de compra	29-07-2019	2.175,00
Orden de compra	29-07-2019	2.713,00

Por estos hechos, la parte reclamante cinco, presentó una denuncia, en fecha 5 de agosto de 2019, con número de diligencia: ******DILIGENCIA.1*** ante los Mossos d'Esquadra, OAC de ******LOCALIDAD*** (Girona).

En relación con esta reclamación, VDF informó a esta Agencia que se realizó, en fecha 29 de julio de 2019, desde una tienda física de un distribuidor, en concreto, en Santa Cruz de Tenerife, un cambio de la tarjeta SIM correspondiente a la línea ******TELÉFONO.4***, cuya titular es la parte reclamante cinco. En concreto, consta el cambio de numeración de la tarjeta SIM original "******SIM.6***" al número "******SIM.7***" ("(…)").

Asimismo, se comprobó que en fecha 30 de julio de 2019, figura la gestión de otro cambio de SIM vinculada a la misma línea móvil, realizado, en la misma tienda física de VDF. En particular, figura el cambio de la SIM Bis a la numeración "******SIM.8***" *("(…)").*

Manifiesta que hasta el 29 de noviembre de 2019, no tuvo constancia del carácter fraudulento de la tramitación de los cambios de SIM realizados en los días 29 y 30 de julio de 2019, a pesar de que, a raíz de lo ocurrido, la parte reclamante cinco, interpuso en el mes de agosto de 2019 un total de 3 reclamaciones:

- La primera, con núm. ***XXXXXXX*** ante el Departamento de Fraudes, solicitando la aplicación de una política más restrictiva de seguridad.

- La segunda con núm. ***XXXXXXX***, ante el Departamento de Atención al cliente, solicitando la aplicación de una clave de seguridad.

- Y la tercera, con núm. ***XXXXXXX,*** en la que reitera sus peticiones sobre una clave de seguridad y una política más restrictiva.

Asimismo, la parte reclamante cinco, interpuso una reclamación ante la SETSI solicitando una indemnización por daños y perjuicios, obteniendo una respuesta negativa por parte de VDF, que no se consideró responsable de las transacciones bancarias realizadas de forma fraudulenta, tras superar la tercera persona, en ambos casos, la política de seguridad.

VDF no ha aportado ***(…).***

UNDÉCIMO: Con fecha 17 de febrero de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante seis (expediente con núm. de referencia E/03065/2020), dirigida contra VDF, tras quedarse sin servicio en la línea ******TELÉFONO.7,*** en fecha 7 de enero de 2020.

Dos días antes, es decir, el 5 de enero de 2020, VDF remitió a una dirección de correo electrónico ******EMAIL.1*** -dirección que no constaba en los datos personales del cliente-, un duplicado de una factura, a una tercera persona distinta del titular de la línea, que efectuó hasta trece llamadas al Servicio de Atención al cliente haciéndose pasar por este. Consta ***(…).***

Por estos hechos, la parte reclamante seis, presentó una denuncia, en fecha 9 de enero de 2020, con número de diligencia ******DILIGENCIA.2*** ante los Mossos d'Esquadra USC de ******LOCALIDAD*** (Barcelona). Denunció haber recibido un SMS procedente de ING en el que se le informaba que alguien había intentado acceder a su cuenta con su número de DNI.

En relación con esta reclamación, VDF informó a esta Agencia que ***(…).***

DUODÉCIMO: Con fecha 17 de marzo de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante siete (expediente con núm. de referencia E/03632/2020), dirigida contra VDF, con relación a las líneas ******TELÉFONO.11, ***TELÉFONO.16*** y ******TELÉFONO.17***, tras aceptarse en fecha 15 de diciembre de 2019, un cambio de titularidad en los servicios adscritos a esas líneas, a favor de una tercera persona. Asimismo, en fecha 4 de enero de 2020, se queda sin servicio en la línea ******TELÉFONO.11.***

En esta última fecha, constan efectuados 5 cargos fraudulentos en la cuenta corriente que comparte con su mujer, que ascienden a un total de 7.740,00 euros y dos cargos efectuados a través de la tarjeta de crédito que ascienden a 2.269,40 euros.

Concepto	Fecha	Importe
Pago en lotería Manises	04-01-2020	1.500,00
Pago en lotería Manises	04-01-2020	240,00
Disposición cajero	04-01-2020	1.000,00
Disposición cajero	04-01-2020	2.000,00
Disposición cajero	04-01-2020	2.000,00

Por estos hechos, la parte reclamante siete, presentó una denuncia, en fecha 4 de enero de 2020, ante la DGPN en las dependencias de ******LOCALIDAD***, con número de atestado ******ATESTADO.7***. Manifestó haber recibido un mensaje de su banco ING indicando que habían anulado su clave PIN y acto seguido se quedó sin cobertura. Tras conseguir comunicarse con VDF descubrió que habían duplicado su tarjeta SIM.

En relación con esta reclamación, VDF informó a esta Agencia que se produjo un cambio de titularidad que asoció los datos de un tercero, D. ***M.M.M.***, al ID ******ID.1*** del reclamante. Posteriormente, tuvo lugar un segundo cambio de titular que asoció el ID de cliente anterior a los datos de otro tercero, D. ***N.N.N.*** Asimismo, confirma que en fecha

4 de enero de 2020, se tramitó un cambio de SIM sobre la línea ******TELÉFONO.11***, asociada al ID ******ID.1***. Dicho cambio de SIM fue gestionado de forma presencial, a través ***(…).***

La parte reclamante siete tiene su domicilio en ******LOCALIDAD***.

VDF no ha aportado ***(…).***

DÉCIMO TERCERO: Con fecha 30 de junio de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante ocho (expediente con núm. de referencia E/08544/2020), dirigida contra VDF, tras quedarse sin servicio en la línea ******TELÉFONO.12,*** en fecha 2 de junio de 2020.

En esa misma fecha, VDF tramitó una orden de modificación sobre los servicios asociados al ID de cliente ******TELÉFONO.13***, del que era titular la parte reclamante ocho, a fin de modificar los servicios VDF One Fibra 50Mb + M + TV + Total + Fijo por la tarifa VDF One Ilimitada Total Fibra 1Gb, a petición de una tercera persona distinta de la parte reclamante ocho.

La parte reclamante ocho tiene su domicilio en Sevilla, no obstante, tanto el duplicado de la SIM como la orden de modificación sobre los servicios asociados a su ID, se realiza en el punto de venta ***(…) ***LOCALIDAD*** (Valencia) a favor de una tercera persona, distinta a la parte reclamante ocho.

El Contrato de Servicio Móvil, Banda Ancha, Fijo y TV para Clientes Particulares por el que se materializa la modificación de los servicios contratados no consta firmado por ningún cliente (ni por el titular de la línea, ni por tercera persona en su nombre).

En fecha 2 de junio de 2020, se realiza una transferencia inmediata a favor de ***Q.Q.Q.*** por importe de 3.506,00 euros desde la cuenta corriente de la parte reclamante ocho.

Asimismo se efectúan una serie de cargos en la tarjeta de crédito Visa/MasterCard de la que es titular, entre los días 2 y 4 de junio de 2020, por los siguientes conceptos:

Concepto	Fecha	Importe
Pago móvil en Soloptical Gran, Valencia	2-06-2020	292,50
Pago móvil en Mezea M3, Chirivella	2-06-2020	1.661,60
Pago móvil en El Rinconet, Alfafar	2-06-2020	1,20
Reintegro, Sedaví	2-06-2020	300,00
Pago móvil en estanco, Valencia	3-06-2020	141,00
Reintegro, Valencia	3-06-2020	900,00
Reintegro, Valencia	3-06-2020	1.000,00
Reintegro, Valencia	3-06-2020	1.000,00
Pago móvil en El Corte Inglés, Valencia	3-06-2020	17,45
Pago móvil en El Corte Inglés, Valencia	3-06-2020	24,45
Pago móvil en El Corte Inglés, Valencia	3-06-2020	20,95
Pago móvil en El Corte Inglés, Valencia	3-06-2020	24,45
Pago móvil en El Corte Inglés, Valencia	3-06-2020	809,00
Pago móvil en Cortefiel, Valencia	3-06-2020	104,85
Pago móvil en Supermoments, Valencia	3-06-2020	110,85

Pago móvil en Turmalina, Valencia	3-06-2020	1698,00
Pago móvil en Druni, Torrent	3-06-2020	724,29
Pago móvil en Joyería Antonio, Torrent	3-06-2020	1.833,00
Pago móvil en Primera Ópticos, Torrent	3-06-2020	175,80
Pago móvil en Estanco, Valencia	3-06-2020	150,00
Pago móvil en Estanco, Valencia	3-06-2020	138,00
Carrefour Saler, Valencia	4-06-2020	1.566,00
Carrefour Turia, Xirivella	4-06-2020	1.566,00

En relación con esta reclamación, VDF informó a esta Agencia que, en fecha 2 de junio de 2020, se tramitó un cambio de SIM sobre la línea ******TELÉFONO.12***. Dicho cambio fue gestionado de forma presencial, a través del Punto de Venta VDF operado por (…), ubicado en ******LOCALIDAD*** (Valencia), tras superar la política de seguridad de VDF. En fecha 3 de junio de 2020, tramitó un nuevo cambio de SIM, con el fin de anular el cambio realizado en fecha 2 de junio, restableciendo a tal efecto la línea ******TELÉFONO.12*** y su control e interrumpir el proceso de activación de las tarifas contratadas.

VDF no ha aportado copia del DNI o documento identificativo recabado en la contratación presencial, alegando que son los puntos de venta los que realizan la verificación y copia de los documentos identificativos y que ya no mantiene relación contractual con el distribuidor. Tampoco aporta el documento identificativo recabado en la solicitud de duplicado SIM.

DÉCIMO CUARTO: Con fecha 8 de junio de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante nueve (expediente con núm. de referencia E/05287/2020) dirigida contra VDF, tras quedarse sin servicio en la línea ******TELÉFONO.13****,* en fecha 7 de enero de 2020 y autorizarse dos cambios en la titularidad de su línea, sin su consentimiento.

Consta la factura número ******FACTURA.3*** emitida por VDF en esa misma fecha, que contiene el cargo correspondiente a la emisión de la tarjeta SIM, donde especifica como dirección de entrega ***XXXXXXXXX*** en el municipio de ******LOCALIDAD*** (Girona), cuando la parte reclamante nueve, tiene su residencia habitual en el municipio de ******LOCALIDAD*** (Las Palmas).

Por estos hechos, en fecha 7 de enero de 2020, presentó una denuncia con número de atestado ******ATESTADO.8*** ante la DGPN en las dependencias de ******LOCALIDAD***. Manifiesta que tras quedarse sin línea, recibió a través del wifi de su empresa la confirmación de una operación, pudiendo comprobar a través de un email un préstamo de 7.000,00 euros y tres disposiciones en cajero por las siguientes cantidades: 2.000,00, 2.000,00 y 1.000,00 euros, así como un traspaso interno de 4.000,00 euros.

Asimismo, consta una reclamación dirigida Servicio de Atención al Cliente, en fecha 8 de enero de 2020, solicitando información sobre los dos cambios de titularidad y la expedición de una tarjeta SIM, sin su consentimiento.

En relación con la reclamación interpuesta, VDF informó a esta Agencia que, con fecha 7 de enero de 2020, se produjeron dos cambios de titularidad sobre el ID ******ID.2***, titularidad de la parte reclamante nueve, a favor de terceras personas. En primer lugar, se produjo un cambio de titularidad que asoció los datos de un tercero, D. ***M.M.M.*** al ID

ID.2** del reclamante. Posteriormente, tuvo lugar un segundo cambio de titular que asoció el ID de cliente anterior a los datos de otra persona, D. ***XXXXXX. Asimismo, también ha podido verificar que en fecha 7 de enero de 2020, se tramitó un cambio de SIM sobre la línea ***TELÉFONO.13***, asociada al ID anterior. Dicho cambio de SIM fue gestionado de forma presencial ***(…)***. En fecha 9 de enero de 2020, después de tener constancia de los hechos objeto de reclamación, y tras verificar que estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento, procedió a bloquear la cuenta del cliente, restringiendo el uso de los servicios asociados al ID ***ID.2.***

VDF no ha aportado ***(…).***

DÉCIMO QUINTO: VDF ha llevado a cabo, posteriormente, medidas y desarrollado planes de acción para prevenir el fraude de los duplicados de tarjetas SIM, que centra en cuatro líneas de actuación:

(…).

DÉCIMO SEXTO: En el periodo temporal de referencia en el que se enmarcan los hechos objeto de las presentes actuaciones, esto es, desde el 29 de julio de 2019 (caso del Reclamante 5, folio 109 del expediente) hasta el 2 de junio de 2020 (caso del Reclamante 8, folio 450 del expediente), VDF manifiesta que ***(…).***

FUNDAMENTOS DE DERECHO

PRIMERO: **Competencia.**

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, 48, 64.2 y 68.1 de la LOPDGDD, la directora de la AEPD es competente para iniciar y resolver este procedimiento.

En la incoación del procedimiento sancionador la AEPD ha actuado conforme a los principios generales del artículo 3.1 de la LRJSP, entre los que se halla el servicio efectivo a los ciudadanos, la buena fe, la confianza legítima o la transparencia de la actuación administrativa.

La AEPD tiene atribuidas una serie de competencias, poderes y funciones previstas en los artículos 55 y siguientes del RGPD que según dispone el artículo 8 de la LRJSP, son irrenunciables y se ejercerán por los órganos administrativos que las tengan atribuidas como propias.

En el ejercicio de las funciones y poderes que le atribuyen los artículos 57 y 58 del RGPD, controla la aplicación del RGPD, realiza investigaciones e impone, en su caso, sanciones administrativas entre las que se pueden incluir las multas administrativas, y ordena las medidas correctoras correspondientes, según las circunstancias de cada caso particular. Así, puede realizar las investigaciones que considere oportunas (artículo 67 de la LOPDGDD), tras lo que puede decidir iniciar de oficio un procedimiento sancionador (artículo 68 LOPDGDD).

En el supuesto examinado, las investigaciones realizadas en aras de determinar la comisión de unos hechos y el alcance de estos pusieron de manifiesto una eventual falta de medidas de seguridad.

SEGUNDO: **Normativa aplicable.**

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."*

TERCERO: **Infracción.**

Las actuaciones reseñadas en los Antecedentes han tenido como objeto analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM por parte de VDF, identificando las vulnerabilidades que pudieran existir en los procedimientos operativos implantados, para detectar las causas por las cuales se podrían estar produciendo estos casos, así como encontrar puntos de incumplimiento, mejora o ajuste, para determinar responsabilidades, disminuir los riesgos y elevar la seguridad en el tratamiento de los datos personales de las personas afectadas.

Los hechos declarados anteriormente probados, vulneran el artículo 5.1.f) y el artículo 5.2 del RGPD y son constitutivos de la infracción prevista en el artículo 83.5.a) del RGPD que considera infracción muy grave la vulneración de: "*los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9*," tipificada con sanción de multa administrativa de 20.000.000,00 euros 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.

También son constitutivos de la infracción tipificada en el artículo 72.1.a) de la LOPDGDD que considera infracción muy grave a los efectos de la prescripción: *"El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".*

El artículo 75 de la LPACAP, se refiere a los "Actos de instrucción" como aquellos necesarios para la determinación, conocimiento y comprobación de los hechos en virtud de los cuales deba pronunciarse la resolución. Pues bien, de la instrucción resultó tras el análisis de las pruebas practicadas y de las alegaciones aducidas conforme a lo previsto en los artículos 76 y 77 de la LPACAP, que VDF a pesar disponer de un documento denominado política de seguridad que contenía las medidas de seguridad que se deberían adoptar en los tratamientos de datos personales necesarios para la prestación de los servicios contratados y a lo largo de su ciclo de vida, estas medidas han resultado a todas luces insuficientes.

Del análisis de los procedimientos seguidos por VDF -documentado con las reclamaciones y los casos adicionales estudiados -, resultan los siguientes hechos de interés:

VDF no ha podido acreditar:

- La identidad de los solicitantes de los duplicados de tarjeta SIM.
- La identidad de los solicitantes en los cambios de titularidad de la línea.
- La identidad de los solicitantes de las copias de las facturas.
- Las grabaciones de las llamadas telefónicas amparándose en que los plazos de conservación han expirado, cuando nos encontramos ante un total de ***XXX*** fraudulentos declarados en el ejercicio 2019.

- El motivo por el cual se ha remitido el duplicado de la tarjeta SIM a una ciudad distinta a la de la residencia de los abonados sin controles o garantías adicionales (casos partes reclamantes: UNO, OCHO y NUEVE).
- La efectividad del check “Víctima de fraude” lo que evidencia un menoscabo en la resiliencia de los sistemas y servicios de tratamiento, ya que no se garantiza la velocidad suficiente ni la trazabilidad de la información en condiciones adversas como son las que acontecen en los casos analizados.
- La efectividad del procedimiento de activación telefónica después de la recogida de la tarjeta SIM de forma presencial.
- La efectividad de la atención multicanal que establece la vía presencial como canal prioritario para la solicitud de los duplicados de SIM, indicando a los gestores que atienden las llamadas que deriven a tienda a los solicitantes que solicitan el duplicado vía telefónica. (…).

Por otro lado, se constató la falta de responsabilidad proactiva.

El concepto de responsabilidad proactiva se encuentra ligado con el concepto de cumplimiento normativo o compliance, ya presente en otros ámbitos normativos (nos referimos, por ejemplo, a la previsión del artículo 31 bis del Código Penal).

Así, el artículo 24 del RGPD determina que “*1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos”.

La responsabilidad proactiva implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento generalizado de las obligaciones en materia de protección de datos. Comprende el establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización, especialmente si es una gran empresa, -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que le permita demostrar su cumplimiento.

Pivota sobre la gestión del riesgo. Tal y como se establece en el Informe 0064/2020 del Gabinete Jurídico de la AEPD se muestra la metamorfosis de un sistema que ha pasado de ser reactivo a convertirse en proactivo, puesto que “en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la LOPDGDD: *“la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del*

tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan".

Requiere de una actitud consciente, comprometida, activa y diligente. La consciencia supone el conocimiento de su organización por parte del responsable del tratamiento y de cómo se ve afectada por la protección de datos y de los riesgos inherentes a los tratamientos de datos personales; el compromiso involucra la voluntad de cumplir y el hacerse verdaderamente responsable de la implantación de las políticas de protección de datos en la organización; la actitud activa está relacionada con la proactividad, la eficacia, la eficiencia y la operatividad; y la diligencia es el cuidado, el celo y la dedicación puesta en el cumplimiento.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, tal y como se infiere de los hechos probados y considerado el contexto del artículo 24 del RGPD en relación con VDF, se constató, entre otros, la falta de un modelo eficaz de evitación del riesgo de suplantación de identidad, la ausencia de medidas de seguridad adecuadas y tendentes a asegurar el procedimiento de identificación y entrega de la tarjeta SIM, la materialización de los riesgos, la reacción temporal tardía frente a los hechos descritos, amén de la insuficiencia de las medidas adoptadas (pues ha reaccionado al recibir los requerimiento de la AEPD y no ha evitado la repetición posterior como muestran las tres reclamaciones posteriores presentadas ante la AEPD).

Asimismo, a pesar de contar con un documento llamado "política de seguridad", éste no supone la implementación de un modelo eficaz de evitación del riesgo de suplantación de identidad, ni la implantación de un sistema de revisión, refuerzo, mejora y control de las medidas de seguridad aplicadas en los distintos canales tendentes a asegurar el procedimiento de identificación y entrega de la tarjeta SIM, con el fin de evitar la materialización de los fraudes.

Máxime cuando la tarjeta SIM constituye el soporte físico a través del cual se accede a los datos de carácter personal de la persona afectada. Si no se garantiza su disposición y control, el acceso a los datos personales del titular, así como el uso o usos posibles por terceros, se convierte en una amenaza que puede tener efectos devastadores en la vida de estas personas.

Por otra parte, conforme al propio principio de responsabilidad proactiva, es el responsable del tratamiento el que debe determinar cuáles son las medidas de seguridad a implantar, pues sólo este último es conocedor en profundidad de su organización, de los tratamientos que lleva a cabo, de los riesgos asociados a los mismos y de las medidas de seguridad precisas a implementar para hacer efectivo el principio de integridad y confidencialidad.

Ahora bien, ha quedado probado que las medidas implantadas por VDF son insuficientes y no sólo porque se haya producido su superación y la cesión de datos personales a un tercero.

De una manera no exhaustiva y a título de ejemplo nos fijaremos en ***(…).***

Así, de la documentación remitida por VDF se infiere la falta de instrucciones específicas sobre qué datos concretos deben de pedirse al llamante para realizar un cambio de SIM, remitiéndose a algunas normas adicionales, como: ***(…).***

Los datos personales asociados a la política de seguridad son los básicos de cualquier cliente: ***(…)***. Basta con poseer datos básicos de un cliente para poder superar la política de seguridad, sin que ninguna pregunta adicional sea formulada respecto de algún

dato que conozcan únicamente la operadora y su cliente. Ningún requisito suplementario es requerido.

Asimismo, VDF no ha aportado ninguna de las grabaciones de las llamadas efectuadas para el cambio de las tarjetas SIM, alegando que el plazo de conservación de esta ha expirado. Llama la atención que detectados por la operadora un total de ***XXX*** casos en los que se ha superado la política de seguridad y siendo conscientes de la situación, al menos en tales casos se hubieran conservado las grabaciones o la transcripción de estas.

Así las cosas, el fraude conocido como "SIM Swapping" es una técnica delincuencial consistente en obtener un duplicado de la tarjeta SIM asociada a una línea de telefonía titularidad de un usuario, con la finalidad de suplantar su identidad para obtener acceso a sus redes sociales, aplicaciones de mensajería instantánea, aplicaciones bancarias. o comercio electrónico, con la finalidad de interactuar y realizar operaciones en su nombre, autenticándose mediante un usuario y contraseña previamente arrebatados a ese usuario, así como con la autentificación de doble factor al recibir el SMS de confirmación en su propio terminal móvil donde tendrán insertada la tarjeta SIM duplicada.

Hay que destacar que en la primera fase de este tipo de estafas el suplantador consigue, de manera fraudulenta, los datos de acceso o las credenciales de la banca online del cliente, pero le falta poder conocer el código de verificación, segundo factor de autentificación, para poder ejecutar cualquier operación. En el momento en el que logra la tarjeta SIM duplicada ya tiene también acceso a este segundo factor de autenticación y, por tanto, desde ese instante puede realizar los actos de disposición patrimonial que desee.

Por lo tanto, es responsabilidad de la operadora establecer unos requisitos adecuados efectivos y eficaces que, si bien de una lectura rápida pueden parecer muy estrictos, de una lectura mucho más cuidadosa se ha evidenciado que no lo eran. Con lo cual, la estafa o suplantación, que aparentemente podría parecer compleja y difícil, se ve que no lo ha sido tanto por la falta de adecuación de las medidas de seguridad a la hora de vigilar que es el titular de la tarjeta SIM o persona por éste autorizada la que peticiona el duplicado.

Todo ello, lo que denota es una falta de diligencia en la gestión del riesgo, así como una actitud reactiva y no proactiva enfocada desde el diseño y la incapacidad para demostrar el cumplimiento.

CUARTO: **Tratamiento de datos personales y responsable del tratamiento**

El artículo 4 del RGPD, bajo la rúbrica "Definiciones", dispone lo siguiente:

"1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmi-

sión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

VODAFONE ESPAÑA, S.A.U. es la responsable de los tratamientos de datos referidos en los antecedentes expuestos, toda vez que conforme a la definición del artículo 4.7 del RGPD es el que determina la finalidad y medios de los tratamientos realizados con las finalidades señaladas en su Política de Privacidad y que se detallan en los hechos probados.

Asimismo, la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular ya que *se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador* (artículo 4.1) del RGPD).

En este sentido, conviene aclarar que, dentro del terminal móvil, va insertada la tarjeta SIM. Es una tarjeta inteligente, en formato físico y de reducidas dimensiones, que contiene un chip en el que se almacena la clave de servicio del suscriptor o abonado usada para identificarse ante la red, esto es, el número de línea telefónica móvil del cliente MSISDN (Mobile Station Integrated Sergvices Digital Network -Estación Móvil de la Red Digital de Servicios Integrados-), así como el número de identificación personal del abonado IMSI (International Mobile Subscriber Identity -Identidad Internacional del Abonado móvil-) pero también puede proporcionar otro tipo de datos como la información sobre el listado telefónico o el de llamadas y mensajes.

La tarjeta SIM es posible introducirla en más de un terminal móvil, siempre que éste se halle liberado o sea de la misma compañía.

En España, desde el año 2007, mediante la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, se exige que los titulares de todas las tarjetas SIM, ya sean de prepago o de contrato, estén debidamente identificados y registrados. Esto es importante por cuanto la identificación del abonado será imprescindible para dar de alta la tarjeta SIM, lo que conllevará que a la hora de obtener un duplicado de esta la persona que lo solicite haya de identificarse igualmente y que su identidad coincida con la del titular.

En suma, tanto los datos personales (nombre, apellidos y DNI) que se tratan para emitir un duplicado de tarjeta SIM como la propia tarjeta SIM (Subscriber Identity Module) que identifica de forma inequívoca y unívoca al abonado en la red, son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos.

QUINTO: **Alegaciones aducidas a la Propuesta de Resolución.**

Se procede a dar respuesta a las mismas según el orden expuesto por VDF (la operadora se remite además en su integridad a las alegaciones presentadas en fecha 3 de marzo de 2021):

PREVIA: SOBRE LO QUE CONSTITUYE EL OBJETO DEL PROCEDIMIENTO SANCIONADOR.

Como alegación previa VDF señala que la Propuesta de Resolución propone la imposición de una multa de 4.000.000'00 por una presunta infracción de los artículo 5.1.f) y 5.2 del RGPD, infracción tipificada como muy grave el artículo 83.5.a) del RGPD y por el artículo 72.1 de la LOPDGDD, porque VDF habría vulnerado los principios de integridad y confidencialidad y de responsabilidad proactiva, al facilitar duplicados de tarjeta SIM a personas que no son las titulares de las líneas móviles, tras la superación por estos terceros de las políticas de seguridad implementadas por VDF.

Asimismo, manifiesta que el expediente sancionador tiene su origen en nueve reclamaciones presentadas ante la Agencia, si bien ésta no sólo ha tenido en cuenta los hechos concretos y especificidades acaecidos en esos casos, sino que ha enjuiciado las medidas de seguridad adoptadas por VDF con carácter general.

Efectivamente, y tal y como se ha puesto de manifiesto a lo largo del procedimiento sancionador, la AEPD tras diversos procedimientos sancionadores por fraude de identidad incoados a VDF, y a raíz de 9 reclamaciones más por fraude de identidad, que implicaban por parte del responsable del tratamiento la emisión del duplicado de la tarjeta SIM del cliente (tras lo cual se han producido gravosos daños económicos a los afectados) investiga en profundidad el origen del problema en aras de averiguar si podía ser debido a errores puntuales -como en muchos casos alegaba VDF- o se debía a un fallo en el modelo de protección de la privacidad.

El foco no se sitúa en los terceros que han superado las políticas de seguridad, sino en el por qué las han superado; esto es, se examina la condición, características y adecuación de las políticas citadas a la normativa de protección de datos y la actuación del responsable del tratamiento al respecto.

Hemos de significar que, por tanto, en este caso la AEPD se ha centrado no tanto en la falta de legitimación en el tratamiento de datos personales sino en la política de protección de datos de la entidad.

PRIMERA. LIMITACION DEL OBJETO DE PROCEDIMIENTO AL EXAMEN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS.

VDF indica que el objeto del presente procedimiento debe limitarse a determinar si ha adoptado las medidas de técnicas y organizativas adecuadas para evitar, en la medida de lo posible, que se expidan duplicados de tarjetas SIM a sujetos que no son los titulares de las líneas móviles. El enjuiciamiento no puede extenderse a las actuaciones anteriores y posteriores llevadas a cabo por los ciberdelincuentes.

Sorprende a la Agencia el hecho de que aduzca que no hemos delimitado las operaciones o actividades de tratamiento cuando el Fundamento de Derecho Cuarto de la Propuesta de Resolución señala que "el objeto de este expediente no es (…), sino la defensa efectiva del derecho fundamental a la protección de datos por los tratamientos efectuados por VDF" sin que en ningún momento extienda su "enjuiciamiento a las actuaciones anteriores y posteriores llevadas a cabo por los ciberdelincuentes"; circunscribiéndose a analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM por parte de VDF, no de otras entidades, como las financieras, que invoca.

La tarjeta SIM identifica un número de teléfono y este número a su vez, identifica a su titular. En este sentido la Sentencia del TJUE en el asunto C -101/2001(Lindqvist) de 6.11.2003, apartado 24, Rec. 2003 p. I-12971: *"El concepto de "datos personales" que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva "toda información sobre una persona física identificada o identificable". Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficione"».*

También, esta opinión se singulariza en relación con los dispositivos de telefonía móvil que permiten la localización del interesado, en el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes (documento WP185):

> *"Dispositivos móviles inteligentes. Los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas. Normalmente existe una identificabilidad directa e indirecta. En primer lugar, los operadores de telecomunicaciones que proporcionan acceso a Internet móvil y a través de la red GSM poseen normalmente un registro con el nombre, la dirección y los datos bancarios de cada cliente, junto con varios números únicos del dispositivo, como el IMEI y el IMSI. (…)"*

En definitiva, la actividad de tratamiento cuestionada ha sido el procedimiento específico para el cambio de tarjeta SIM de VDF y la adecuación de las medidas de seguridad implementadas por VDF en el marco de la gestión del riesgo para la correcta identificación de los clientes en el momento de expedir el duplicado de la tarjeta SIM.

SEGUNDA. DEL CUMPLIMIENTO DEL PRINCIPIO DE CONFIDENCIALIDAD E INTEGRIDAD (GARANTÍAS EN MATERIA DE SEGURIDAD) Y DE RESPONSABILIDAD PROACTIVA.

Argumenta VDF que sí ha cumplido con los principios de confidencialidad e integridad y responsabilidad proactiva, así como con la obligación de adoptar las medidas técnicas y organizativas adecuadas: las medidas de seguridad adoptadas por VDF no tienen carácter estático, sino que las mismas se han ido revisando y actualizando a lo largo del tiempo.

Así, relata de nuevo las actuaciones efectuadas consistentes en llevar a cabo acciones de mitigación en los dos canales de VDF en los que se pueden realizar cambios de SIM:

(…).

Al respecto hay que señalar que precisamente el que nos encontremos ante el fraude de un tercero hace que sea necesario asegurarse que la persona a la que se expide el duplicado de la tarjeta SIM es quien realmente dice ser y deben adoptarse las medidas necesarias de prevención adecuadas para verificar la identidad de una persona cuyos datos van a ser objeto de tratamiento tal y como se reconoce en el Fundamento Jurídico Séptimo de la SAN, SCA, de 5 de mayo de 2021 ("Por otro lado, en cuanto al hecho de que nos encontramos ante el fraude de un tercero, como dijimos en la SAN de 3 de octubre de 2013 (Rec. 54/2012) -: *" Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento...").*

A lo largo del presente procedimiento VDF ha manifestado reiteradamente que los du-

plicados fraudulentos de las tarjetas se han producido tras haber superado los defraudadores su política de seguridad. Considera que es inevitable que a pesar de la existencia de la política de seguridad pueda haber casos en los que a través de ciertos mecanismos dicha política de seguridad pueda ser sobrepasada de forma fraudulenta sin que por ello pueda existir reproche a VDF.

Sin embargo, ha quedado probado que la política de seguridad de VDF ha resultado insuficiente para la adecuada protección de los derechos fundamentales de las personas cuyas tarjetas SIM han sido fraudulentamente duplicadas; teniendo en cuenta que la adopción de medidas se ha producido no tras el análisis de los riesgos que implica el tratamiento de los datos para la emisión de duplicados de tarjeta SIM, realizado por VDF, sino cuando se ha puesto en su conocimiento los hechos, mediante el traslado de las reclamaciones presentadas ante la AEPD; lo que pone de manifiesto una conducta reactiva de VDF ante hechos consumados (comunicación de las reclamaciones) más que la conducta proactiva exigida por el RGPD que requeriría un análisis continuado de los riesgos y la adopción de las correspondientes medidas para tratar de mitigarlos, máxime teniendo en cuenta los perjuicios económicos que se podrían derivar del uso posterior de los duplicados de esas tarjetas SIM fraudulentas, como ha quedado demostrado en el procedimiento.

En resumen, esta alegación no puede ser tomada en consideración porque VDF no ha cumplido con la obligación de acreditar fehacientemente el cumplimiento del principio de responsabilidad proactiva (artículo 5.2 del RGPD) a través de proceso continuo" de adaptación y "gestión continua de los riesgos potenciales asociados al tratamiento de datos", lo que ha posibilitado que VDF haya expedido duplicados fraudulentos a terceros.

TERCERA. LA ADOPCIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS NO ES UNA OBLIGACIÓN ABSOLUTA.

VDF alega en su descargo que la adopción de medidas técnicas y organizativas no es una obligación absoluta: las cifras obrantes en el expediente son un indicio relevante de que VDF ha cumplido con el principio de integridad y confidencialidad.

Así, en apoyo de esta alegación VDF indica que las cifras obrantes en el expediente demuestran que VDF ha cumplido con el principio de integridad y confidencialidad; esgrimiendo como argumentos que VDF ha procedido a la implementación de medidas objetivamente idóneas para proteger la integridad y confidencialidad de los datos personales de los clientes teniendo en cuenta el número de casos en los que dichas medidas de seguridad se han visto superadas, tomando como referencia el periodo temporal en el que se enmarcan los hechos objeto de las presentes actuaciones, esto es, desde el 29 de julio de 2019 (caso del Reclamante 5, folio 109 del expediente) hasta el 2 de junio de 2020 (caso del Reclamante 8, folio 450 del expediente), señalan que VDF ha rechazado un total de ***X.XXX*** solicitudes de duplicados de tarjetas SIM, evitando potenciales problemas de fraude y se han materializado ***XXX*** casos, lo que demostraría que las medidas de seguridad implementadas funcionan, según VDF.

En primer lugar, y sobre que la adopción de medidas técnicas y organizativas no es una obligación absoluta, que alega VDF, debe indicarse que no se exige una obligación de resultado, sino de actividad, pero para evaluar dicha actividad e implementación de medidas y su consideración como "adecuadas" es inevitable analizar los métodos utilizados por el tercero para acceder ilícitamente al proceso de duplicado, las salvaguardas implementadas por VDF e inevitablemente, el resultado. Esos tres elementos son los que van a determinar la adecuación al riesgo y no como pretende centrar el

debate, VDF sobre si es infalible o no su sistema.

El enfoque de riesgos y el modelo flexible al riesgo impuesto por el RGPD -partiendo de la doble configuración de la seguridad como un principio relativo al tratamiento y una obligación para el responsable o el encargado del tratamiento- no impone en ningún caso la infalibilidad de las medidas, sino su adecuación constante a un riesgo, que, como en el supuesto examinado es cierto, probable y no desdeñable, alto y con un impacto muy significativo en los derechos y libertades de los ciudadanos.

Segundo, cabe señalar que lo que dejan patente estos datos es que VDF es consciente de que del total de solicitudes de duplicado de tarjetas SIM susceptibles de ser consideradas como fraudulentas, que según el propio criterio de VDF, ascendería a ***X.XXX*** en el período temporal en que se enmarcan las actuaciones del presente procedimiento y teniendo en cuenta las medidas de seguridad implantadas, XXX, es decir, el ***X,XX*** % de las solicitudes susceptibles de ser consideradas fraudulentas no son detectadas por VDF, y que VDF entiende que ese porcentaje supone que las medidas implantadas funcionan de forma satisfactoria.

Si bien a juicio de la AEPD, unas medidas de seguridad que permiten un porcentaje en torno al ***XX*** % de expedición de duplicado tarjetas SIM fraudulentas pone de relieve la insuficiencia de esas medidas de seguridad adoptadas y la necesidad de que por parte de VDF se adopten medidas adecuadas para reducir significativamente los casos de duplicados fraudulentos de tarjetas SIM.

En resumen esta alegación tampoco puede prosperar, además, porque ha quedado constatado que el porcentaje de casos en los que se han visto superadas las medidas de seguridad adoptadas por VDF se aproximan al ***XX*** % de las solicitudes susceptibles de ser consideradas fraudulentas no son detectadas mediante la aplicación de las medidas contenidas en la política de seguridad que dice tener implementada VDF para este tratamiento.

CUARTA. FALTA DE NEGLIGENCIA EN LA ACTUACIÓN DE VDF.

VDF afirma que su actuación no ha sido negligente. Aduce en su defensa que en el presente procedimiento sancionador se han evaluado las circunstancias de nueve casos concretos; que las cifras obrantes en el expediente (que señalan que no han sido discutidas por la Agencia) ponen de manifiesto que estamos ante casos aislados, de lo que se puede inferir que la actuación de VDF no ha sido negligente; por todas las medidas adoptadas por VDF para prevenir el duplicado fraudulento de tarjetas; la realización de actividades delictivas de terceros para acceder a determinados datos personales de los afectados; y por último la existencia de errores humanos que han llevado a la emisión de los duplicados fraudulentos.

No es cierto, como pretende hacer ver VDF que en el presente procedimiento se hayan evaluado las circunstancias de nueve casos concretos, puesto que como se ha indicado anteriormente, este procedimiento, partiendo de las nueve reclamaciones, se ha dirigido a analizar si las medidas técnicas y organizativas adoptadas por VDF para la expedición de duplicados de tarjetas SIM a los titulares de las líneas telefónicas son apropiadas para asegurar la mitigación de los posibles riesgos para los derechos y libertades fundamentales de los titulares de las líneas.

Las circunstancias de los nueve casos en los que se ha presentado reclamación ante la AEPD ponen de manifiesto la insuficiencia de las medidas de seguridad adoptadas por VDF, que además, reconoce que tales medidas han sido insuficientes en un total de ***XXX*** casos en el periodo al que se refiere el presente procedimiento sancionador, lo

que muestra que las medidas de seguridad no fallan solo en casos aislados como pretende hacer valer VDF.

Además, hay que tener en cuenta que la gravedad de los hechos probados ~~que~~ se plasma en la alarma social generada por la realización de estas prácticas fraudulentas, sin que sea determinante el número de reclamaciones presentadas.

Hace referencia VDF, para su descargo, al conjunto de medidas de seguridad que ha adoptado (un poco antes y durante la tramitación del procedimiento sancionador) y que dice que va renovando a lo largo del tiempo. Sobre este particular significar, en primer lugar, que las medidas de seguridad adoptadas por VDF ya incoado el procedimiento sancionador no inciden sobre la infracción ya cometida. Segundo, que, las medidas implantadas son las mínimas exigibles a cualquier organización con las características y en el contexto en el que actúa una operadora de telecomunicaciones. Un repaso a las mismas así lo muestra. Por ejemplo, la remisión de comunicados dirigidos a sus trabajadores y distribuidores alertando sobre el fraude y las concretas medidas de seguridad implantadas entra dentro de una actuación ordinaria del responsable del tratamiento (sin ello es imposible que estas sean efectivas); lo mismo acontece con el bloqueo de la tarjeta SIM o la restricción de mensajes una vez detectado el fraude (no sería de recibo permitir la continuación de la operativa por el delincuente) y marcar al cliente como víctima de fraude.

Tal y como se ha probado, estas medidas de seguridad no eran adecuadas ni suficientes, pues la cesión de datos a terceros se ha producido sin verificar de forma fehaciente la identidad de los interesados.

VDF hace mención en su descargo a la actuación de los delincuentes. La falta de medidas de seguridad es un hecho objetivo; tal incumplimiento resulta ajeno, además, a la actuación de los terceros a quienes VDF ha cedido los datos, en el sentido de que la actividad delictiva llevada a cabo por estos últimos no influye en la comisión de la infracción. Más bien al contrario, la falta de medidas de seguridad es lo que posibilita la actividad delictiva.

La intervención fraudulenta de un tercero, lo que ha revelado es el deficiente análisis de los riesgos, así como la insuficiente implantación, revisión y control de las medidas de seguridad por parte de la operadora. Terceros ajenos a los titulares de los datos han superado las medidas de seguridad establecidas por VDF en múltiples ocasiones. Esto nos muestra que la identificación del titular de los datos no se producía con las suficientes garantías, independientemente de que la identificación se realizara por el propio titular o por un tercero de forma fraudulenta.

VDF manifiesta que los duplicados de tarjetas SIM se han producido consecuencia de errores humanos.

El factor humano, la evidente posibilidad de cometer errores por los seres humanos, es uno de los riesgos más importantes a considerar siempre en relación con la determinación de las medidas de seguridad. El responsable del tratamiento debe contar con el error humano como un riesgo más que probable. Los errores humanos se combaten desde el enfoque de riesgos, el análisis, la planificación, implantación y control de las medidas técnicas y organizativas adecuadas y suficientes.

Significar que no es desdeñable la importante cantidad de errores humanos que se producen en VDF de manera continuada, constante y repetida, tal y como se constata de los hechos probados.

Una vez, dos veces, puede tratarse de un error humano que sobrepase las medidas de seguridad. Continuos errores humanos lo que exteriorizan es un problema más profundo en la organización, una falta de visión de los riegos, de análisis y de planificación (privacidad desde el diseño), una ausencia de dimensionamiento de las medidas de seguridad, una omisión en la implantación de las adecuadas o de revisión de las inadecuadas, la inexistencia de demostración del cumplimiento… En suma, una falta de medidas de seguridad apropiadas y un incumplimiento de las obligaciones derivadas de la responsabilidad proactiva, máxime cuando los "errores" persisten en el tiempo (considerando las posteriores reclamaciones presentadas ante la AEPD contra VDF por hechos similares tras la incoación del procedimiento sancionador).

Un criminal puede intentar provocar el error humano, pero son las medidas de seguridad adecuadas quienes actúan de freno. Es palpable por tanto la falta de diligencia de VDF.

Por otro lado, y estrictamente en cuanto a la negligencia en la actuación de VDF, cabe señalar que la SAN -Sala Contencioso-Administrativo- 392/2015, de 17 de noviembre que en su Fundamento Jurídico Tercero recoge la doctrina del Tribunal Constitucional sobre la aplicación al derecho administrativo sancionador de los principios del orden penal, en los siguientes términos:

> "El Tribunal Constitucional ha declarado reiteradamente que los principios del orden penal, entre los que se encuentra el de culpabilidad, son de aplicación, con ciertos matices, al derecho administrativo sancionador, al ser ambos manifestaciones del ordenamiento punitivo del Estado (STC 18/1987 , 150/1991), y que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad aun a título de mera negligencia (SSTC 76/1990 y 164/2005).
>
> El principio de culpabilidad, garantizado por el artículo 25 de la Constitución, limita el ejercicio del "ius puniendi" del Estado y exige, según refiere el Tribunal Constitucional en la sentencia 129/2003, de 20 de junio, que la imposición de la sanción se sustente en la exigencia del elemento subjetivo de culpa, para garantizar el principio de responsabilidad y el derecho a un procedimiento sancionador con todas las garantías (STS de 1 de marzo de 2012, Rec 1298/2009).
>
> Ciertamente, el principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, de 26 noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone que solo pueden ser sancionados por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Obviamente, ello supone que dicha responsabilidad sólo puede ser exigida a título de dolo o culpa, quedando desterrada del ámbito del derecho administrativo sancionador la llamada "responsabilidad objetiva", y comprendiendo el titulo culposo la imprudencia, negligencia o ignorancia inexcusable. Esta "simple inobservancia" no puede ser entendida, por tanto, como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, pues la jurisprudencia mayoritaria de nuestro Tribunal Supremo (a partir de sus sentencias de 24 y 25 de enero y 9 de mayo de 1983) y la doctrina del Tribunal Constitucional (después de su STC 76/1990), destacan que el principio de culpabilidad, aún sin reconocimiento explícito en la Constitución, se infiere de los principios de legalidad y prohibición de exceso (artículo 25.1 CE), o de las propias exigencias inherentes a un Estado

de Derecho, por lo que se requiere la existencia de dolo o culpa (en este sentido STS de 21 de enero de 2011, Rec 598/2008).

No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo que en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas. Según la STC 246/1991 " (...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma " (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998 , parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005 , y de 23 de octubre de 2010, Rec 1067/2006 , que "aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" .

En el supuesto que nos atañe resulta notoria la existencia de antijuridicidad y culpabilidad en la conducta infractora de la entidad responsable del tratamiento de los datos personales, VDF, quien como responsable del tratamiento de datos de emisión de duplicados de tarjetas SIM, que decide sobre la finalidad, contenido y uso de los datos personales incluidos en el tratamiento, tiene la obligación de obrar con mayor diligencia a la hora de tramitar la emisión de duplicados, asegurándose de contar con el consentimiento de su titular, a fin de no incurrir en el tratamiento no consentido de sus datos personales. Dicha condición impone un deber especial de diligencia a la hora de llevar a cabo el uso o tratamiento de los datos personales, en lo que atañe al cumplimiento de los deberes que la legislación sobre protección de datos establece para garantizar los derechos fundamentales y las libertades públicas de las personas físicas, y especialmente su honor e intimidad personal y familiar, cuya intensidad se encuentra potenciada por la relevancia de los bienes jurídicos protegidos por aquellas normas y la profesionalidad de los responsables o encargados, máxime cuando operan con ánimo de lucro en el mercado de datos; en este sentido se ha pronunciado también la SAN 392/2015, de 17 de noviembre (Ver su Fundamento de Derecho Tercero).

Al respecto, resulta significativo que la operadora responsable del tratamiento no justifique debidamente la concurrencia en su conducta de la diligencia que le era exigible ni acredite la adopción de las cautelas exigibles para evitar el tratamiento no consentido del dato de carácter personal que nos ocupa (la emisión de duplicados de tarjetas

SIM de forma fraudulenta), que debe atribuirse a la conducta negligente de VDF, con independencia de que la contratación tuviera lugar ante un distribuidor de dicha compañía, o se llevara a cabo por vía telefónica o telemática utilizándose por un tercero los datos personales de los reclamantes pasando las medidas de seguridad para realizar el duplicado de las tarjetas SIM.

En conclusión, el objeto de este procedimiento se ha dirigido a analizar si las medidas técnicas y organizativas adoptadas por VDF para la expedición de duplicados de tarjetas SIM a los titulares de las líneas telefónicas son apropiadas para asegurar la mitigación de los posibles riesgos para los derechos y libertades fundamentales de los titulares de las líneas, no a evaluar las circunstancias que se hayan producido en nueve casos concretos, teniendo en cuenta en la alarma social generada por la realización de estas prácticas fraudulentas, sin que sea determinante el número de reclamaciones presentadas. Habiendo quedada acredita la negligencia por la insuficiencia de las medidas adoptadas, lo que ha supuesto que se vean afectados al menos ***XXX*** casos según reconoce VDF.

QUINTA. APLICACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD.

Manifiesta VDF que subsidiariamente y para el caso de que se entendiera que sí puede imponérsele una sanción, considera la misma desproporcionada al entender que se propone una sanción de aproximadamente 444.000 euros por cada caso, debiendo reducirse su cuantía por las circunstancias que expresa.

En cuanto a la supuesta desproporcionalidad de la sanción propuesta, conviene indicar que el RGPD prevé expresamente la posibilidad de graduación, mediante la previsión de multas susceptibles de modulación, en atención a una serie de circunstancias de cada caso individual efectivas, proporcionadas y disuasorias (artículo 83.1 y 2 RGPD), condiciones generales para la imposición de las multas administrativas que sí han sido objeto de análisis por esta Agencia, a las que hay que sumar los criterios de graduación previstos en la LOPDGDD, objeto de desarrollo en el FD Octavo.

A mayor abundamiento, a la hora de demostrar la proporcionalidad de la sanción propuesta hay que señalar que si se aplicaran las sanciones previstas en la normativa anterior, teniendo en cuenta que las infracciones cometidas por VDF se catalogan como infracciones muy graves y el artículo 45.3 de la LOPD de 1999 preveía que “Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros prevista para las infracciones muy graves” por cada uno de las reclamaciones, como son 9 reclamaciones la multa que se le hubiera impuesto con la normativa anterior estaría comprendida entre los 2.700.000 y los 5.400.000 euros, con lo que la multa actualmente fijada estaría dentro del rango de la sanción prevista en la normativa anterior, que ya no es aplicable.

Si bien hay que reiterar que no se impone la sanción por aquellos casos en los que se han presentado reclamaciones, sino porque estos casos ponen de relieve el incumplimiento de las garantías en materia de seguridad (artículo 5.1.f) RGPD) y de responsabilidad proactiva (artículo 5.2 del RGPD) que se pone de manifiesto la deficiencia de las medidas de seguridad adoptadas por VDF en el tratamiento de datos de duplicado de tarjetas SIM que permite el duplicado de dichas tarjetas SIM por motivos fraudulentos.

Además, hay que tener en cuenta que en la actualidad el RGPD no fija una cuantía mínima y que el artículo 83.5 establece que “*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de*

20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".

Hay que señalar que la multa administrativa acordada será efectiva porque conducirá a la operadora a cumplir con la responsabilidad proactiva y a aplicar las medidas técnicas y organizativas que garanticen un grado de seguridad correspondiente al valor de criticidad del tratamiento. También es proporcional a la vulneración identificada, en particular a su gravedad, el círculo de personas físicas afectadas y los riesgos en los que se han incurrido y a la situación financiera de la compañía.

Y por último, es disuasoria. Una multa disuasoria es aquella que tiene un efecto disuasorio genuino. A este respecto, la Sentencia del TJUE, de 13 de junio de 2013, Versalis Spa/Comisión, C-511/11, ECLI:EU:C:2013:386, dice:

> *" 94.Respecto, en primer lugar, a la referencia a la sentencia Showa Denko/Comisión, antes citada, es preciso señalar que Versalis la interpreta incorrectamente. En efecto, el Tribunal de Justicia, al señalar en el apartado 23 de dicha sentencia que el factor disuasorio se valora tomando en consideración una multitud de elementos y no sólo la situación particular de la empresa de que se trata, se refería a los puntos 53 a 55 de las conclusiones presentadas en aquel asunto por el Abogado General Geelhoed, que había señalado, en esencia, que el coeficiente multiplicador de carácter disuasorio puede tener por objeto no sólo una «disuasión general», definida como una acción para desincentivar a todas las empresas, en general, de que cometan la infracción de que se trate, sino también una «disuasión específica», consistente en disuadir al demandado concreto para que no vuelva a infringir las normas en el futuro. Por lo tanto, el Tribunal de Justicia sólo confirmó, en esa sentencia, que la Comisión no estaba obligada a limitar su valoración a los factores relacionados únicamente con la situación particular de la empresa en cuestión."*
>
> *"102. Según reiterada jurisprudencia, el objetivo del factor multiplicador disuasorio y de la consideración, en este contexto, del tamaño y de los recursos globales de la empresa en cuestión reside en el impacto deseado sobre la citada empresa, ya que la sanción no debe ser insignificante, especialmente en relación con la capacidad financiera de la empresa (en este sentido, véanse, en particular, la sentencia de 17 de junio de 2010, Lafarge/Comisión, C-413/08 P, Rec. p. I-5361, apartado 104, y el auto de 7 de febrero de 2012, Total y Elf Aquitaine/Comisión, C-421/11 P, apartado 82)."*

La Sentencia de fecha 11 de mayo de 2006 dictada en el recurso de casación 7133/2003 establece que: "*Ha de tenerse en cuenta, además, que uno de los criterios rectores de la aplicación de dicho principio régimen sancionador administrativo (criterio recogido bajo la rúbrica de «principio de proporcionalidad» en el apartado 2 del artículo 131 de la citada Ley 30/1992) es que la imposición de sanciones pecuniarias no debe suponer que la comisión de las infracciones tipificadas resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas".*

También es importante la jurisprudencia que resulta de la Sentencia de la Sala Tercera del Tribunal Supremo, dictada en fecha 27 de mayo de 2003 (rec. 3725/1999) que dice: *La proporcionalidad, perteneciente específicamente al ámbito de la sanción, constituye uno de los principios que rigen en el Derecho Administrativo sancionador, y*

representa un instrumento de control del ejercicio de la potestad sancionadora por la Administración dentro, incluso, de los márgenes que, en principio, señala la norma aplicable para tal ejercicio. Supone ciertamente un concepto difícilmente determinable a priori, pero que tiende a adecuar la sanción, al establecer su graduación concreta dentro de los indicados márgenes posibles, a la gravedad del hecho constitutivo de la infracción, tanto en su vertiente de la antijudicidad como de la culpabilidad, ponderando en su conjunto las circunstancias objetivas y subjetivas que integran el presupuesto de hecho sancionable -y, en particular, como resulta del artículo 131.3 LRJ y PAC, la intencionalidad o reiteración, la naturaleza de los perjuicios causados y la reincidencia-. (SSTS 19 de julio de 1996, 2 de febrero de 1998 y 20 de diciembre de 1999, entre otras muchas).

SEXTA. NUEVAS PRUEBAS APORTADAS POR VDF.

Finalmente, VDF enumera las nuevas pruebas de las pretende valerse en el presente procedimiento sancionador a los efectos de acreditar su falta de culpabilidad o la rebaja de la cuantía de la sanción. A saber, ***(…).***

Al respecto hay que señalar que el artículo 89.2 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común establece que "En el caso de procedimientos de carácter sancionador, una vez concluida la instrucción del procedimiento, el órgano instructor formulará una propuesta de resolución que deberá ser notificada a los interesados. La propuesta de resolución deberá indicar la puesta de manifiesto del procedimiento y el plazo para formular alegaciones y presentar los documentos e informaciones que se estimen pertinentes", por lo que los documentos aportados en esta alegación se entienden pertinentemente aportados y se incorporan al expediente del presente procedimiento.

Si bien no se comparte la valoración de VDF sobre que deban ser considerados como documentos acreditativos de su falta de culpabilidad en el presente expediente, o, en su caso, modular a la baja la sanción propuesta por la Agencia, toda vez que los documentos aportados no aportan una información adicional a la que se recoge en los Documentos 4 y 7 propuestos como pruebas a practicar en el Escrito de Alegaciones al Acuerdo de inicio:

(…).

De acuerdo con lo anteriormente expuesto, hemos de concluir que, analizados los escritos de alegaciones al Acuerdo de inicio así como a la Propuesta de resolución, los hechos y fundamentos de derecho en que se basan, no desvirtúan ni los Hechos ni los Fundamentos de Derecho recogidos tanto en el Acuerdo de inicio como en la Propuesta de resolución o en la presente Resolución.

SEXTO: **Principios relativos al tratamiento.**

Considerado el derecho a la protección de datos de carácter personal como el derecho de las personas físicas a disponer de sus propios datos, es necesario determinar los principios que lo configuran.

En este sentido, el artículo 5 RGPD, referido a los "Principios relativos al tratamiento" dispone:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; (…)

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»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de nuestros datos.

En este sentido, el considerando 75 del RGPD determina: *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*.

Asimismo, el considerando 83 del RGPD establece: *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 se-*

guridad 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.

Hemos de atender a las circunstancias singulares de las nueve reclamaciones presentadas, a través de las cuales puede constatarse que, desde el momento en el que la persona suplantadora realiza la sustitución de la SIM, el teléfono de la víctima se queda sin servicio pasando el control de la línea a las personas suplantadoras. En consecuencia, los reclamantes ven afectados sus poderes de disposición y control sobre sus datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos según ha señalado el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre de 2000 (FJ 7). De manera que, al conseguir un duplicado de la tarjeta SIM, se posibilita bajo determinadas circunstancias, el acceso a los contactos o a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder modificar las contraseñas. En definitiva, podrán suplantar la identidad de los afectados, pudiendo acceder y controlar, por ejemplo: las cuentas de correo electrónico; cuentas bancarias; aplicaciones como WhatsApp; redes sociales, como Facebook o Twitter, y un largo etc. En resumidas cuentas, una vez modificada la clave de acceso por parte de los suplantadores pierden el control de sus cuentas, aplicaciones y servicios, lo que supone una gran amenaza.

De ahí que la seguridad y la confidencialidad de los datos personales se consideren esenciales para evitar que los interesados sufran efectos negativos.

En consonancia con estas previsiones, el considerando 39 RGPD dispone: *Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.*

Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que

los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

El considerando 7 dispone: *(…) Las personas físicas deben tener el control de sus propios datos personales. (…)*

Los hechos declarados anteriormente probados, son constitutivos de una vulneración del artículo 5.1.f) del RGPD al facilitar VDF duplicados de la tarjeta SIM a terceras personas que no son las legítimas titulares de las líneas móviles e incluso modificar la titularidad de los servicios contratados, tras la superación por las personas suplantadoras de las políticas de seguridad implantadas por la operadora, lo que evidencia un incumplimiento del deber de proteger la información de los clientes.

Este acceso no autorizado a la tarjeta SIM resulta determinante para las actuaciones posteriores desarrolladas por las personas suplantadoras que tienen por objeto obtener un beneficio económico, ya que el suplantador aprovecha el espacio de tiempo que transcurre hasta que el usuario detecta el fallo en la línea, se pone en contacto con la operadora, y ésta detecta el problema, para realizar operaciones bancarias fraudulentas tras acceder a las claves de banca on-line del legítimo abonado.

La emisión y entrega del duplicado a un tercero no autorizado supone para los afectados la pérdida del control de sus datos personales. Por lo tanto, el valor de ese dato personal, integrado en un soporte físico -tarjeta SIM-, es real e incuestionable, motivo por el cual VDF tienen el deber legal de garantizar su seguridad, tal como lo haría con cualquier otro activo.

Cabe traer a colación la sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional, que configura el derecho a la protección de datos como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o qué datos puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Así, de acuerdo con los Fundamentos jurídicos 4, 5, 6 y 7 de la sentencia del alto tribunal:

> **"4.** Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.
>
> Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de

relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo, fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

5. (…)

Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente,

que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil

ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle

para que los rectifique o los cancele." (el subrayado de todos los párrafos es nuestro)

Por tanto, cualquier actuación que supone privar a la persona de aquellas facultades de disposición y control sobre sus datos personales, constituye un ataque y una vulneración de su derecho fundamental a la protección de datos.

También se ha producido una vulneración del principio de responsabilidad proactiva.

Directamente relacionado con el principio de responsabilidad proactiva previsto en el artículo 5.2. del RGPD se encuentra la *"Responsabilidad del responsable del tratamiento",* artículo 24 del RGPD:

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento

En consonancia con estas previsiones el considerando 74 del RGPD dispone: *Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas.*

Igualmente, relacionado con el principio de responsabilidad proactiva se encuentra el principio de *"Protección de datos desde el diseño y por defecto",* recogido en el artículo 25 del RGPD:

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

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

En consonancia con estas previsiones, el considerando 78 del RGPD dispone:

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

En concreto, a la luz del RGPD considerando 78, el principio de protección de datos desde el diseño es la clave que seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que *«el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto».*

De hecho, la seguridad de los datos no se logra únicamente con el equipo adecuado (hardware y programas informáticos), sino que también exige la existencia de normas internas de organización adecuadas.

A lo largo del presente procedimiento ha quedado acreditado que los procedimientos de emisión de duplicados de tarjetas SIM de VDF requieren un correcto análisis, planificación, establecimiento, mantenimiento, actualización y control, incluyendo la demostración del cumplimiento (observancia del principio de responsabilidad proactiva), especialmente en relación con las medidas de seguridad adecuadas y suficientes, con el objeto de que se garantice la seguridad de los datos personales de los clientes de ma-

nera efectiva y en particular, su custodia, para evitar el acceso no autorizado a los duplicados de las tarjetas SIM y/o servicios de sus titulares.

SÉPTIMO: **Condiciones generales para la imposición de la multa administrativa.**

En el artículo 83.2 del RGPD se dispone que:

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

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

Por su parte, el artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado. (…)"

De acuerdo con los preceptos transcritos a efectos de fijar el importe de la sanción como responsable de la infracción tipificada en el artículo 83.5.a) del RGPD, procede graduar la multa que corresponde imponer respecto de ambas infracciones, previa valoración de las alegaciones aducidas a los efectos de una correcta aplicación del principio de proporcionalidad.

Por una parte, se han tenido en cuenta los siguientes agravantes:

- Artículo 83.2.a) RGPD:

  · Naturaleza, gravedad y duración:

  En relación con la naturaleza de los datos personales sobre los que se ha perdido la disposición (de forma temporal), además de la línea telefónica, afectan en el caso de las partes reclamantes uno y seis, además de quedarse sin servicio, a la remisión de un duplicado de factura con los datos personales del legítimo titular de la línea y en el caso de la parte reclamante ocho, a la suscripción de un contrato de Servicio Móvil, Banda Ancha, Fijo y TV para Clientes Particulares que contenía los datos bancarios de su legítimo titular. Estos hechos, confirman la naturaleza de la infracción como muy grave puesto que acarrea una pérdida de disposición y control sobre los datos personales.

  Con relación al periodo temporal respecto al que acontecen los hechos, en la Propuesta de Resolución se estimaba la alegación en cuanto a que no supera el año. El órgano de instrucción reconocía su error de apreciación, sin que por otra parte, se considerase su relevancia. La duración de los hechos acontece desde el 29 de julio de 2019 (caso de la

parte reclamante cinco) hasta el 2 de junio de 2020 (caso de la parte reclamante ocho). Sin embargo, posteriormente, esta Agencia ha registrado hasta tres reclamaciones más denunciando hechos similares. Sobre estas reclamaciones, de conformidad con el artículo 65.4 de la LOPDGDD, se ha dado traslado al Delegado de Protección de Datos de VDF, para que procediese a su análisis y diera respuesta a esta Agencia en el plazo de un mes.

> .- Reclamación A: ***(…).*** Hechos según manifestaciones de la parte reclamante: Se han facilitado duplicados de la tarjeta SIM en fechas 31/01/2020, 27/04/2020 y 08/06/2020 (en dos ocasiones) a terceras personas, quedándose sin línea y valiéndose dichos terceros de su línea para realizar operaciones fraudulentas en la cuenta bancaria de la reclamante (retirada de efectivo, solicitudes de préstamos, cargos fraudulentos).
>
> .- Reclamación B: ***(…).*** Hechos según manifestaciones de la parte reclamante: Se ha realizado un duplicado de tarjeta SIM sin su consentimiento en fecha 03/09/2020. Declara que ha sufrido disposiciones de su cuenta bancaria a consecuencia de estos hechos.
>
> .- Reclamación C: ***(…)***. Hechos según manifestaciones de la parte reclamante: Se ha realizado un duplicado de tarjeta SIM sin su consentimiento en fecha 22/01/2021.

Durante ese transcurso de tiempo en el que VDF ha bloqueado la tarjeta SIM se han realizado diversas transacciones y se ha solicitado un crédito bancario del que ha tenido conocimiento a través de su correo electrónico. En los tres casos, las reclamaciones han sido objeto de admisión a trámite, no obstante, no han sido objeto de acumulación al presente procedimiento por cuanto las actuaciones previas de investigación que determinaron la necesidad de incoar este procedimiento, se orientaron a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona responsable y las circunstancias relevantes del procedimiento seguido para gestionar las solicitudes de cambio de SIM, identificando posibles vulnerabilidades, sin que fuera determinante el número de reclamaciones registradas, dada la alarma social generada por la realización de estas prácticas fraudulentas, ya que tras la entrada en vigor de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015, sobre servicios de pago en el mercado (en vigor desde el 14 de septiembre de 2019), el teléfono móvil pasa a tener un rol muy importante en la realización de pagos online al ser necesario para la confirmación de transacciones, y convierte a este dispositivo -y por extensión a la tarjeta SIM-, en objetivo claro de los ciberdelincuentes.

Ahora, la operadora aduce que esas tres reclamaciones adicionales no deberían ser tenidas en cuenta como agravantes.

Pues bien, tal y como se explicó en la Propuesta de Resolución, esas tres reclamaciones registradas con posterioridad al 2 de junio de 2020, no son tenidas en cuenta como agravantes, sin perjuicio de que este goteo continuo de reclamaciones presentadas ante la AEPD muestre de forma indubitada una problemática existente en la organización de VDF reflejada en los Hechos Probados.

En suma, la aplicación del agravante del artículo 83.2.a) del RGPD se refiere a todos los aspectos anteriormente analizados, puestos de manifiesto en los Hechos Probados, a la alarma social generada por la realización de estas prácticas fraudulentas y por la altísima probabilidad de materialización del riesgo, sin que sea determinante el número de reclamaciones presentadas. Y ello, porque lo que se ha analizado en el presente procedimiento sancionador es la política de protección de datos implantada por el responsable del tratamiento a raíz de diversas reclamaciones presentadas ante la AEPD.

· Núm. de interesados afectados:

Se registraron nueve reclamaciones denunciando estos hechos. VDF declaró ***XXX*** casos en 2019.

Casos fraudulentos detectados declarados 2019	Número total de clientes de telefonía móvil (fuente VDF)	Número total de solicitudes de cambio de tarjeta SIM 2019 (fuente VDF)	% casos SIM fraudulentos declarados sobre número de líneas
XXX	12.422.064	***XXX.XXX***	***X,XXX***%

Y aunque el porcentaje resultante represente un ***X,XXX*** % se considera suficiente para que la Agencia vele por la aplicación del RGPD.

Reitera VDF que, los XXX casos no pueden ser tenidos en cuenta sin ponerlos en su debido contexto alegando una serie de circunstancias, en relación con el total de clientes de VDF, con el total de solicitudes de duplicado de tarjetas SIM y con el número de solicitudes de tarjetas SIM denegadas.

Señalar al respecto que la AEPD ha tenido en cuenta los ***XXX*** casos poniéndolos en su debido contexto teniendo en cuenta las circunstancias aludidas por VDF.

Ahora bien, a mayor abundamiento, lo que sí deja patente la referencia de los ***XXX*** casos es que, VDF es consciente de que del total de solicitudes de duplicado de tarjetas SIM susceptibles de ser consideradas como fraudulentas, que según el propio criterio de VDF, ascendería a ***XXXX*** en el período temporal en que se enmarcan las actuaciones del presente procedimiento, ***XXX***, es decir, el ***X,XX*** % de esas solicitudes de duplicado de tarjetas SIM susceptibles de ser consideradas fraudulentas no son detectadas por VDF, de lo que resulta la presencia de una probabilidad nada desdeñable de materialización del riesgo.

· Nivel de los daños y perjuicios sufridos:

Alto. Es cierto que el sistema de verificación de las entidades bancarias responde a la voluntad de estas y no de VDF. No obstante, también es cierto, que si VDF asegurase el procedimiento de identificación y entrega, ni siquiera podría activarse el sistema de verificación de las entidades bancarias. La persona estafadora tras conseguir la activación de la nueva SIM, toma el control de la línea telefónica, pudiendo así, a continuación, realizar operaciones bancarias fraudulentas accediendo a los SMS que las entidades bancarias envían a sus clientes como confirmación de las operaciones que ejecutan. Esta secuencia de hechos puesta de manifiesto en las nueve reclamaciones interpuestas genera una serie de daños y perjuicios graves que deberían haberse tenido en cuenta en una evaluación de impacto relativa a la protección de datos (considerando 89, 90, 91 y artículo 35 del RGPD). Respecto a la devolución de las cantidades reintegradas, se confirma únicamente la devolución de las cantidades sustraídas en el caso de la parte reclamante cuatro. En definitiva, desde el momento que se entrega un duplicado a una persona distinta al titular de la línea o persona autorizada, el cliente pierde el control de la línea y los riesgos, daños y perjuicios, se multiplican. Además, los hechos acontecen con una inmediatez abrumadora.

VDF insiste respecto del grado de responsabilidad que, en su caso, pueda achacárseles, no puede hacerse depender de una actuación de un tercero que escapa su control, esto es: las medidas de seguridad implementadas por una u otra entidad bancaria o incluso el hecho de que el afectado disponga o no de banca electrónica.

En relación con esta alegación, amén de lo ya indicado anteriormente, el grado de responsabilidad cae dentro de su ámbito y no de terceros, debiendo señalar que la SAN -Sala Contencioso Administrativo- de 5 de mayo de 2021, establece que: "*Por otro lado, en cuanto al hecho de que nos encontramos ante el fraude de un tercero, como dijimos en la SAN de 3 de octubre de 2013 (Rec. 54/2012)-: " Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento".*

En cuanto a la alegación de VDF relativa a la no constancia ni valoración alguna de los daños realmente sufridos que no hayan sido compensados por la propia VDF o las entidades bancarias, hay que señalar que, se confirma únicamente la devolución de las cantidades sustraídas en el caso de la parte reclamante cuatro, no existiendo constancia de reintegro en los demás casos de la devolución de las cantidades sustraídas.

A mayor abundamiento, los daños y perjuicios sufridos por los reclamantes, constan como Hechos Probados en el presente procedimiento

en relación con las reclamaciones presentadas ante la AEPD, (retirada de efectivo de cajeros, realización de operaciones financieras como contratación de préstamos; realización de transferencias; adquisiciones de diversos productos; contrataciones de servicios de sociedad de la información, etc.); y que, tal y como asevera VDF, pueda haber una compensación posterior por la propia VDF o por las entidades bancarias. en virtud de una obligación legal, no implica una disminución de la reprochabilidad de la conducta infractora de VDF, en materia de protección de datos respecto a la expedición de duplicados de tarjetas SIM.

- Artículo 83.2.b) RGPD:

  · Intencionalidad o negligencia en la infracción:

  Como ya indicamos en la Propuesta de Resolución, negar la concurrencia de una actuación negligente por parte de VDF equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no compartimos esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida. Resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica que *"…el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

  Ahora VDF sigue argumentando su disconformidad respecto de la siguiente afirmación de la Agencia: "*Igualmente, el hecho de que VDF haya implementado posteriormente modificaciones en las medidas técnicas u organizativas existentes, corrobora que aquellas otras no proporcionaban la seguridad adecuada";* asimismo, señala que no se puede convertir en perjudicial para VDF el hecho de cumplir con el RGPD, y que si la sanción se impone por la falta de la, a juicio de la Agencia, debida diligencia, la negligencia que constituye precisamente el hecho infractor no puede, a su vez, ser valorada como agravante.

  Confunde VDF lo que constituye el tipo infractor (en este caso en relación con la falta de responsabilidad proactiva) con la circunstancia agravante de negligencia en la infracción. Identifica falta de responsabilidad proactiva y la diligencia debida implícita en ésta, con negligencia en la infracción, este último como agravante de su conducta. Así, aduce que, falta de diligencia debida es negligencia y asimila ambos conceptos.

  Pues bien, la sanción se impone por la falta de garantías en la seguridad del tratamiento del artículo 5.1.f) del RGPD y del principio de res-

ponsabilidad proactiva del artículo 5.2 del RGPD. El hecho infractor consiste en que VDF, como responsable del tratamiento de expedición de duplicados de tarjetas SIM no ha sido capaz de demostrar de forma fehaciente que en dicho tratamiento ha cumplido los principios de protección de datos recogidos en el artículo 5 del RGPD, al no haber adoptado las medidas adecuadas para la protección de los datos objeto del tratamiento de expedición del duplicado de tarjetas SIM. Máxime cuando tal y como hemos señalado en la SAN de 17 de octubre de 2007 (rec. 63/2006) precitada "*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".*

La negligencia como agravante se conecta entonces, no con el tipo infractor mismo (que incluye mucho más que la diligencia debida), sino con hechos circundantes a este, puesto que nos encontramos con una gran empresa que realiza tratamientos de datos personales de sus clientes a gran escala, de manera sistemática y continua y que debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos, tal y como establece la jurisprudencia. Máxime cuando dispone de medios de toda índole más que suficientes para cumplir adecuadamente. No es lo mismo si la infracción es cometida por VDF que por una persona física o por una pequeña empresa. En el primer caso es más reprobable el incumplimiento. Así se infiere del considerando 148 del RGPD que impone estar a las circunstancias concurrentes para calificar una infracción como grave o leve a los efectos del RGPD.

En este expediente la negligencia como agravante se percibe, entre otros, en la tardanza de adopción de medidas correctoras una vez producido el duplicado de la tarjeta SIM, toda vez que las mismas son adoptadas, no tras tener constancia VDF de los duplicados fraudulentos de las tarjetas SIM, sino tras la comunicación de la AEPD de las reclamaciones presentadas. El hecho de no corregir las vulnerabilidades a tiempo ha agravado el daño a las personas afectadas.

Los incumplimientos tienen grados, resultando este más gravoso por las circunstancias descritas, entrando de lleno en el campo de la negligencia.

- Artículo 83.2.d) RGPD:

  · Grado de responsabilidad del responsable:

  Se considera que las medidas técnicas y organizativas implementadas son insuficientes. Los datos personales que recabe VDF tanto para la contratación del servicio como durante su provisión, son de su responsabilidad y deben ser tratados de forma que se permita el buen desarrollo de la relación contractual entre las partes, garantizando en todo momento la aplicación de los principios del artículo 5 RGPD.

- Artículo 83.2.e) RGPD:

  · Toda infracción anterior cometida por el responsable:

Núm. procedimiento	Fecha resolución sancionadora	Sanción
PS/00139/2020	03/07/2020	9.000,00
PS/00168/2020	20/07/2020	45.000,00
PS/00009/2020	28/07/2020	48.000,00
PS/00186/2020	31/08/2020	60.000,00
PS/00303/2020	26/10/2020	36.000,00
PS/00341/2020	28/10/2020	30.000,00
PS/00348/2020	06/11/2020	42.000,00
PS/00356/2020	16/11/2020	42.000,00
PS/00308/2020	16/11/2020	36.000,00
PS/00415/2020	30/12/2020	54.000,00
PS/00430/2020	10/02/2021	120.000,00

Aduce VDF que este punto no fue incluido por la Agencia como circunstancia agravante en el Acuerdo de Inicio y muestra su disconformidad con este hecho, porque se incluyó como agravante cuando VDF incluyó en su escrito de alegaciones de 3 de marzo una referencia a que no había sido sancionada por infracción de los artículos 5.1 f) y 5.2 del RGPD en relación con hechos similares a los tratados en este expediente. También porque ninguna de las once resoluciones sancionadoras citadas por la Agencia en la Propuesta de Resolución se refieren a infracciones de los artículos 5.1 f) y 5.2 del RGPD en relación con hechos similares a los tratados en este expediente.

Al respecto hay que señalar que el trámite de Acuerdo de inicio de procedimiento sancionador se realiza de conformidad con las evidencias que se disponen cuando se dicta y sin perjuicio de lo que resulte de la instrucción del procedimiento; siendo a raíz de lo incluido en el escrito de alegaciones de 3 de marzo cuando como consecuencia de la instrucción del procedimiento se acuerda su inclusión al comprobarse que la AEPD había dictado once resoluciones sancionadoras previas contra VDF.

En relación con la argumentación de que las infracciones por las que había sido sancionada VDF no se referían a infracciones de los artículos 5.1.f) y 5.2 del RGPD, señalar que el artículo 83.2.e) establece que "*Al*

decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". El considerando 148 del RGPD añade que ha de referirse a "cualquier infracción anterior pertinente" o "relevante" de la traducción del texto original en inglés –"relevant". Los procedimientos listados en la tabla expuesta son relevantes y están directamente relacionados con el actual. La mayor parte de ellos, también en el ahora examinado, se producen partiendo de un fraude de identidad no detectado por la compañía, que acarrea un tratamiento sin consentimiento de datos personales, cediéndose los datos personales a un tercero distinto de su titular y por defectos en el modelo de protección de datos establecido o por insuficiencia de medidas adecuadas. Muestran incumplimientos anteriores en materia de fraude de identidad y falta de medidas en procedimientos de identificación de identidad.

En cuanto a la consideración de la previsión del artículo 83.2.e) del RGPD como atenuante, tal y como pretendía la parte reclamada, la SAN, de 5 de mayo de 2021, rec. 1437/2020, indica que: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante".*

- Artículo 83.2.g) RGPD:

  · Categorías de datos personales afectados:

  El dato personal afectado por el tratamiento tiene una naturaleza especialmente sensible ya que como indicaba el Acuerdo de inicio "*El acceso no autorizado a un duplicado de tarjeta SIM se considera particularmente grave ya que posibilita la suplantación de identidad. Y si bien no se vieron afectados "categorías especiales de datos personales" según define el RGPD en su artículo 9, esto no significa que los datos sustraídos no fueran de naturaleza sensible*", ya que posibilita la suplantación de identidad.

  La entrega de un duplicado de SIM a favor de un tercero distinto del legítimo titular se considera particularmente grave ya que imposibilita el envío o recepción de llamadas, SMS, o el acceso al servicio de datos, que pasa a estar en manos de la persona suplantadora.

  Obtenido el duplicado, se abre la vía de acceso a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder cambiar las contraseñas. En suma, posibilita la suplantación de identidad.

Y si bien no se han visto afectados “Categorías especiales de datos personales” según define el RGPD en el artículo 9, ello no significa que los datos sustraídos no fueran de naturaleza sensible. No se trata del dato personal que se requiere para la expedición del duplicado de la tarjeta, si no de la tarjeta misma como dato personal asociada a una línea de telefonía titular de un usuario, que se obtiene con la finalidad de suplantar su identidad para obtener acceso -entre otros- a las aplicaciones bancarias o comercio electrónico, con la finalidad de interactuar y realizar operaciones en su nombre, autenticándose mediante un usuario y contraseña previamente arrebatados a ese usuario, así como con la autentificación de doble factor al recibir el SMS de confirmación en su propio terminal móvil donde tendrá inserida la tarjeta SIM duplicada.

- Artículo 76.2.b) LOPDGDD:

  · Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal:

  El desarrollo de la actividad empresarial que desempeña VDF requiere un tratamiento continuo y a gran escala de los datos personales de los clientes. El número de líneas de telefonía móvil de voz informadas en el “Antecedente DÉCIMO CUARTO” y “Fundamento de Derecho SÉPTIMO”, posiciona a VDF como una de las operadoras de telecomunicaciones más grandes de nuestro país.

  A mayor abundamiento, a la hora de demostrar la proporcionalidad de la sanción propuesta hay que señalar que si se aplicarán las sanciones previstas en la normativa anterior, teniendo en cuenta que las infracciones cometidas por VDF se catalogan como infracciones muy graves y el artículo 45.3 de la LOPD de 1999 preveía que “Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros prevista para las infracciones muy graves” por cada uno de las reclamaciones, como son 9 reclamaciones la multa que se le hubiera impuesto con la normativa anterior estaría comprendida entre los 2.700.000 y los 5.400.000 euros, con lo que la multa actualmente fijada estaría dentro del rango de la sanción prevista en la normativa anterior, que ya no es aplicable.

  Si bien hay que dejar claro, como ya hemos indicado, que no se impone por aquellos casos en los que se han presentado reclamaciones, sino porque estos casos ponen de relieve el incumplimiento de las garantías en materia de seguridad (artículo 5.1.f) RGPD) y de responsabilidad proactiva (artículo 5.2 del RGPD) que se pone de manifiesto en la deficiencia de las medidas de seguridad adoptadas por VDF en el tratamiento de datos de duplicado de tarjetas SIM que permite la expedición de duplicados de forma fraudulenta.

  Además, hay que tener en cuenta que en la actualidad el RGPD no fija una cuantía mínima y que el artículo 83.5 establece que “*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el*

apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".

Por otra parte, se han tomado en consideración, como atenuantes:

- Artículo 83.2.c) RGPD:

  · Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados:

    Positivas. A saber: ***(…).***

- Artículo 83.2.f) RGPD:

  · Grado de cooperación con la autoridad de control:

    Alto. La Agencia considera que VDF ha cooperado de forma favorable con la investigación, proporcionando respuesta a todos los requerimientos y lo tiene en consideración.

- Artículo 76.2.c) LOPDGDD:

  · Los beneficios obtenidos como consecuencia de la comisión de la infracción.

    Se descarta la obtención de un beneficio económico más allá de percibir el precio del coste fijado para la emisión de los duplicados de las tarjetas SIM.

- Artículo 76.2.h) LOPDGDD:

  · 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.

    Diversos operadores de telecomunicaciones, entre los que se encuentra VDF, suscribieron con AUTOCONTROL un Protocolo que, sin perjuicio de las competencias propias de la AEPD, prevé mecanismos para la resolución privada de controversias relativas a la protección de datos en el ámbito de contratación y publicidad de servicios de comunicaciones electrónicas, con fecha 15 de septiembre de 2017. Protocolo cuya aplicación efectiva debe ser considerado como atenuante.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la directora de la AEPD, de conformidad con las evidencias de las que se dispone en el presente procedimiento y teniendo en cuenta los antecedes de hecho, los hechos probados y los fundamentos jurídicos anteriormente expuestos

RESUELVE

PRIMERO: IMPONER a **VODAFONE ESPAÑA, S.A.U.**, con CIF A80907397, por una infracción del artículo 5.1.f) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD, una multa de 3.940.000'00 euros (tres millones novecientos cuarenta mil euros).

SEGUNDO: NOTIFICAR la presente resolución a **VODAFONE ESPAÑA, S.A.U.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el artículo 98.1.b) de la LPACAP, en el plazo de pago voluntario establecido en el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el artículo 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la AEPD en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al artículo 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la AEPD en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el artículo 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la AEPD, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva

del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

Mar España Martí
Directora de la AEPD