- **Expediente Nº: PS/00080/2022**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 3 de mayo de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **DKV SEGUROS Y REASEGUROS, S.A.E.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: PS/00080/2022

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: D.ª ***A.A.A.*** (en adelante, la parte reclamante), en fecha 4 de febrero de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra DKV SEGUROS Y REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA con NIF A50004209 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La reclamación se recibe a través de la Autoridad Catalana de Protección de Datos indicando que los hechos no están comprendidos dentro de los supuestos sobre los que tiene competencia***.*** La reclamante manifiesta que ha recibido en su dirección de correo electrónico, en numerosas ocasiones, autorizaciones de pruebas médicas de terceros que no conoce. En algunos casos se incluye el tipo de prueba diagnóstica. Cada vez que ha recibido una autorización lo ha comunicado, reenviando el correo a la entidad (autorizaciones y atención al cliente). No se ha solventado y sigue recibiendo autorizaciones que no le corresponden.

Junto a la reclamación aporta copia de los correos electrónicos recibidos correspondientes a otras personas e intercambios de correos con el reclamado poniendo de manifiesto la situación.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, fue recibido en fecha 12 de marzo de 2021, como consta en el certificado que obra en el expediente.

En fecha 11 de abril de 2021, se recibe en esta Agencia escrito de respuesta indicando ***(…).***

TERCERO: En fecha 14 de junio de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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

En primer lugar, se verifica que no se encuentran notificaciones de brecha remitidas por el reclamado a esta Agencia.

Se verifica que la reclamante aporta conversaciones mantenidas por correo electrónico con el reclamado, de diferentes fechas. La primera conversación aportada contiene los siguientes documentos:

- Correo electrónico recibido el 08/10/2020 correspondiente a una tercera persona. En el correo aparece el nombre y apellidos de la tercera persona y una indicación sobre la autorización enviada: “Dicho documento está protegido con contraseña por seguridad, siendo el NIF del cliente para el que se solicita la autorización.” También figura “Si precisa cualquier aclaración o información al respecto, le atenderemos a través del correo electrónico ******EMAIL.1***.”

- Contestación al mismo, a la dirección indicada ******EMAIL.1*** indicando que no le corresponde.

- Contestación del reclamado a esta contestación de la reclamante con el texto “En estos momentos estamos trabajando en su solicitud…”.

- Segunda contestación del reclamado indicando “le informamos que debe ponerse en contacto con su sucursal … ******EMAIL.2***…”

- Correo electrónico de contestación de la reclamante al reclamado, reenviando toda la historia del correo a la dirección indicada “******EMAIL.2***”

- Contestación del reclamado a la reclamante indicando que “Lamentamos no poder atenderle en estos momentos ya que no disponemos de la documentación para poder gestionar correctamente su solicitud.”

Aporta una muestra de otros documentos relacionados con autorizaciones de terceras personas recibidas en su correo electrónico, correos recibidos en fechas 10/07/2020, 30/10/2020 (14:33h), 30/10/2020 (12:37h), 03/12/2020 y 26/01/2021.

En el de fecha 30/10/2020 (14:33h), dirigido a un “colaborador”, aparece la autorización adjunta sin indicación de que está protegida por contraseña, aportando la reclamante copia de dicha autorización en la que aparecen los siguientes datos, entre otros:

- Número de autorización.

- Datos del asegurado: nombre y apellidos y Número de póliza.

- Datos de la autorización/prueba:

“(…)”

“(…)”

En el de fecha 30/10/2020 (12:37h) aparece la autorización adjunta sin indicación de que está protegida por contraseña, pero la reclamante no aporta copia de la autorización.

Aporta copia de otra autorización de fecha 25/11/2020 en la que aparecen los siguientes datos, entre otros:

- Número de autorización.

- Datos del asegurado: nombre y apellidos y Número de póliza.

- Datos de la autorización/prueba:

“(…)”

“(…)”.

Aporta copia de un correo electrónico de fecha 15/12/2020, remitido por la reclamante a cuatro direcciones de correo electrónico (******EMAIL.3***, ******EMAIL.4***, *****EMAIL.5**, ******EMAIL.1***). En el correo lista los nombres de siete personas de las que ha recibido autorizaciones, exponiendo que en numerosas ocasiones recibe autorizaciones dirigidas a diferentes personas que no conoce ni tiene vínculo con ellas y que cada vez que ha recibido una autorización de este tipo lo ha notificado, sin corregirse el problema.

Sobre la cronología de los hechos.

(…).

Datos afectados.

(…).

Comunicación del incidente a los afectados.

(…).

Acciones tomadas para solucionar el incidente y minimizar el impacto.

(…).

Sobre la calificación del incidente como brecha de seguridad de datos personales.

(…).

Sobre las medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente en el tratamiento de datos involucrado.

(…).

Medidas adoptadas para que no se vuelva a producir un incidente similar en el futuro.

(…).

Contrato con encargados.

(…).

Contrato con VIVAZ.

(…).

Origen de la incidencia.

(…).

QUINTO: A la vista de los hechos denunciados y de conformidad con las evidencias que se disponen en este momento, la Inspección de Datos de esta Agencia Española de Protección de Datos considera que el tratamiento de los datos personales que realizó la parte reclamada no cumpliría las condiciones que impone la normativa vigente en materia de protección de datos, por lo que procede la apertura del presente procedimiento sancionador.

FUNDAMENTOS DE DERECHO

PRIMERO: De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

SEGUNDO: Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

1. Los datos personales serán:

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En relación con este principio, el Considerando 39 del referido RGPD señala que:

"[…]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".

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado vulneró el artículo 5.1 f) del RGPD, *principios relativos al tratamiento.*

En el caso concreto que se examina, consta que la parte reclamada remitió, desde el 16 de abril de 2020 al 9 de marzo de 2021, a tercera persona, 51 correos electrónicos que no iban dirigidos a ella.

En efecto, tal como se acredita en el expediente, consta que la reclamante recibió ***(…).***

Por otra parte, la parte reclamada reconoció los hechos, manifestando a esta Agencia que el incidente ***(…),*** concluyendo además ***(…).***

TERCERO: Establece el artículo 4.12 del RGPD que se considera "*violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione 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*."

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

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

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"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."

De las actuaciones practicadas consta la existencia de indicios razonables y suficientes de que las medidas de seguridad, tanto de índole técnica como organizativas, con las que contaba la parte reclamada en relación con los datos de salud que sometía a tratamiento, no eran las adecuadas en el momento de producirse los accesos indebidos.

La consecuencia de esta implantación de medidas deficientes de seguridad fue la exposición a tercera persona ajena de los datos personales relativos a la salud de

otros clientes, es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

Hay que añadir que, en relación con la categoría de datos a la que tercera persona ajena ha tenido acceso, se encuentran en la categoría de especiales según lo dispuesto en el art. 9 del RGPD, circunstancia que supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por el responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

El hecho de que trabajadores de dos encargados diferentes hayan cometido el mismo error demuestra que no se trata de un fallo humano concreto, sino de una defectuosa configuración del CRM, lo que pone manifiesto que dichos errores son tan sólo la muestra de la falta de medidas de seguridad adoptadas por el responsable.

CUARTO: El artículo 33 del RGPD, *Notificación de una violación de la seguridad de los datos personales a la autoridad de contro*l, establece que: *"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.*

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Si bien es cierto que la entidad reclamada conocido el incidente adoptó medidas tendentes a poner remedio al mismo, el artículo 33 del RGPD establece de forma explícita que las brechas de seguridad, siempre que en una brecha se vean afectados datos de carácter personal e implique un riesgo para los derechos y libertades de las personas físicas, deben notificarse por el responsable del tratamiento en el plazo de 72 horas después de que haya tenido constancia de ella a la Autoridad de Control (AEPD), circunstancia que se cumpliría en el presente caso, toda vez que además, los datos afectados pertenecen a la categoría de datos regulada en el artículo 9.1 del citado RGPD (Tratamiento de categorías especiales de datos personales).

En el presente caso, consta que el reclamado ha sufrido una brecha de seguridad de los datos personales teniendo constancia de ella desde el 13 de julio de 2020 y no lo ha notificado a esta Agencia. Una violación puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales. En el RGPD se explica que estos efectos pueden incluir la pérdida de control sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional. También puede incluir cualquier otro perjuicio económico o social significativo para esas personas.

Por último, el propio responsable de los tratamientos manifiesta que ***(…)*** ha provocado que sucedieran los hechos reclamados a esta Agencia, pero lo cierto es que la reclamante puso en conocimiento del incidente a la entidad reclamada, y esta hizo caso omiso del aviso.

De conformidad con lo que antecede, se estima que la actuación de la entidad podría suponer la vulneración del artículo 33 del RGPD, infracción tipificada en su artículo 83.4.a) del mismo texto legal.

QUINTO: De conformidad con las evidencias de las que se dispone en el presente momento de acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que la parte reclamada incumpliría lo dispuesto en el artículo 5.1.f) del RGPD, lo que podría suponer la comisión de una infracción tipificada en el artículo 83.5 del RGPD.

La falta de implementación de medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado en el tratamiento de datos personales podría constituir, por parte de la entidad reclamada, infracción a lo dispuesto en el artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD.

Asimismo, el incumplimiento del deber de notificar a la autoridad de protección de datos una violación de seguridad de los datos personales, podría constituir infracción a lo previsto en el artículo 33 del Reglamento, tipificada en el artículo 83.4.a) del mismo texto legal.

SEXTO: El artículo 83.5 del RGPD dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "Infracciones" determina lo siguiente: "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica."*

A efectos del plazo de prescripción de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente: *"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679."

La vulneración de los artículos 32 y 33 RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43."
(…)

A efectos del plazo de prescripción de las infracciones, el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves"*, establece lo siguiente:

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

(…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD, arriba transcritos.

SÉPTIMO: A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

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

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

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

liar 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,
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 con 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."

Sanción por la infracción del artículo 5.1.f) del RGPD.

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción por infracción del artículo 5.1 f), procede graduar la multa teniendo en cuenta:

Como agravante:
Artículo 83.2.a) RGPD: *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*:

El error se mantiene desde el 16/04/2020 al 09/03/2021.

Asimismo, la reclamante puso, de manera reiterada, en conocimiento de la reclamada la situación, sin que esta actuara de ninguna forma hasta recibir el traslado de la reclamación–"***(…)"***

En cuanto al volumen de los tratamientos efectuados, la reclamante recibe 51 correos electrónicos de 32 afectados distintos.

Artículo 83.2 g) RGPD*: las categorías de los datos de carácter personal afectados por la infracción;* toda vez que se han visto afectadas categorías especiales de datos personales. En este sentido, el RGPD otorga siempre al tratamiento de estos datos, una especial protección y consideración. Así el Considerando 75 del RGPD, considera el tratamiento de datos relativos a la salud, como tratamiento de riesgo.

Sanción por la infracción del artículo 32 del RGPD.

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción por infracción del artículo 32 del RGPD, procede graduar la multa teniendo en cuenta:

Como agravantes:

Artículo 83.2 g) RGPD*: las categorías de los datos de carácter personal afectados por la infracción;* toda vez que se han visto afectadas categorías especiales de datos personales. En este sentido, el RGPD otorga siempre al tratamiento de estos datos, una especial protección y consideración. Así el Considerando 75 del RGPD, considera el tratamiento de datos relativos a la salud, como tratamiento de riesgo.

Artículo 76.2 a) LOPDGDD: "El carácter continuado de la infracción." Es de destacar *el* carácter continuado de la infracción. El error se mantiene desde el 16/04/2020 al 09/03/2021.

Artículo 76.2 b) LOPDGDD:" La vinculación de la actividad del infractor con la realización de tratamientos de datos personales". La actividad de la entidad reclamada exige un continuo tratamiento de datos de carácter personal. Asimismo, la entidad reclamada realiza para el desarrollo de su actividad, un elevado volumen de tratamiento de datos personales.

Sanción por la infracción del artículo 33 del RGPD.

Artículo 83.2 g) RGPD*: las categorías de los datos de carácter personal afectados por la infracción;* toda vez que se han visto afectadas categorías especiales de datos personales. En este sentido, el RGPD otorga siempre al tratamiento de estos datos, una

especial protección y consideración. Así el Considerando 75 del RGPD, considera el tratamiento de datos relativos a la salud, como tratamiento de riesgo.

Artículo 76.2 b) LOPDGDD:" La vinculación de la actividad del infractor con la realización de tratamientos de datos personales". La actividad de la entidad reclamada exige un continuo tratamiento de datos de carácter personal. Asimismo, la entidad reclamada realiza para el desarrollo de su actividad, un elevado volumen de tratamiento de datos personales

Consta que el reclamado sufrió una brecha de seguridad de los datos personales teniendo constancia de ella desde el 13 de julio de 2020 y no lo notificó a esta Agencia.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 100.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad y de 60.000 € por cada una de las infracciones de los artículos 32 y 33 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales.

OCTAVO: Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

NOVENO: De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a DKV SEGUROS Y REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, con NIF A50004209, por la presunta infracción del artículo 5.1. f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD.

SEGUNDO: INICIAR PROCEDIMIENTO SANCIONADOR a DKV SEGUROS Y REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, con NIF A50004209, por la presunta infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción den el artículo 73 apartado f) de la LOPDGDD.

TERCERO: INICIAR PROCEDIMIENTO SANCIONADOR a DKV SEGUROS Y REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, con NIF A50004209, por la presunta infracción del artículo 33 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción en el artículo 73 r) de la LOPDGDD.

CUARTO: NOMBRAR instructor a ***B.B.B.*** y, como secretario, a ***C.C.C.***, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

QUINTO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

SEXTO: QUE a los efectos previstos en el art. 64.2 b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de 100.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad y de 60.000 € por cada una de las infracciones de los artículos 32 y 33 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales, sin perjuicio de lo que resulte de la instrucción.

SÉPTIMO: NOTIFICAR el presente acuerdo a DKV SEGUROS Y REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, con NIF A50004209, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en CIENTO SETENTA Y SEIS MIL EUROS (176.000€) resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en CIENTO SETENTA Y SEIS MIL EUROS (176.000€) y su pago implicará la terminación del procedimiento.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en CIENTO TREINTA Y DOS MIL EUROS (132.000 €.)

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (80000 euros o 36000 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-150322

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

>>

SEGUNDO**:** En fecha 28 de mayo de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **132000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos,

el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **PS/00080/2022**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **DKV SEGUROS Y REASEGUROS, S.A.E.**.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

936-240122

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