- **Expediente N.º: EXP202213638**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO:

(…) (en adelante, las parte reclamantes) con fecha 18 de noviembre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS*** con NIF ***A28007268*** (en adelante, GENERALI). Los motivos en que basa la reclamación son los siguientes:

En sus escritos, las partes reclamantes manifiestan haber recibido comunicación a través de correo electrónico o por vía postal de GENERALI en el cual se informaba del acaecimiento de un ciberincidente de seguridad en sus sistemas. Según el contenido

de dicha comunicación, el incidente se debió un "*acceso ilegítimo a los Sistemas de Información, que ha provocado que parte de la información que conservan de cuando fue cliente de GENERALI España, y en cumplimiento de nuestras obligaciones legales y contractuales, se ha podido ver expuesta."* Asimismo, se indica en la comunicación que dicha información *"podría incluir sus datos y los de los asegurados en su antigua póliza relativos a nombre, apellidos, dirección, teléfono fijo y móvil, correo electrónico, DNI, fecha y país de nacimiento, estado civil y el código IBAN de su cuenta corriente*".

De la documentación aportada por las partes reclamantes en sus diversos escritos destacan:

- Capturas de pantallas donde se muestra la comunicación recibida vía e-mail o correo postal por parte de GENERALI a través de la cual se facilita la información sobre la citada brecha de seguridad y su afectación a los datos personales de las partes reclamantes.
- Captura de pantalla de un correo remitido por uno de los reclamantes a la parte reclamada donde solicita el ejercicio del derecho de supresión de sus datos.
- Captura de pantalla de carta enviada por uno de los reclamantes a la parte reclamada solicitando la no renovación de la póliza y la cancelación de todos sus datos personales.
- Captura de pantalla de correo electrónico de uno de los reclamantes solicitando información del motivo por el que conservaban sus datos no siendo cliente de la compañía desde el año 2018, así como captura de pantalla de respuesta por la parte reclamada

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 dichas reclamaciones 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.

Los traslados, que se practicaron 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), fueron notificados formalmente como consta en los correspondientes acuses de recibo que obran en el expediente.

Con fecha 03/02/2023 se recibe en esta Agencia escritos de respuesta de dichos traslados, cuyo contenido se expone más abajo en el informe de investigación realizada por la Subdirección General de Inspección de Datos de la presente autoridad.

TERCERO:

Con fecha 07/02/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las reclamaciones presentadas por las partes reclamantes.

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, la cual finalizó con un informe donde constaban las siguientes conclusiones:

En relación con la detección de la brecha, el vector de entrada y su impacto, se concluye en el informe de las actuaciones de investigación que:

- El ataque se detectó el 5 de octubre de 2022 tras notar problemas de rendimiento y saturación en el servidor de aplicaciones. Dicho problema era consecuencia del elevado número de peticiones que el ataque estaba llevando a cabo en la aplicación de mantenimiento de clientes (SMC), la cual era utilizada por mediadores de seguros para acceder a los datos de los clientes mediados por ellos. Ha quedado constatado que los atacantes comprometieron las credenciales de acceso de uno de los corredores y las utilizaron para entrar en esta aplicación y ejecutar un ataque automatizado de fuerza bruta contra el formulario de consulta de clientes, realizando para ello intentos con múltiples números de NIF aleatorios. En esa misma fecha se tuvo constancia de que el ataque se venía realizando desde el 19 de septiembre de 2022 sin ser detectado por los sistemas de la parte reclamada.

- El día 6 de octubre de 2022 se averiguó el usuario a través del cual se estaba causando el ataque que estaba causando el ataque y se procedió al cambio de sus credenciales, lo que contuvo el ataque.

- Por declaración del responsable ha quedado constatado que, tras detectarse el ataque, no se pudo tener constancia de la afectación de datos personales puesto que se carecía de logs o trazas en la aplicación afectada, por lo que no se pudo conocer cuántas de las peticiones lanzadas por los atacantes llegaron a tener éxito. Afirman que en esta fecha únicamente se conocía el posible escenario potencialmente afectado, que correspondía a las 37 personas físicas (clientes o exclientes) de ese corredor de seguros. No obstante, en fecha posterior (11 de noviembre de 2022) se conoció que el escenario potencialmente afectado había sido bastante superior al existir un fallo en el software que estaba permitiendo a un corredor acceder a datos personales no solo de sus clientes sino también de cualquier excliente de GENERALI. En fecha 6 de octubre de 2022 se realizó una valoración inicial del nivel de riesgo y severidad de la brecha (con la información que se disponía) y se concluyó que no era necesario notificar el incidente a la AEPD ni a los afectados.

- El 11 de noviembre de 2022 se tuvo constancia de la filtración de datos personales al conocerse la venta de una base de datos de exclientes de GENERALI a través de un grupo de *Telegram*, obteniéndose como evidencia una muestra de 24315 registros que corroboraba la afectación de los siguientes datos personales filtrados:

- Nombre y Apellidos.
- DNI persona afectada.
- DNI tomador póliza.
- Teléfono1 y Teléfono2.
- Fecha y país de nacimiento.
- Estado Civil
- Dirección Completa, CP, Población, Comunidad.
- IBAN.

Fue en esta misma fecha cuando se detectó la existencia de un error en el software SMC que había permitido a las atacantes acceder no solo a los clientes del propio corredor afectado, sino también a todos los exclientes de la parte reclamada. En esta fecha se procede a realizar nueva evaluación del riesgo y severidad del incidente, concluyéndose la necesidad de notificar tanto a AEPD como a las personas afectadas.

En relación con la comunicación de la brecha a los afectados, ha quedado constatado que GENERALI procedió a comunicar a los exclientes potencialmente afectados de la siguiente forma:

- Para las personas incluidas en el fichero de muestra obtenido de los atacantes se informa el 15 de noviembre de 2022 vía email o correo postal. En total se informa a 24352 personas.
- Para extomadores de póliza no incluidos en fichero de muestra se comunicó vía email o correo postal en fechas comprendidas entre el 16 y 28 de noviembre de 2022 (1.092.543 personas potencialmente afectadas).
- Para exasegurados de pólizas individuales se carecía de datos de contacto y se decidió incluir la información en la comunicación realizada al extomador de la póliza (399153 personas potencialmente afectadas).
- Para exasegurados de pólizas colectivas se decide realizar una comunicación pública en WEB al carecerse de datos de contacto, esta comunicación estuvo visible desde 30 de noviembre de 2022 al 31 de marzo de 2023 (166621 personas potencialmente afectadas).

Ha quedado constatado que no existían análisis de riesgos para los derechos y libertades de las personas en la actividad de tratamiento afectada por la brecha, donde se hubieran identificado y evaluado las posibles amenazas que generen daños o perjuicios sobre las personas afectadas por estos tratamientos, y concluya con las medidas técnicas y organizativas adecuadas para gestionar dichos riesgos. Por el contrario, únicamente existía un documento donde se realizaba un análisis o descripción general del tratamiento con el propósito de determinar la necesidad de llevar a cabo una evaluación de impacto (EIPD), concluyendo que el tratamiento tiene un nivel de impacto bajo y que no es necesario llevar a cabo esta EIPD.

En relación con las medidas preventivas técnicas y organizativas implantadas en momentos previos a la brecha se acredita:

- ***(…)***

Respecto a las medidas reactivas implantadas tras la brecha de seguridad ha quedado acreditado:

- ***(…)***

Las carencias en las medidas técnicas desplegadas para registrar y monitorizar la actividad de los usuarios en la aplicación SMC ***(…)*** tuvo como consecuencia que, tras la detección del ataque en fecha 5 de octubre de 2022, no se pudo tener constancia de su impacto real y los datos personales de exclientes de la parte reclamada que habían sido accedidos, no siendo hasta el día 11 de noviembre de 2022 cuando se conoció el impacto de la filtración a través de la muestra obtenida. Tras la brecha se introducen nuevas medidas reactivas **para disponer de trazas completas en este aplicativo y controlar las transacciones solicitadas por los usuarios.**

En relación con los plazos de conservación de los datos personales de los exclientes que finalizaban su vínculo contractual (fin de pólizas de seguros) ha quedado constatado:

- ***(…).***
- Que tras finalizar la vinculación contractual de un cliente (fin de la póliza), se ponía fin al plazo de conservación de los datos personales para la finalidad con la que se habían recogido inicialmente (contrato de seguros). No obstante, ha quedado constatado que continuaba tratando los datos personales con otras finalidades que justifican haciendo referencia a la siguiente normativa:
    - Ley 50/1980 sobre desenvolvimiento del contrato de seguros (plazo conservación 2 años).
    - Ley 58/2003 sobre prescripción en materia tributaria (plazo conservación 4 años).
    - Código de Comercio sobre conservación de justificantes del negocio (plazo conservación 6 años).
    - Ley 20/2015 sobre conductas fraudulentas relativas a seguros (plazo conservación 5 años).
    - Ley 10/2010 sobre prevención blanqueo capitales (plazo conservación 5 años).

Pese a cambiar la finalidad por la que se seguían tratando los datos personales, ha quedado constatado que tanto los agentes de seguros (que tienen la condición de encargados de tratamiento) como corredores de seguros (que tienen condición de responsables de tratamiento), seguían accediendo a los datos personales de estos exclientes, aunque sin posibilidad de editarlos. Como medida reactiva tras la brecha se modificó la aplicación SMC para que los mediadores únicamente tuvieran acceso a datos de clientes con póliza en vigor (tomadores, asegurados y beneficiarios).

QUINTO:

De acuerdo con el informe recogido de la herramienta AXESOR, la entidad GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS es una empresa con un ***(…)*** euros en el año 2022. En relación con el volumen de negocio según el citado informe alcanza ***(…)***, expresado en “Volumen de primas del ejercicio 2022”, en el documento “Informe sobre la situación financiera y de solvencia” de dicho ejercicio 2022 y que ha sido incorporado al expediente.

SEXTO:

Con fecha 6 de febrero de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción de los artículos 5.1.f), 25, 32 y 35 del RGPD, tipificados en los artículos 83.4 del y 83.5 del RGPD.

SEPTIMO:

En fecha 14/03/2024 tuvo entrada en el registro de la presente autoridad escrito presentado por GENERALI, a través del cual se presentaban diversas alegaciones frente al acuerdo de inicio de fecha de 6 de febrero de 2024. Del contenido de dicho escrito destaca lo siguiente:

Acerca de las inexactitudes contenidas en el acuerdo de inicio del presente procedimiento sancionador:

La representación de Generali alega varias imprecisiones en el acuerdo de inicio del procedimiento sancionador de la Agencia Española de Protección de Datos.

Así, en primer lugar, Generali cuestiona la afirmación de que los datos de 800.000 exclientes, incluyendo información sensible como IBAN, aparecieron en un foro de Telegram y eran accesibles al público. Según Generali, esta afirmación no se corresponde con los documentos del expediente administrativo. Argumentan que un usuario de un foro de Telegram afirmó tener los datos personales, pero no proporcionó información específica ni evidencia de acceso público a estos datos. La empresa de ciberseguridad Lazarus detectó el mensaje y notificó a Generali, proporcionando una muestra limitada de datos para verificar la veracidad de la afirmación. No se ha probado que los datos estuvieran disponibles o accesibles públicamente en el foro de Telegram, solo que alguien afirmó poseerlos.

En cuanto a los perjuicios sufridos por los interesados, Generali argumenta que no se ha acreditado ningún perjuicio real a los afectados por la brecha de seguridad. Afirman que solo un reclamante ha manifestado la intención de buscar compensación por daños morales no acreditados, no existiendo otras reclamaciones de perjuicios en el expediente administrativo por lo que considera que los riesgos y daños mencionados son meramente potenciales y no reales.

Asimismo, se opone a la afirmación de que la infracción se agrava por el tratamiento de datos sensibles, incluyendo datos de salud. Generali refuta esto, señalando que el sistema afectado no contiene categorías especiales de datos según el artículo 9 del RGPD. Señala que Generali ha aportado registros de actividades de tratamiento y comunicaciones a los afectados, indicando que los datos comprometidos eran identificativos, de contacto y de medios de pago, pero no datos de salud.

Por otro lado, Generali defiende que, contrariamente a lo señalado por la AEPD, es legal y necesario que los mediadores de seguros accedan a información de exclientes para cumplir con diversas obligaciones. Además, la Ley de Contrato de Seguro establece plazos de prescripción (dos años para seguros de daños, cinco para seguros de personas) durante los cuales pueden surgir reclamaciones derivadas de contratos ya terminados. En este sentido, los mediadores necesitan acceso a la información para justificar su retribución y cumplir con obligaciones fiscales y contables, mientras que los agentes de seguros, actuando como encargados del tratamiento de las aseguradoras, necesitan acceder a la información relevante para cumplir con sus obligaciones legales y contractuales.

Sobre la afectación a los principios del derecho sancionador derivados de la interpretación efectuada por la AEPD.

Generali alega que el acuerdo de inicio incurre en importantes vulneraciones de los principios del derecho administrativo sancionador, particularmente el principio non bis in idem y las disposiciones del artículo 29.5 de la Ley de Régimen Jurídico del Sector Público (LRJSP) en relación con el concurso medial de infracciones.

Generali sostiene que la AEPD está imponiendo múltiples sanciones por hechos que son, en esencia, idénticos o están intrínsecamente relacionados, lo que compromete el principio non bis in idem. Este principio establece que una persona no puede ser sancionada dos veces por los mismos hechos. En este caso, la AEPD considera que Generali ha incurrido en cuatro infracciones distintas del RGPD: no adoptar medidas de seguridad adecuadas (artículo 32.1), no cumplir con el principio de protección de datos desde el diseño (artículo 25.1), no realizar una evaluación de impacto en la protección de datos (EIPD) (artículo 35), y vulnerar el principio de confidencialidad (artículo 5.1 f).

Generali argumenta que estas cuatro imputaciones derivan del mismo hecho: la brecha de seguridad en la aplicación SMC. Indica que la AEPD, al imponer sanciones por cada una de estas infracciones, estaría duplicando las sanciones por el mismo hecho, ya que todas las infracciones están inextricablemente vinculadas. Señala que la AEPD no está imputando la falta de medidas de seguridad en general, sino específicamente en relación con el tratamiento de datos en el SMC. Generali argumenta que la AEPD sigue un razonamiento inverso: toma el resultado de la brecha de seguridad para deducir la falta de medidas de seguridad, la ausencia de protección desde el diseño y la falta de una EIPD. Este enfoque, según Generali, es incorrecto y lleva a la imposición de múltiples sanciones por un único hecho.

Sobre las supuestas infracciones imputadas a Generali.

En esta alegación, Generali aborda de manera exhaustiva las infracciones específicas que la Agencia Española de Protección de Datos le imputa. La compañía sigue un orden argumentativo que difiere del acuerdo de inicio, comenzando por el principio de protección de datos desde el diseño.

En primer lugar, Generali explica el alcance del principio de protección de datos desde el diseño, tal como lo expone el Comité Europeo de Protección de Datos (EDPB) en sus Directrices 4/2019. Estas directrices detallan que las medidas técnicas y organizativas pueden variar desde soluciones técnicas avanzadas hasta la formación

básica del personal. Generali argumenta que ha cumplido con sus obligaciones en virtud del artículo 25.1 del RGPD, asegurando que ha llevado a cabo un análisis exhaustivo de los riesgos y aplicado las medidas necesarias para mitigar dichos riesgos. Afirma que el hecho consistente en que el sistema de Generali permitía a los mediadores acceder a datos de exclientes, lo cual, según Generali, está justificado por la normativa de distribución de seguros que impone ciertas obligaciones legales.

En cuanto a la supuesta vulneración del artículo 35 del RGPD, Generali defiende que no era necesaria una Evaluación de Impacto en la Protección de Datos (EIPD) para el aplicativo SMC. Generali sostiene que ha realizado un análisis de riesgos que concluyó que el tratamiento de datos no implicaba un alto riesgo para los derechos y libertades de los interesados. Además, argumenta que la AEPD pretende introducir nuevos criterios no contemplados en el RGPD, lo cual excede su competencia.

Respecto a la insuficiencia de medidas de seguridad (artículo 32 del RGPD), Generali reafirma que ha implementado medidas adecuadas para proteger los datos personales y que la brecha de seguridad fue resultado de factores ajenos a su control, como el compromiso de las credenciales de un mediador. Generali argumenta que ha adoptado medidas reactivas de manera diligente y que el hecho de que estas medidas se hayan implementado rápidamente demuestra su compromiso con la seguridad de los datos, no una admisión de insuficiencia previa.

Finalmente, sobre la supuesta vulneración del principio de confidencialidad (artículo 5.1.f del RGPD), Generali sostiene que la AEPD está sancionando la existencia de la brecha de seguridad como un resultado en lugar de una falta de medios, lo que contradice la jurisprudencia del Tribunal Supremo que establece que la obligación de seguridad es una obligación de medios, no de resultados. Generali argumenta que la notificación de la brecha a los afectados no debería interpretarse como una admisión de insuficiencia de las medidas de seguridad.

En conclusión, Generali defiende que cada una de las imputaciones realizadas por la AEPD se basa en supuestos incorrectos o en interpretaciones erróneas de la normativa aplicable, y que ha cumplido con sus obligaciones bajo el RGPD de manera diligente y adecuada.

Sobre la vulneración del principio de proporcionalidad:

Generali argumenta que, en caso de que se determine que ha infringido la normativa de protección de datos, se debe considerar el principio de proporcionalidad al determinar la sanción. Para ello, Generali cita la jurisprudencia del Tribunal Supremo, que establece que la sanción debe ser proporcional a la infracción cometida, considerando todas las circunstancias concurrentes.

Generali critica que la AEPD no haya realizado una evaluación meticulosa de estas circunstancias, y señala que no se han considerado atenuantes relevantes, como las medidas reactivas adoptadas rápidamente, la falta de sanciones previas, la notificación voluntaria del incidente a la AEPD, y la adhesión a códigos de conducta.

Generali también refuta las circunstancias agravantes aplicadas por la AEPD, argumentando que estas se basan en hechos inexactos o en una apreciación objetiva sin pruebas específicas de negligencia.

En conclusión, Generali sostiene que, si se llegara a determinar una infracción, la sanción debería ser significativamente menor debido a la presencia de varios atenuantes y la falta de justificación para las agravantes invocadas por la AEPD.

OCTAVO:

En fecha 12 de abril de 2024 tiene entrada en el registro de la presente autoridad escrito de Generali, a través del cual manifiesta haber procedido al abono del pago voluntario sin reconocimiento de responsabilidad, en los siguientes términos:

"XI: Que en uso de la facultad otorgada por el mencionado artículo 85.2 de la LPACAP, Generali ha procedido al abono del importe del 80% de la sanción propuesta, es decir, de la cuantía mencionada en el expositivo anterior. A tal efecto, se aporta como DOCUMENTO NÚMERO 1 justificante del pago efectuado por Generali.

XII. Que, como consecuencia del mencionado pago, mi representada renuncia al ejercicio ante esa AEPD de cualquier acción o recurso en vía administrativa contra la sanción que, eventualmente y frente a lo sustentado por Generali, pudiera imponerse, tal y como prescribe el artículo 85.3 de la LPACAP, por lo que manifiesta que no interpondrá contra la resolución que finalmente se dictase, recurso potestativo de reposición ante esa AEPD.

XIII. Que, no obstante, y como se ha indicado en los expositivos anteriores, el mencionado pago se realiza en uso de la facultad establecida en el artículo 85.3 y no supone en ningún caso conformidad con el contenido del Acuerdo de Inicio ni con el de la resolución que en su caso se dictase, si se correspondiese, en todo o en parte, con el contenido de dicho Acuerdo. Del mismo modo, la realización del citado pago en ningún caso debe ser interpretado como un reconocimiento por parte de Generali de la responsabilidad por la comisión de las supuestas infracciones que pudieran serle imputadas en la citada resolución. A tal efecto, se reitera expresamente la intención de Generali de impugnar la citada resolución, en caso de no implicar el archivo del presente expediente, ante la jurisdicción contencioso-administrativa."

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO:

Queda acreditado, que en fecha el 5 de octubre de 2022, fue detectado por la parte reclamada un ataque de fuerza bruta contra el formulario de consulta de clientes mediante el uso de credenciales de un corredor, realizando para ello intentos con múltiples números de NIF aleatorios y respecto al cual se decidió no notificar el incidente.

Este hecho ha sido confirmado por la propia parte reclamada durante el transcurso de las actuaciones de investigación *"El 5/10/22 se detectó ataque de fuerza bruta usando credenciales de un corredor. Aplicadas las reglas de ENISA y la AEPD se decide no*

notificar el incidente (que podría afectar a 37 interesados). En esa fecha se bloquea el acceso a dicho corredor y se modifican sus credenciales, cesando el ataque."

SEGUNDO:

En fecha 11 de noviembre de 2022 se tuvo constancia por la parte reclamada de la filtración de datos personales en virtud del ataque producido tras una comunicación de la empresa de ciberseguridad ***(…)*** que afectaban e los siguientes datos personales:

- Nombre y Apellidos.
- DNI persona afectada.
- DNI tomador póliza.
- Teléfono1 y Teléfono2.
- Fecha y país de nacimiento.
- Estado Civil
- Dirección Completa, CP, Población, Comunidad.
- IBAN.

TERCERO:

Ha quedado constatado que GENERALI procedió a comunicar a exclientes potencialmente afectados de la brecha producida, en virtud del artículo 33 del RGPD de la siguiente forma:

- Para las personas incluidas en el fichero de muestra obtenido de los atacantes se informa el 15 de noviembre de 2022 vía email o correo postal a un total de 24.352 personas.
- Para extomadores de póliza no incluidos en fichero de muestra se comunicó vía email o correo postal en fechas comprendidas entre el 16 y 28 de noviembre de 2022 a un total de 1.092.543 personas potencialmente afectadas.
- Para exasegurados de pólizas individuales se carecía de datos de contacto y se decidió incluir la información en la comunicación realizada al extomador de la póliza (399153 personas potencialmente afectadas).
- Para exasegurados de pólizas colectivas se decide realizar una comunicación pública en WEB al carecerse de datos de contacto, esta comunicación estuvo visible desde 30 de noviembre de 2022 al 31 de marzo de 2023 (166621 personas potencialmente afectadas).

CUARTO:

Ha quedado constatado que en el momento del ataque la parte reclamada no disponía de análisis de riesgos para los derechos y libertades de las personas en la actividad de tratamiento con el fin de identificar y evaluado las posibles amenazas que generen daños o perjuicios sobre las personas afectadas por estos tratamientos.

Este hecho se manifiesta en las actuaciones de investigación a través de las cuales se solicitó de forma reiterada la aportación del citado análisis de riesgo, recibiendo como

respuesta que "*el tratamiento es previo a la entrada en vigor del RGPD,* ***(…)*****,** *por lo que no ha sido objeto de un análisis posterior al ya aportado, sin perjuicio de las medidas adoptadas como consecuencia de la brecha de seguridad detectada".*

QUINTO:
Queda acreditado que, en el momento del ataque, la parte reclamada no tenía aprobada una Evaluación de Impacto de Protección de Datos (EIPD) para el tratamiento de su actividad.

Ello se desprende de la propia manifestación de la parte reclamada, así como del documento aportada por la misma a través del cual se realizaba un análisis o descripción general del tratamiento con el propósito de determinar la necesidad de llevar a cabo una evaluación de impacto (EIPD), concluyendo que el tratamiento tenía un nivel de impacto bajo y que no era necesario llevar a cabo esta EIPD.

SEXTO:
Queda acreditado que, en el momento del ataque, no estaba implementado el segundo factor de autenticación en los aplicativo de la parte reclamada para los mediadores de seguro.

Este hecho ha sido manifestado por la parte reclamada y confirmado mediante la acreditación de las medidas reactivas implementadas tras el acaecimiento de la brecha: ***"(…)"***

SEPTIMO:
Queda acreditado que, hasta la adopción de las medidas reactivas por la parte reclamada tras la brecha producida, **y debido a un fallo técnico en la actualización del software Sistema de Mantenimiento de Clientes (SMC),** los mediadores de seguros podían acceder tanto a datos de sus clientes como de exclientes que ya no tenían vinculo contractual ya fueron extomadores de pólizas como de exasegurados en póliza.

Ello ha sido corroborado por la parte reclamada y confirmado en la comunicación de las medidas reactivas: ***"(…)."***

OCTAVO:
Ha quedado constatado **la inexistencia de logs las transacciones para garantizar la trazabilidad en el sistema, lo cual impidió conocer de forma inmediata el impacto real de la brecha y los datos personales afectados**. Ello se desprende de la propia manifestación de la parte reclamada durante el transcurso de las actuaciones de investigación: **"No hay logs de aplicativos que permitan ayudar a definir cuántos hits de aciertos ha tenido el ataque masivo***".*

NOVENO:
De las actuaciones de investigación realizados queda acreditado que GENERALI poseía, en el momento previo a la brecha, las siguientes medidas preventivas técnicas y organizativas:

- ***(…)***

DÉCIMO:

Queda acreditado que GENERALI adoptó las medidas reactivas implantadas tras la brecha de seguridad:

- ***(...)***

FUNDAMENTOS DE DERECHO

I Competencia

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

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

II Terminación del procedimiento

El artículo 85 apartado segundo de la LPCAP establece que *"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."*

Dicho abono voluntario implica, tal y como indica el apartado tercero del mismo artículo, la reducción correspondiente sobre el importe de la sanción: *"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."*

En estos términos, teniendo en cuenta el abono voluntario que ha realizado y comunicado Generali antes de que se dictase propuesta de resolución por parte de esta autoridad, se procede a la terminación del presente procedimiento sancionador en los términos indicados en la parte dispositiva de esta resolución.

No obstante, resulta oportuno destacar que, de forma previa al citado pago voluntario, Generali presentó escrito de alegaciones frente al acuerdo de inicio, procediendo a un análisis pormenorizado de las infracciones indicadas y rebatiendo jurídicamente cada una de ellas. Dicho hecho obliga a la presente autoridad a pronunciarse sobre tales alegaciones y ello en virtud de lo dispuesto del artículo 88 de la LPACAP, el cual establece de forma expresa que:

"La resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo."

Por lo expuesto, en cumplimiento de dicho mandato legal, a través de la presente resolución se procede a la contestación de las alegaciones formuladas por Generali frente al acuerdo de inicio, amén de declarar la terminación del procedimiento por pronto pago en los términos establecidos en el artículo 85.2 y 88 de la LPACAP.

III Contestación a las alegaciones formuladas frente al acuerdo de inicio

Acerca de las inexactitudes contenidas en el acuerdo de inicio del presente procedimiento sancionador.

En primer lugar, Generali afirma que los datos de los exclientes no fueron accesibles al público a través de un foro de Telegram. Sin embargo, de las actuaciones de investigación realizadas se desprende que el 11 de noviembre de 2022 fue confirmada la venta de una base de datos de exclientes de Generali en un grupo de Telegram, lo que corrobora la exposición pública de estos datos. Así, en las citadas conclusiones del inspector actuante se indica de forma expresa que se tuvo constancia por parte de GENERALI de la filtración de datos personales:

"El 11 de noviembre de 2022 se tuvo constancia de la filtración de datos personales al conocerse la venta de una base de datos de exclientes de GENERALI a través de un grupo de Telegram, obteniéndose como evidencia una muestra de 24315 registros que corroboraba la afectación de los siguientes datos personales filtrados:
o Nombre y Apellidos.
o DNI persona afectada.
o DNI tomador póliza.
o Teléfono1 y Teléfono2.
o Fecha y país de nacimiento.
o Estado Civil
o Dirección Completa, CP, Población, Comunidad.
o IBAN"

Dicha evidencia contradice la afirmación de Generali de que no hubo acceso público a los datos comprometidos.

Por otro lado, dicho hecho viene confirmado por Generali durante el transcurso de las actuaciones de investigación, como contestación al previo requerimiento de la presente autoridad respecto a los posibles sitios web donde la información estuvo filtrada, indicando en relación ello que el proveedor Lazarus les trasladó que los datos se habían localizado a través de un grupo de Telegram.

No obstante lo anterior, conviene destacar que independientemente de que los datos fueran o no accesibles en un foro, el simple hecho de que hayan sido expuestos a un tercero no autorizado constituye ya una violación del principio de confidencialidad en los términos establecidos por el artículo 5.1 f) RGPD.

En relación a los perjuicios sufridos por los afectados, Generali sostiene que no se ha probado ningún daño real. A tal respecto, resulta fundamental destacar que, teniendo en cuenta el contenido del RGPD, no es necesario que se produzca un daño "real" para que se cometan las infracciones propuestas en el acuerdo de inicio. En el RGPD, la vulneración del principio de confidencialidad prevista en el artículo 5.1.f), la protección de datos por el defecto señalada en el artículo 25, la adopción de medidas de seguridad adecuadas al riesgo prevista en el artículo 32, o la obligación de la Evaluación de Impacto exigida por el artículo 35 del RGPD, no se exige en ninguna de ellas que se produzca un daño "real" para que dichos preceptos se entiendan infringidos.

A tal respecto, resulta importante determinar lo que se entiende por daño o perjuicio en el contexto del RGPD y los derechos de los interesados. Generali argumenta que no se ha probado ningún daño "real", pero no especifica si se refiere a un daño tangible o físico, un perjuicio económico, o si está limitando el daño a una manifestación material y concreta.

El RGPD establece claramente en su artículo 5.1.f) que la pérdida de confidencialidad de los datos personales constituye una infracción, ya que los datos expuestos quedan a disposición de terceros no autorizados. Este hecho, din duda afecta al titular de los datos, al perder su capacidad de control sobre sus datos personales. Además, el considerando 85 del RGPD indica que la pérdida de confidencialidad e integridad supone un riesgo que puede conllevar daños físicos, materiales o inmateriales, lo cual demuestra que no es necesario un daño tangible o económico para que el RGPD considere que se ha vulnerado el derecho del interesado:

"*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 definitiva, la infracción del RGPD no exige un "daño real" o tangible para considerarse como tal. La pérdida de control sobre los datos y la materialización del riesgo ya constituye una violación de los derechos del interesado, de acuerdo con lo anteriormente indicado.

La protección de datos de carácter personal supone un derecho fundamental que debe ser garantizado y la vulneración de las obligaciones indicadas por el RGPD se producen con independencia de si se materializa o no en un daño tangible para los

individuos afectados. Debe de tenerse en cuenta que el reglamento se enfoca en la prevención de riesgos y en la protección de los derechos y libertades de los individuos lo cual implica que en diversas ocasiones la mera posibilidad de que los datos puedan ser utilizados de manera indebida ya es suficiente para considerar que se ha vulnerado alguna de las obligaciones previstas por la norma.

Por lo expuesto, la argumentación de Generali sobre la supuesta ausencia de perjuicios reales no resulta suficiente para justificar el incumplimiento de sus obligaciones. La normativa de protección de datos se basa en identificar los riesgos en los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, así como en prevenir y mitigar la materialización de los riesgos asociados al tratamiento de datos personales. La falta de prueba de un daño concreto para cada afectado no exime a Generali de su responsabilidad en el cumplimiento de las obligaciones previstas en el RGPD.

Respecto a los datos pertenecientes a categorías especiales, Generali alega que el sistema afectado no contenido categorías de datos especiales de los previstos en el RGPD. Sin embargo, es importante señalar que, tal y como conoce la parte reclamada, Generali gestiona seguros de salud, lo que implica necesariamente el tratamiento de datos relativos a la salud, los cuales se encuentran dentro del artículo 9 del RGPD como categorías especiales de datos personales.

El hecho de que la brecha de datos personales no haya afectado específicamente a este tipo de datos en esta ocasión no exime a Generali del cumplimiento de las obligaciones previstas en el RGPD teniendo en cuenta la naturaleza de este tipo de datos especiales de los que forma parte su tratamiento. Ello implica que las evaluaciones de impacto en la protección de datos (EIPD), las medidas de seguridad y el diseño de los sistemas por defecto deben tener en cuenta las circunstancias especiales, así como los riesgos inherentes a la gestión de los citados datos.

Por lo expuesto, la argumentación de Generali ***(…)*** no resulta suficiente para desvirtuar las obligaciones más amplias que tienen en virtud del RGPD. Si bien, la existencia de tales datos no es el fundamento principal en el incumplimiento de las obligaciones por parte de Generali, sí que puede ser tenido en cuenta a efectos de valorar la gravedad de la infracción.

Por último, Generali defiende la necesidad legal de que los mediadores de seguros accedan a información de exclientes para cumplir con diversas obligaciones contractuales y normativas. A tal respecto resulta crucial diferenciar entre el cumplimiento de la obligación de mantener los datos de exclientes para efectos de obligaciones legales y el acceso a esos datos por parte de los mediadores respecto de personas que ya no poseen la condición de cliente.

En este contexto, Generali tiene la obligación de conservar los datos personales de exclientes para cumplir con varias disposiciones normativas, como las relacionadas con las obligaciones fiscales, el blanqueo de capitales, y las reclamaciones contractuales que pueden surgir incluso después de la finalización de la relación contractual. No obstante, esta obligación de conservación no justifica el acceso abierto a estos datos por parte de los mediadores de seguros. Permitir a los mediadores de seguros acceso sin restricción alguna a la información de exclientes, además de

vulnerar el principio de confidencialidad, compromete gravemente la protección y la seguridad de los datos personales.

Aunque Generali tenga la obligación de conservar estos datos por razones legales, dicha obligación no exime de la responsabilidad de garantizar que el acceso esté restringido exclusivamente al personal autorizado, en relación las funciones del puesto de trabajo y bajo circunstancias justificadas.
Conservar los datos personales de exclientes no implica que cualquier empleado o mediador de seguros tenga derecho a acceder libremente a esta información, pues ello supone un uso indebido y desproporcionado que no está justificado por la naturaleza de la obligación de conservación.

De hecho, tales afirmaciones son también compartidas por la parte reclamada. De las actuaciones de investigación se desprende que, tras la brecha, Generali implementó medidas para restringir el acceso de los mediadores solo a los datos de clientes con pólizas en vigor, hecho que manifiesta que las actuaciones anteriores resultaban insuficientes para garantizar la protección adecuada de los datos personales, tal y como consta en el hecho probado séptimo

Alegación segunda: Sobre la afectación a los principios del derecho sancionador derivados de la interpretación efectuada por la AEPD

Generali argumenta que el acuerdo de inicio incurre en vulneraciones de los principios del derecho administrativo sancionador, particularmente el principio non bis in idem y las disposiciones del artículo 29.5 de la Ley de Régimen Jurídico del Sector Público (LRJSP) en relación con el concurso medial de infracciones. En este sentido, conviene en primer lugar hacer una breve referencia a la aplicación del mencionado principio en el ámbito europeo, teniendo en cuenta la naturaleza que posee el RGPD.

El artículo 50 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) establece el principio non bis in idem, que prohíbe el doble enjuiciamiento y la doble sanción penal dentro de la Unión Europea. A diferencia del artículo 4 del Protocolo 7 del Convenio Europeo de Derechos Humanos (CEDH), que se aplica solo a nivel nacional, el artículo 50 de la CDFUE tiene un alcance transnacional, protegiendo a las personas de ser juzgadas o sancionadas dos veces por la misma infracción en cualquier Estado miembro de la Unión Europea, siempre que se aplique el Derecho de la Unión.

Bajo el título "Derecho a no ser juzgado o condenado penalmente dos veces por la misma infracción", el artículo 50 dispone:

"Nadie podrá ser juzgado o condenado penalmente por una infracción respecto de la cual ya haya sido absuelto o condenado en la Unión mediante sentencia penal firme conforme a la ley."

La Carta, considerada fuente primaria del Derecho de la Unión según el artículo 6 del Tratado de la Unión Europea, contempla a todos los Estados miembros como un único espacio jurídico en lo que respecta a la regla del non bis in idem, siempre que apliquen el Derecho de la Unión.

Asimismo, el Tribunal de Justicia de la Unión Europea ha aplicado los criterios Engel, originados en la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH), para interpretar el artículo 50 de la CDFUE. Estos criterios determinan si una sanción tiene carácter penal basándose en la calificación jurídica de la infracción, la naturaleza de la infracción y la sanción, así como la gravedad de la sanción. De este modo, la prohibición del doble castigo puede extenderse no solo a procesos penales sino también a procedimientos administrativos con sanciones de carácter o naturaleza penal.

La Carta, en su artículo 52.3, dispone que los derechos que correspondan a derechos garantizados por el CEDH tendrán el mismo sentido y alcance. El TJUE ha destacado que el artículo 50 de la CDFUE debe interpretarse de manera uniforme y autónoma, sin depender de la ratificación o reservas al CEDH por parte de los Estados miembros.

En cuanto a los requisitos jurisprudenciales establecidos por el TJUE para que tenga lugar el mencionado principio reconocido en el artículo 50 el tribunal europeo ha manifestado en diversas sentencias (STJUE de 18 de julio de 2007, Lucchini Siderurgica, C-119/05, EU:C:2007:434, STJUE de 16 de noviembre de 2010, Mantello, C-261/09, EU:C:2010:683, Sentencia de 20 de marzo de 2018, Menci, C-524/15, EU:C:2018:197) la necesidad de concurrencia de tres criterios para que concurra el citado principio:

- Identidad del infractor: La misma persona o entidad debe ser objeto de los procedimientos o sanciones. *"El mismo individuo debe ser objeto de ambos procedimientos o sanciones. Esto asegura que no se persiga judicialmente o sancione a diferentes personas por los mismos hechos."*

- Identidad de los hechos: Los hechos deben ser los mismos ("idem factum"), es decir, un conjunto de circunstancias concretas indisolublemente ligadas entre sí. *"Los hechos materiales deben ser los mismos. Esto significa que deben ser un conjunto de circunstancias concretas derivadas de acontecimientos que son, en esencia, los mismos en la medida en que implican al mismo autor y están indisolublemente ligados en el tiempo y el espacio."*

- Identidad de la norma protegida: *"La infracción debe afectar al mismo bien jurídico protegido."*

No obstante, este principio ha sido matizado y modulado por la doctrina jurisprudencial del TJUE, entre la cual podemos destacar las siguientes resoluciones referidos al alcance del mismo:

- Sentencia de 22 de marzo de 2022, Nordzucker, C-151/20, EU:C:2022:203: El TJUE reafirma en esta sentencia la importancia de la identidad de los hechos materiales ("idem factum") para aplicar el principio non bis in idem. El tribunal permite la acumulación de procedimientos sancionadores cuando las sanciones se derivan de diferentes infracciones legales que persiguen distintos intereses generales. En el caso de Nordzucker, aunque las conductas sancionadas estaban relacionadas, las infracciones legales eran distintas, justificando así la acumulación de sanciones.

- Sentencia de 20 de marzo de 2018, Menci, C-524/15, EU:C:2018:197:La sentencia Menci aborda la cuestión de la duplicación de sanciones penales en el contexto de la evasión fiscal. El TJUE establece que el principio non bis in idem prohíbe la duplicación de sanciones penales por los mismos hechos, pero permite excepciones cuando las sanciones persiguen objetivos complementarios de interés general. Además, el tribunal subraya la necesidad de proporcionalidad y coordinación en la acumulación de sanciones. En este caso, la acumulación de sanciones fiscales y penales se consideró justificada debido a los objetivos complementarios en juego.

- Sentencia de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105 :En la sentencia Åkerberg Fransson, el TJUE analiza la aplicación del principio non bis in idem en el contexto de sanciones fiscales y penales por la misma infracción de no declarar impuestos. El tribunal concluye que la acumulación de sanciones administrativas y penales por los mismos hechos no es contraria al principio non bis in idem si se respetan los principios de proporcionalidad y coordinación. En este caso, tanto la multa fiscal como el proceso penal fueron considerados de carácter penal, pero la acumulación de sanciones se permitió bajo ciertas condiciones.

En resumen, el principio non bis in idem según el artículo 50 de la CDFUE y su interpretación por el TJUE protege a las personas de ser sancionadas dos veces por la misma infracción en cualquier Estado miembro de la Unión Europea, garantizando un espacio jurídico único y coherente en la aplicación del Derecho de la Unión. Este marco legal y jurisprudencial resulta útil para analizar la alegación de Generali sobre la supuesta vulneración de este principio por parte de la AEPD.

En el caso que nos ocupa, respecto a las infracciones indicadas en el acuerdo de inicio, si bien sí existe identidad del infractor, no ocurre lo mismo con la identidad de los hechos y el bien jurídico protegido. En este sentido, teniendo en cuenta la naturaleza administrativa y específica de la norma el bien jurídico protegido no puede ser entendido de forma general como la protección de los datos personales, sino el principio o principios o contenido esencial que en dicha materia se basa la obligación o infracción concreta y motiva la sanción. Teniendo en cuenta los criterios anteriormente citados, se desprende que cada una de las infracciones indicadas en el acuerdo son independientes y diferenciadas, en los términos que seguidamente se exponen:

Vulneración del principio de confidencialidad (artículo 5.1.f del RGPD)

La obligación de confidencialidad que el artículo 5.1.f) del RGPD impone al responsable del tratamiento es una obligación de resultado, de tal manera que para que el precepto se encuentre infringido es preciso que se quiebre la confidencialidad de los datos. De esta forma, nos encontraríamos ante una infracción de resultado, a diferencia de lo dispuesto el artículo 32 del RGPD, que como luego se verá, impone una obligación de medios.

En el caso que nos ocupa, los hechos que suponen la vulneración de dicho principio y, en consecuencia, la infracción, se manifiesta en la brecha de datos personales acaecida. Como resultado del ataque, se produjo la exposición no autorizada de datos personales, incluyendo nombres, direcciones, números de teléfono, DNI, y datos bancarios como el IBAN.

Ciertamente, el principio de responsabilidad previsto en el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispone que: "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."

No obstante, según lo dictaminado en la STS 7887/2011 de 24 de noviembre de 2011, Rec. 258/2009, "(...) desde su sentencia 76/1990, de 26 de abril, el Tribunal Constitucional viene declarando que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, doctrina que se reafirma en la sentencia 164/2005, de 20 de junio de 2005 , 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. Ahora bien, 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."

Sucede así que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad (véase la sentencia de esta Sala del Tribunal Supremo de 20 de noviembre de 2011, recurso de casación en interés de ley 48/2007), 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."

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en la STS 6262/2009, de 9 de octubre de 2009, Rec 5285/2005, y STS 6336/2009, de 23 de octubre de 2009, 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".

Así las cosas, ninguna de las circunstancias concurrentes en el caso permite excluir este elemento subjetivo de la infracción.

En cuanto al bien jurídico protegido por el artículo 5.1.f del RGPD es la confidencialidad de los datos personales**.** Este principio establece que los datos personales deben ser tratados de manera que se garantice una seguridad adecuada, incluyendo la protección contra el tratamiento no autorizado o ilícito. La

confidencialidad implica que los datos personales no sean accesibles ni divulgados a personas no autorizadas y que se mantengan protegidos en todo momento durante su tratamiento.

Protección de datos desde el diseño y por defecto (artículo 25.1 del RGPD)

El artículo 25.1 del RGPD establece la obligación de los responsables del tratamiento de integrar medidas organizativas y técnicas apropiadas de todo tipo, desde el diseño y por defecto. Esta disposición asegura que la protección de datos personales sea considerada y aplicada desde las fases más tempranas de desarrollo y durante todo el ciclo de vida del tratamiento de datos. La protección desde el diseño implica identificar, evaluar y analizar los riesgos en los derechos y libertades de los interesados, adoptando todo tipo de medidas técnicas y organizativas apropiadas a los efectos de mitigar dichos riesgos referidos al tratamiento que se pretende llevar a cabo antes de iniciarlo, a los efectos de 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 RGPD y proteger los derechos de los interesados . Por otro lado, la protección de datos por defecto se refiere aplicar las medidas técnicas y organizativas apropiadas de todo tipo 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. 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, limitando la cantidad de datos personales recolectados y procesados a lo estrictamente necesario, garantizar que los datos personales sean accesibles solo a personas autorizadas y para fines autorizados, y establecer configuraciones predeterminadas que prioricen la seguridad.

En el caso de Generali, la infracción se evidencia en ***(…).*** La falta de estas medidas permitió el acceso no autorizado a datos personales de exclientes, y la configuración del sistema no garantizaba el principio de minimización en el tratamiento de datos personales ni restringía el acceso solo a datos necesarios y limitado a finalidades determinadas.

Resulta crucial entender que en este caso el hecho objeto de infracción no es la brecha de datos personales en sí misma, sino las carencias en el diseño y configuración de sus sistemas y procesos. En este caso, la brecha fue el acontecimiento que permitió descubrir la deficiencia del sistema implementado y, por ende, el incumplimiento del principio, pero no la causa del incumplimiento. El artículo 25.1 del RGPD obliga a los responsables del tratamiento de datos a integrar medidas de protección de datos desde la fase de diseño de cualquier sistema que trate datos personales y a asegurar que, por defecto, solo se procesen los datos necesarios para cada finalidad específica. Ello implica que, independientemente de si ocurre o no una brecha, el sistema debe estar concebido y operado de tal manera que minimice la posibilidad de exposición indebida de datos personales. Por lo tanto, el hecho objeto de sanción bajo el artículo 25.1 del RGPD ***(…),*** y no la brecha de datos personales que posteriormente ocurrió. Constituye, por tanto, una infracción en sí mismo y de manera independiente de la brecha de datos personales.

El bien jurídico protegido por el artículo 25.1 del RGPD es la protección de los datos personales desde su concepción y durante todo su ciclo de vida. Este artículo asegura

que se adopten medidas proactivas para integrar salvaguardias de protección de datos en el diseño de sistemas y procesos y que se configuren dichos sistemas de manera que se priorice la protección por defecto. El contenido esencial se centra en asegurar que la protección de los datos no sea un añadido posterior o una consideración secundaria, sino una parte integral del diseño y funcionamiento de todos los sistemas y procesos que tratan datos personales.

Insuficiencia de medidas de seguridad adecuadas al riesgo (artículo 32 del RGPD)

El artículo 32 del RGPD es un precepto clave que establece la obligación de los responsables y encargados del tratamiento de implementar medidas técnicas y organizativas de seguridad adecuadas para garantizar la seguridad de los datos personales. Este artículo destaca la importancia de proteger los datos contra diversas amenazas, como la destrucción, pérdida, alteración, comunicación o acceso no autorizados. A través de estas medidas, el RGPD busca asegurar que los datos personales se mantengan seguros y protegidos en todo momento.

El artículo 32 no especifica medidas exactas que deben adoptarse, sino que exige que estas medidas sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo que supone el tratamiento de los datos personales. Ello supone que los responsables del tratamiento deben evaluar continuamente los riesgos y adaptar sus medidas de seguridad en consecuencia, obligación que no es una garantía de que no ocurrirán brechas de datos personales, sino más bien una obligación de medios para garantizar un nivel de seguridad adecuado al riesgo del tratamiento concreto.

La seguridad de los datos personales, como bien jurídico protegido por el artículo 32, abarca tanto aspectos técnicos (como el uso de cifrado y seudonimización) como organizativos (como políticas de acceso y procedimientos de formación). Este enfoque integral garantiza que se aborden todos los aspectos de la seguridad de los datos, desde la infraestructura técnica hasta la conducta del personal.

El artículo 32 del RGPD, a diferencia del 5.1 f), impone una obligación de medios, lo que significa que los responsables del tratamiento deben demostrar que han tomado todas las medidas técnicas y organizativas apropiadas de seguridad para garantizar un nivel de seguridad adecuado al riesgo, en lugar de garantizar un resultado específico. Esto se traduce en la necesidad de un enfoque proactivo y continuo para la gestión de la seguridad de los datos, ajustando las medidas según evolucionen los riesgos y las amenazas.

En el caso que nos ocupa la falta de adopción de medidas técnicas y organizativas apropiadas se manifestó a través de la brecha de datos personales; sin embargo, no fue ésta la que conllevó el incumplimiento de la obligación prevista en el artículo 32. Por el contrario, fue la posterior verificación de las medidas adoptadas, lo que puso en evidencia el incumplimiento de dicha obligación de manera independiente de la brecha de datos personales (no había medidas adecuadas aún si no se hubiera producido la brecha) y, en consecuencia, la infracción prevista en el RGPD.

La finalidad del artículo 32 del RGPD es la procurar un nivel de seguridad adecuado al riesgo del tratamiento de datos personales, a través de la aplicación de medidas técnicas y organizativas apropiadas de seguridad, específicamente de seguridad, pues

aquí la Ley sí distingue. Y todo ello es independiente de que se produzca una pérdida de confidencialidad y/o de integridad, pues la ausencia de dicho nivel de seguridad adecuado al riesgo tiene entidad por sí mismo para determinar la vulneración del precepto.

Asimismo, nos remitimos respecto del incumplimiento de esta obligación a lo que se ha contestado en la alegación tercera en relación con la falta de medidas técnicas y organizativas en relación con la brecha de datos personales.

Falta de Evaluación de Impacto en la Protección de Datos (artículo 35 del RGPD)

El artículo 35 del RGPD establece la obligación de realizar una Evaluación de Impacto en la Protección de Datos cuando un tipo de tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas.
Tal y como establecen las Directrices del Grupo de Trabajo del Artículo 29 sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 Adoptadas el 4 de abril de 2017:

"Una EIPD es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales4 evaluándolos y determinando las medidas para abordarlos. Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento"

En el presente supuesto, el hecho que motiva el incumplimiento y la infracción consiste precisamente en la falta de realización de una EIPD, a pesar de que los riesgos inherentes a sus tratamientos de datos lo requerían. En consecuencia, ni la brecha acaecida ni la falta de adopción de las medidas tienen relevancia alguna en el incumplimiento de la obligación; únicamente la ausencia de dicha evaluación cuando se está obligado a ello es el hecho que determina el incumplimiento del artículo 35 del RGPD.

Generali no realizó una EIPD a pesar de que sus operaciones de tratamiento de datos presentaban altos riesgos para los derechos y libertades de los interesados. Como se indicaba en el acuerdo de inicio, Generali actúa en un entorno donde se tratan grandes volúmenes de datos personales, algunos de los cuales tienen naturaleza sensible.

El bien jurídico protegido por el artículo 35 del RGPD es la evaluación y mitigación de riesgos en los derechos y libertades de las personas físicas asociados al tratamiento de datos personales. Este artículo exige que los responsables del tratamiento realicen una EIPD cuando las operaciones de tratamiento puedan suponer un alto riesgo para los derechos y libertades de los interesados. La finalidad es garantizar que se identifiquen y mitiguen los riesgos potenciales antes de que se materialice el daño, así como establecer medidas de contención si el riesgo se ha materializado, protegiendo así de manera efectiva los datos personales.

En conclusión, cada una de las infracciones que se indican en el acuerdo de inicio representa una infracción diferenciada y autónoma, sin que exista un concurso entre

ellas, incluido el medial. El incumplimiento del artículo 32 del RGPD se enfoca en la falta de adopción de medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo , mientras que la falta de protección de datos desde el diseño del artículo 25.1 del RGPD se centra en la ausencia de integración de salvaguardias y medidas de todo tipo desde la concepción de los sistemas a fin de cumplir con los principios del RGPD y con todos los requisitos del mismo, protegiendo los derechos de los interesados. La falta de una evaluación de impacto en la protección de datos del artículo 35 del RGPD constituye la ausencia de realización de un obligatorio y determinado análisis de riesgos cuando un tratamiento entraña un alto riesgo y refleja la omisión en identificar y mitigar riesgos de manera proactiva, mientras que la vulneración del principio de confidencialidad artículo 5.1.f del RGPD, establecido para garantizar la integridad y confidencialidad de los datos personales, subraya la brecha de datos personales resultante en la exposición no autorizada de datos personales. Estas infracciones protegen bienes jurídicos distintos y provienen de hechos diferentes en determinados aspectos críticos de la gestión de datos personales, constituyendo infracciones diferentes y justificando sanciones independientes.

Por otro lado, conviene hacer referencia a la argumentación de Generali argumenta que las sanciones deberían considerarse bajo el principio de concurso medial según el artículo 29.5 de la LRJSP, que establece que cuando de la comisión de una infracción derive necesariamente la comisión de otra, se deberá imponer únicamente la sanción correspondiente a la infracción más grave. Sin embargo, en el contexto del RGPD, el artículo 83.3 proporciona un marco específico para abordar las infracciones concurrentes, asegurando que todas las violaciones relevantes se imputen y se consideren, pero sin que ello resulte en una penalización excesiva o injusta.

Además, las directrices del Comité Europeo de Protección de Datos (EDPB) sobre el cálculo de las multas también reconocen la posibilidad de infracciones concurrentes y establecen que cada infracción debe ser considerada por separado en su propio contexto, aunque la sanción total se ajuste para evitar duplicaciones injustas.

No obstante, en el presente caso no concurre la aplicación del artículo 83 del RGPD puesto que, como se ha indicado, nos encontramos con incumplimientos basados en conductas perfectamente diferenciadas que motivan de forma autónoma la comisión de distintas infracciones previstas en el RGPD. Cada una de las infracciones imputadas a Generali responde a hechos específicos y fundamentos jurídicos distintos, sin que sea necesario que una de ellas concurra para que se den las demás.

Alegación tercera: Sobre las supuestas infracciones imputadas a Generali

En esta alegación, Generali aborda de manera exhaustiva las infracciones específicas que se indicaban en el acuerdo de inicio. A continuación, se analiza y se rebate los argumentos indicados respecto a cada una de ellas.

Principio de protección de datos desde el diseño (artículo 25.1 del RGPD).

Generali afirma que ha cumplido con el principio de protección de datos desde el diseño al realizar un análisis exhaustivo de los riesgos asociados con el tratamiento de datos y al implementar las medidas necesarias para mitigarlos. Sin embargo, Generali confirmó que la aplicación del Servicio de Mantenimiento de Clientes permitió a los mediadores acceder a datos de exclientes. Este acceso no autorizado a los datos

personales de exclientes demuestra que Generali no implementó adecuadamente las medidas técnicas y organizativas necesarias desde el diseño de sus sistemas para limitar el acceso a los datos únicamente a los fines específicos para los cuales fueron recogidos.

Además, Generali sostiene que este acceso está justificado por la normativa reguladora de la distribución de seguros privados, que exige que los distribuidores puedan acceder a información de clientes cuyas pólizas hayan sido resueltas. Amén de que con este argumento se contradicen con sus propias acciones -pues Generali ha indicado que ha adoptado la medida consistente en ***(…)***-, sin embargo, ese argumento no exime a Generali de su obligación de implementar medidas desde el diseño. La normativa de protección de datos y la normativa sectorial deben coexistir, y Generali tiene la responsabilidad de asegurar que se cumplan ambas, en su caso, implementando medidas que limiten el acceso a datos personales a las personas autorizadas por razón de sus funciones y a lo estrictamente necesario en atención a la finalidad para la que son tratados. La protección de datos desde el diseño exige, entre otras cuestiones, que, antes de que el tratamiento se lleve a término, se evalúen los roles y las responsabilidades de las personas que va a manejar datos personales en el ámbito del responsable del tratamiento para evitar que se produzca un acceso a un número indeterminado de personas físicas.

Generali también argumenta que la aplicación fue puesta en funcionamiento antes de la plena aplicación del RGPD, y que, por lo tanto, no es razonable esperar que en su diseño inicial se hayan tenido en cuenta las obligaciones impuestas por el reglamento. A tal respecto, conviene indicar que la entrada en vigor del RGPD exige que los responsables del tratamiento de datos revisen y actualicen sus sistemas y procesos para cumplir con las nuevas obligaciones legales. La implementación de medidas adecuadas desde el diseño no se limita al momento inicial de creación de un sistema, sino que es un proceso continuo que debe adaptarse a los cambios en la normativa y en los riesgos (cambiantes) en los derechos y libertades de las personas físicas respecto del tratamiento de datos personales. Por el contrario, la falta de actualización adecuada de la aplicación SMC para cumplir con el RGPD manifiesta una falta de diligencia por parte de Generali en este aspecto. Asimismo, conviene señalar que el hecho de que la aplicación fuera puesta en funcionamiento antes de la plena aplicación del RGDP tal y como afirman no exime del cumplimiento de la obligación prevista, una vez la norma desplegó plenos efectos tras plena aplicabilidad en mayo de 2018.

Finalmente, Generali afirma que ha implementado medidas reactivas tras el incidente de seguridad, hecho que en realidad refuerza el argumento de la AEPD de que no se tuvieron en cuenta todas las implicaciones en materia de protección de datos en relación con la protección de datos desde el diseño y por defecto, en concreto, nos referimos a la medida consistente en la falta de segmentación de perfiles que se adoptó tras la brecha de datos personales.

En conclusión, la argumentación de Generali no justifica adecuadamente la falta de medidas de protección de datos desde el diseño y por defecto. Las acciones y omisiones de Generali demuestran que no se tomaron todas las medidas necesarias para asegurar que los datos personales fueran protegidos desde el inicio, y que los

accesos se limitaran estrictamente a las personas adecuadas y a los fines necesarios, como exige el RGPD.

Vulneración del artículo 35 del RGPD en relación con la Evaluación de Impacto en la Protección de Datos:

Generali afirma que no era necesario realizar una EIPD para la aplicación SMC porque, según su análisis de riesgos, el tratamiento no implicaba un alto riesgo para los derechos y libertades de las personas físicas. Sin embargo, como se indicaba en el acuerdo de inicio, existen varios factores que justifican la necesidad de una EIPD, incluyendo el considerable volumen de datos personales tratados y la combinación de datos financieros (en este caso el IBAN) , con los identificativos y de contacto, ya que multiplica el riesgo de suplantación de identidad y daños patrimoniales graves.

El artículo 35 del RGPD requiere una EIPD para tratamientos que, debido a su naturaleza, alcance, contexto o fines, pueden implicar un alto riesgo. La gestión de datos de una gran cantidad de clientes ciertamente entra en esta categoría, ya que el impacto de una posible violación de datos sería considerablemente mayor. Generali no puede descartar la necesidad de una EIPD basándose únicamente en su propio análisis, especialmente cuando trata datos de gran escala y naturaleza sensible.

Asimismo, Generali argumenta que no trata datos de categorías especiales en el SMC, basándose en su propia interpretación de los datos manejados. Sin embargo, el hecho de que Generali gestione seguros de salud implica el tratamiento de datos médicos en algún momento, aunque estos datos específicos no estuvieran directamente involucrados en el SMC. La evaluación de riesgos debe considerar todos los posibles escenarios de tratamiento y los datos que puedan estar siendo tratados. La falta de una EIPD para evaluar estos riesgos demuestra una falta de previsión y diligencia por parte de Generali.

En este sentido, hemos de significar que la jurisprudencia del TJUE ha reconocido el concepto amplio de las categorías especiales de datos personales.

En este sentido, la STJUE de 4 de octubre de 2024, en el asunto C 21/23, y específicamente respecto de los datos de salud, determina que cuando el tratamiento de datos personales puedan revelar indirectamente informaciones sensibles de una persona, dichos datos se encuadran en el régimen previsto en el artículo 9 del RGPD: "*82 En particular, no cabe interpretar tales disposiciones en el sentido de que el tratamiento de datos personales que puedan desvelar indirectamente informaciones sensibles sobre una persona física queda fuera del régimen de protección reforzado establecido por las mencionadas disposiciones, pues de quedar fuera se menoscabaría el efecto útil de ese régimen y la protección de las libertades y de los derechos fundamentales de las personas físicas que pretende garantizar (sentencia de 1 de agosto de 2022, Vyriausioji tarnybinės etikos komisija, C 184/20, EU:C:2022:601, apartado 127)".*

Incluso, indica la citada STJUE que determina que las categorías especiales de datos personales están sometidos a la prohibición del art. 9 del RGPD independientemente de que sea información exacta o no y de que el tratamiento tenga por finalidad obtener datos personales que pertenezcan a dicha categoría: *"87 Esta prohibición de principio es independiente de que la información revelada por el tratamiento en cuestión sea o*

no exacta y de que dicho farmacéutico actúe con el fin de obtener información comprendida en alguna de las categorías especiales contempladas en el artículo 8, apartado 1, de la Directiva 95/46 y el artículo 9, apartado 1, del RGPD. En efecto, teniendo en cuenta los riesgos significativos para las libertades fundamentales y los derechos fundamentales de los interesados, generados por cualquier tratamiento de datos personales comprendidos en tales categorías, estas disposiciones tienen por objeto prohibir dichos tratamientos, con independencia de la finalidad que expresen y de la exactitud de la información en cuestión [véase, en este sentido, la sentencia de 4 de julio de 2023, Meta Platforms y otros. (Condiciones generales del servicio de una red social), C 252/21, EU:C:2023:537, apartados 69 y 70]".

Generali también afirma que el artículo 35.3 del RGPD y la lista de tratamientos que requieren una EIPD no se aplican a su tratamiento específico. Sin embargo, esta interpretación que realiza es restrictiva y no toma en cuenta la naturaleza completa del tratamiento de datos por parte de Generali, y todo ello amén de que la lista es orientativa y no exhaustiva y pretende orientar a los responsables del tratamiento para que identifiquen aquellos tratamientos que requieran una EIPD.

En conclusión, Generali no ha justificado adecuadamente la falta de una EIPD. La gestión de un gran volumen de datos personales y el tratamiento de categorías especiales de datos personales, como en este caso, requieren una evaluación exhaustiva de los riesgos, que debe documentarse mediante una EIPD. La ausencia de esta evaluación refleja una falta de cumplimiento con el artículo 35 del RGPD.

Insuficiencia de medidas de seguridad (artículo 32 del RGPD):

Generali argumenta que la AEPD ha interpretado incorrectamente la naturaleza de las obligaciones impuestas por dicho artículo y que ha basado su decisión en una evaluación errónea de los hechos.

Generali afirma que la obligación de adoptar medidas de seguridad es una obligación de medios, no de resultados, según la jurisprudencia del Tribunal Supremo. Esto significa que la empresa debe demostrar que ha tomado todas las medidas razonablemente necesarias y adecuadas para proteger los datos personales, pero no se la puede responsabilizar automáticamente por una brecha de seguridad si esas medidas resultaron insuficientes para prevenirla.

Conviene señalar de nuevo que la infracción del artículo 32 del RGPD no se debe a la brecha de datos personales en sí misma, sino que la brecha de datos personales simplemente puso manifiesto las deficiencias y carencias en las medidas de seguridad que Generali debería haber implementado previamente. Estas deficiencias no se manifestaron directamente por la brecha, sino tras la verificación y el análisis que tuvo lugar tras el acaecimiento de la misma. Tras la comprobación posterior se puso en evidencia que las medidas de seguridad existentes no eran suficientes para prevenir un acceso no autorizado, lo que demuestra un incumplimiento de la obligación de adoptar medidas de seguridad adecuadas y proporcionadas al riesgo. Y ello independientemente de la producción de la brecha de datos personales.

Se ha de indicar que la medida referida a título de ejemplo por Generali corresponde a una medida propia de la protección de datos desde el diseño.

Generali ha mencionado la implementación de medidas reactivas de seguridad después del incidente como:

- ***(…)***

Las medidas precitadas ponen de manifiesto que las medidas implantadas con anterioridad eran claramente insuficientes para garantizar un nivel de seguridad adecuado al riesgo de forma independiente de la brecha producida.

Así, por ejemplo, no se había previsto ***(…)***.

En conclusión, Generali no ha cumplido con las obligaciones del artículo 32 del RGPD de manera efectiva. El análisis posterior a la brecha, así como las medidas reactivas adoptadas posteriormente evidencian una insuficiencia en las medidas de seguridad preventivas que deberían haber determinado, implementado y aplicado, algo que Generali no ha demostrado haber hecho de manera satisfactoria antes del incidente.

Vulneración del principio de confidencialidad (artículo 5.1.f del RGPD):
Generali argumenta que no se ha producido una infracción, ya que el principio de confidencialidad se habría visto comprometido únicamente debido a la brecha de datos personales, y no por una falta intrínseca de medidas adecuadas.

Sin embargo, esta postura no es sostenible.
Así, por ejemplo, la ***(…)***.

Asimismo, si bien tenían antes de la brecha de datos personales medidas para el ***(…).*** Esta medida de seguridad no sirve para detectar otro tipo de ataques habituales. Era una medida de seguridad claramente insuficiente.

En este sentido se ha de significar que es muy habitual en la actualidad que los ataques de denegación de servicio sean distribuidos, es decir, que se lancen desde muchas direcciones IP diferentes, por lo que se tendrían que haber previsto medidas comúnmente utilizadas para prevenir, detectar y reaccionar ante este otro tipo de ataques. Este tipo de medidas no estaban implementadas, resultando que la brecha de datos personales se produjo porque no fue detectado un ataque distribuido.

Generali también afirma que el ataque ***(…)*** fue un factor fuera de su control. Sin embargo, la seguridad de los sistemas de información debe contemplar la posibilidad de ataques externos con fuerza bruta, como el que aconteció – ***(…)***-; de ahí las medidas preventivas como la autenticación multifactor, que debería haberse implementado antes del incidente; no se alcanza a comprender ***(…)***, resultando que era una medida de seguridad que no estaba debidamente implementada y que ha sido establecida con posterioridad a la brecha de datos personales. Así, tal y como ha aquedado acreditado:

- ***(…).***

La brecha de datos personales permitió el acceso no autorizado a un número considerable de datos personales, incluyendo datos identificativos, información de contacto, información financiera y direcciones residenciales, suponiendo una pérdida de confidencialidad.

Generali también sostiene que la necesidad de comunicar los hechos a un número tan elevado de personas afectadas refleja la gravedad del incidente. Este argumento, lejos de exonerar a Generali, manifiesta el impacto que puede tener la brecha de datos personales en su relación con el principio de confidencialidad. La gran escala de la notificación es una indicación clara de la magnitud de la vulneración del principio de confidencialidad en cuanto a que la brecha de datos personales entraña un alto riesgo para los derechos y libertades de las personas físicas.

En resumen, la vulneración del principio de confidencialidad ha quedado perfectamente constatada mediante la exposición de datos personales a terceros no autorizados. La exposición de datos personales en la magnitud observada es un claro indicativo de que no se cumplió con la obligación de garantizar la confidencialidad de los datos personales, tal como exige el artículo 5.1.f del RGPD.

Alegación cuarta: sobre la vulneración del principio de proporcionalidad

La cuarta alegación de Generali sobre la vulneración del principio de proporcionalidad carece de fundamento cuando se analizan los hechos y las disposiciones legales aplicables. La AEPD ha evaluado cuidadosamente las circunstancias concurrentes y ha aplicado el principio de proporcionalidad al determinar las sanciones, de acuerdo con el artículo 83 del RGPD. Generali sostiene que la AEPD no consideró ciertas atenuantes y aplicó agravantes sin justificación, lo cual es refutable en los términos que seguidamente se exponen.

Así, Generali argumenta que las medidas reactivas adoptadas tras el incidente deberían ser consideradas atenuantes. Sin embargo, el hecho de que se hayan tomado medidas reactivas no exime a la empresa de la responsabilidad inicial por no haber implementado medidas de seguridad apropiadas al nivel de riesgo, debiendo desplegarse la diligencia apropiada cuando se trata de una empresa que gestiona un gran volumen de datos personales, incluyendo categorías especiales de datos personales. Las acciones correctivas, aunque necesarias, no compensan la falta de medidas proactivas adecuadas para proteger los datos personales en empresas de dicha naturaleza, cuyas posibles consecuencias pueden agravarse y amplificarse teniendo en cuenta el tratamiento a gran escala que realizan.

Generali también alega que no ha sido objeto de sanciones anteriores y que esto debería considerarse un atenuante. Sin embargo, la gravedad de la infracción actual y el impacto potencial sobre un gran número de personas, en este caso justifican una sanción adecuada con independencia del historial sancionador previo de la entidad. En este sentido la Audiencia Nacional en su sentencia 1437/2020 de 5 de mayo de 2021 afirmado que *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"*;

Por lo que respecta a la afirmación de Generali de que la AEPD tuvo conocimiento del incidente a través de la notificación voluntaria de la empresa, debe de recordarse que dicha comunicación se trata de una obligación prevista por el propio RGPD y no un acto voluntario que merezca consideración como atenuante.

En cuanto a la adhesión a códigos de conducta, Generali menciona su participación en la elaboración de guías de buenas prácticas. Aunque estos esfuerzos son positivos, no eximen a la entidad de la responsabilidad de cumplir con todas las disposiciones del RGPD de manera efectiva y continua.

La AEPD ha aplicado correctamente las circunstancias agravantes. La gran escala del tratamiento de datos, la naturaleza de los datos tratados y la especial negligencia en la adopción de medidas adecuadas de protección justifican la aplicación de agravantes. Estas agravantes no se basan en apreciaciones subjetivas sin fundamento, sino en una evaluación detallada de los hechos, los riesgos y el impacto de la infracción que se exponen en la presente resolución.

En conclusión, la AEPD ha seguido una metodología adecuada y justificada para evaluar tanto las circunstancias atenuantes como las agravantes en este caso, motivándolo, y ha aplicado el principio de proporcionalidad conforme a la normativa vigente. Las sanciones propuestas reflejan la gravedad de las infracciones.

IV Obligación incumplida del artículo 5.1 f)

De acuerdo con el apartado 1.f) del artículo 5 RGPD los datos deben ser:

"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»)"

De la misma forma, el Considerado 39 RGPD dispone 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."*

El citado principio de confidencialidad tiene como fin garantizar que los datos personales sean accesibles únicamente para aquellas personas autorizadas a utilizarlos y para los fines específicos para los cuales se han recogido. En dichos términos, cualquier exposición o tratamiento no autorizado de datos personales constituiría una violación del citado principio. Ello ocurre cuando los datos personales son accesibles a individuos o entidades no autorizados, o cuando son utilizados para fines distintos a los que fueron originalmente recogidos o consentidos por su titular.

En el presente caso, de las actuaciones de investigación realizadas por esta autoridad se desprende una vulneración del principio de confidencialidad al no garantizar una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito, mediante la aplicación de medidas técnicas y

organizativas apropiadas, que se ha visto materializada con la exposición no autorizada de datos personales de un número considerablemente alto de personas. Dentro de los datos expuestos, se encontraban datos de identificación personal, datos de contacto, información financiera y direcciones residenciales.

El número de afectados y potencialmente afectados resulta de las comunicaciones formales del incidente realizada por la propia parte reclamada a dichos afectados y que fueron asimismo aportadas durante las citadas actuaciones. Así, afirma haber comunicado el incidente a 24.352 personas directamente afectadas que estaban incluidas en el fichero de muestra obtenido de los atacantes a través de la empresa de ciberseguridad *Lazarus*. A ello se suma la comunicación a 1.092.543 extomadores de pólizas no incluidos en el fichero de muestra y 399.153 exasegurados de pólizas individuales, cuyos datos de contacto no estaban disponibles. Por último, se incluye una comunicación pública para 166.621 exasegurados de pólizas colectivas, lo que eleva el número total de personas potencialmente afectadas a más de 1.6 millones.

La necesidad de comunicar los hechos a un número tan elevado de personas (más de un millón y medio), además de reflejar la relevancia de la brecha de datos personales, también manifiesta el reconocimiento de su gravedad por la parte reclamada. La detección del ataque y la posterior investigación que reveló la producción del acceso no autorizado a datos personales confirma dicha afirmación.

Resalta asimismo el número de datos personales comprometidos por cada afectado. El hecho de que se hayan expuesto datos detallados como el DNI, datos de contacto, y direcciones personales, entre otros, manifiesta la magnitud del incumplimiento. Debe de tenerse en cuenta que, en un número considerable de casos, se expusieron datos financieros como el IBAN, lo que, junto a la combinación de datos identificativos y de lo calización, expone a las personas afectadas a un riesgo significativo de fraude, como el robo de identidad y el fraude financiero, actuaciones delictivas que, desafortunadamente, son frecuentes en la actualidad.

No puede obviarse tampoco la circunstancia de alguien afirmó poseer determinados datos de exclientes (800.000, según comunica la parte reclamada,) en un foro de *Telegram*, y que la empresa de ciberseguridad *Lazarus* facilitara una muestra a la parte reclamada. Siendo *Telegram* una plataforma de mensajería accesible al público, plantea un escenario preocupante, pues la puesta a disposición de esta información en un entorno abierto y fácilmente accesible aumenta el riesgo de que dichos datos sean utilizados de manera indebida.

Por último, de las actuaciones de investigación se desprende que la vulneración del principio de confidencialidad, en el presente caso, no se limita únicamente al ciberataque producido. De igual forma, la circunstancia de que los mediadores de seguros, tanto agentes como corredores, en el momento del incidente pudieran visualizar y acceder a los datos de exclientes, a pesar de haber finalización su relación comercial con la parte reclamada supone una nueva manifestación de la vulneración de este.

Asimismo, nos remitimos respecto del incumplimiento de esta obligación a lo que se ha contestado en la alegación tercera en relación con la falta de medidas técnicas y organizativas en relación con la brecha de datos personales.

Por lo expuesto, se desprende una vulneración del artículo de 5.1.f) del RGPD al no garantizar una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito, mediante la aplicación de medidas técnicas y organizativas apropiadas.

V Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone:

"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; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"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, el artículo 72 "Infracciones consideradas muy graves" de la LOPDGDD indica:

"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. (…)"

VI Sanción por incumplimiento del artículo 5.1 f)

Según el artículo 83.2 del RGPD "*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".

De la misma forma, el artículo 76 de la LOPDGDD establece una serie de criterios para graduar la posible sanción, siguiendo lo dispuesto en el apartado k) del anterior artículo:

"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."

Teniendo en cuenta dichos preceptos, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

Agravante prevista en el apartado a) del artículo 83.2 del RGPD:

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;

En el presente caso la gravedad de la infracción se desprende de varios aspectos: el número considerable de interesados afectados y de datos personales de los mismos, así como el hecho de que varios de dichos de datos personales se encontrarán a la venta en una red de mensajería electrónica. Dichas circunstancias, reunidas de forma conjunta, aumenta el potencial riesgo de daños para los individuos afectados, ya que los datos de los que son titulares pueden caer en manos de actores malintencionados con la intención de cometer fraudes, extorsiones u otras actividades delictivas.

Agravante prevista en el apartado b) del artículo 83.2 del RGPD:

b) la intencionalidad o negligencia en la infracción;

En este caso cabe apreciar una negligencia grave por la parte reclamada. En este sentido, 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. 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, dado que la actividad de la recurrente es de constante y abundante gestión de datos de carácter personal es exigible un mayor rigor y exquisito cuidado con el fin de ajustarse a las previsiones (Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (rec. 63/2006).

Agravante prevista en el apartado b) del artículo 76 LOPDGDD*: La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*

La concurrencia de la citada agravante deriva de la naturaleza de la actividad de la parte reclamada. Resulta evidente que, como aseguradora, realiza de forma periódica operaciones que implican la gestión y tratamiento de grandes volúmenes de datos personales. Esta especial vinculación con los datos personales que gestiona implica una mayor responsabilidad en evitar que dichos datos sean expuestos o indebidamente tratados por personas autorizadas. Por el contrario, la vulneración del principio de confidencialidad por entidades cuya actividad presenta dicha vinculación agrava la conducta infractora, lo que, en consecuencia, motiva la concurrencia de la presente agravante.

No se aprecia la concurrencia de circunstancias atenuantes.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el citado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto, en el acuerdo de inicio se proponía como sanción una multa de cuantía de **1.000.000 € (UN MILLON DE EUROS).**

VII Obligación incumplida del artículo 32

El artículo 32 “Seguridad del tratamiento” del RGPD establece*:*

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

Resulta necesario señalar que el citado precepto no establece un listado de medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve dicho tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, determinando aquellas medidas técnicas y organizativas adecuadas teniendo en cuenta la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad adecuado al riesgo se debe tener particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o

acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

Por su parte, el considerando 83 del RGPD señala *que "(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".*

En el presente supuesto, las investigaciones llevadas a cabo por la presente autoridad de control han revelado que, con independencia de la brecha producida, si bien la parte reclamada había implementado ciertas medidas de seguridad de datos, las mismas no eran suficientes para cumplir con las exigencias previstas en el citado artículo 32. Como se ha indicado, dicho precepto establece la necesidad de implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo. La inadecuación o insuficiencia en este caso se desprende de varias manifestaciones realizadas por la propia parte reclamada en el curso de las citadas actuaciones de investigación.

De la misma forma, dicha entidad ha confirmado carencias en las medidas técnicas desplegadas ***(…).*** Esta deficiencia impide que la parte reclamada pueda realizar un análisis de la actividad que se está desarrollando en la citada aplicación. Ello supone una mayor dificultad en identificar patrones de uso anómalos, acceso no autorizado, o cualquier otra forma de abuso o mal uso de los datos personales, incluyendo el que pueda realizar su propio personal.

Por otro lado, conviene hacer referencia a las numerosas medidas reactivas adoptadas por la parte reclamada tras el incidente y que fueron puestas en conocimiento de la presente autoridad durante las actuaciones de investigación. La adopción de tales medidas reactivas pone de manifiesto la ausencia de ciertas medidas de seguridad básicas teniendo en cuenta el riesgo derivado de su actividad. ***(…).***

Así, por ejemplo, ***(…)***, medida de seguridad insuficiente e independiente de la brecha de datos personales.

Si bien las medidas reactivas son esenciales para resolver las vulnerabilidades y prevenir futuras brechas, la necesidad de su adopción resalta una inadecuación o insuficiencia de las medidas adoptadas, lo que implícitamente implica un reconocimiento por la parte reclamada de la existencia de deficiencias en su enfoque de seguridad de datos.

Por último, no puede esconderse el considerable número de usuarios que gestiona la parte reclamada al ejercer su actividad, circunstancia que conlleva intrínsicamente un riesgo elevado en términos de protección de datos personales y, en consecuencia, la implementación de medidas de seguridad apropiadas al nivel de riesgo. Debe de tenerse en cuenta que, en ese contexto, los riesgos asociados al tratamiento se amplifican debido a la cantidad de datos gestionados y a la potencial gravedad de cualquier brecha. Ello implica que cualquier fallo en las medidas de seguridad no solo afectaría a un mayor número de individuos, sino que también podría tener consecuencias más graves, tanto en términos de impacto para los posibles afectados como de responsabilidad para la parte reclamada.

Asimismo, nos remitimos respecto del incumplimiento de esta obligación a lo que se ha contestado en la alegación tercera en relación con la falta de medidas técnicas y organizativas de seguridad apropiadas al nivel de riesgo.

Por lo expuesto, de las mencionadas actuaciones de investigación y afirmaciones de la propia entidad, con independencia del incidente producido y de las consecuencias del mismo, se desprende una falta de adecuación al riesgo de las medidas de seguridad adoptadas por la parte reclamada, teniendo en cuenta la cantidad de datos que gestionaba esta última.

VIII Tipificación y calificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone: “*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 este respecto, la LOPDGDD, en su artículo 71 “Infracciones” establece que *“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, el artículo 73 “Infracciones consideradas graves” de la LOPDGDD indica: “*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.

IX Sanción por la infracción del artículo 32 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 32 se sancionará, *"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;"

Teniendo en cuenta el ya mencionado artículo 82.2 del RGPD en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

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;

En el presente caso la gravedad de la infracción se desprende del potencial riesgo que existe en la protección de datos personales con la falta de adopción de medidas seguridad básicas por la parte reclamada, teniendo en cuenta el considerable volumen de datos que gestiona y la naturaleza de los mismos. Dichas circunstancias hacen que los efectos de cualquier brecha de datos personales que pueda acontecer se amplifiquen con perjuicios considerables a los posibles afectados resultantes de la misma.

b) la intencionalidad o negligencia en la infracción;

Teniendo en cuenta la doctrina anteriormente indicada, esta agravante deriva de una falta de debida diligencia en la adopción de las medidas de seguridad adecuadas al riesgo por la parte reclamada. Debe tenerse en cuenta que en el presente caso, teniendo en cuenta la naturaleza y volumen de datos gestionados por la parte reclamada, se exige un especial deber legal de cuidado que, en el presente caso, no ha concurrido, lo que conlleva una negligencia grave en su actuación. (Sentencia de la Audiencia Nacional de 17 de octubre de 200, número de recurso 63/2006).

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto, en el acuerdo de inicio se proponía como posible sanción una multa de cuantía de **1.000.000 € (UN MILLÓN DE EUROS)**

X Obligación incumplida del artículo 25 del RGPD

Por su parte el artículo 25 del RGPD, en relación a la Protección de datos desde el diseño y por defecto, establece lo siguiente:

"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."

Como puede observarse, el artículo 25 RGPD contempla la protección de datos, no como un añadido posterior, sino como un elemento integral y prioritario en el diseño de sistemas, procesos y productos. Ello implica que las medidas de seguridad deben ser consideradas desde las primeras etapas de desarrollo de cualquier sistema o proceso que trate cualquier tipo de dato de carácter personal, lo que conlleva a situar la protección de datos en un aspecto central del diseño de dichos sistemas y procesos.

El principio de protección de datos desde el diseño refleja un cambio fundamental de una postura reactiva a una proactiva, lo cual es una manifestación del enfoque basado en el riesgo que promueve el RGPD, enfatizando la anticipación y prevención en la gestión de los datos personales. Bajo este enfoque, la responsabilidad de proteger los datos personales se inicia desde las etapas más tempranas de planificación de cualquier actividad de tratamiento de datos. Ello significa que el responsable del tratamiento debe incorporar las medidas que garanticen su protección en el mismo momento en que se está diseñando y planificando el tratamiento de datos personales. Dicho enfoque proactivo implica identificar y abordar los riesgos potenciales desde el inicio, integrando las garantías necesarias directamente en los procesos y sistemas de tratamiento de datos.

En este sentido, al aplicar la protección desde el diseño, se deben considerar todos los elementos que conforman el tratamiento de datos, incluyendo la naturaleza de los mismos, los fines del tratamiento, así como las posibles consecuencias para los derechos y libertades de los individuos afectados. El objetivo es garantizar que los principios de protección de datos, como el de minimización, la limitación de la finalidad y la seguridad de los datos, se implementen de manera efectiva y coherente a lo largo de todo el ciclo de vida del tratamiento de datos.

Así se expresa en las Directrices 4/2019 del CEPD relativas al artículo 25 Protección de datos desde el diseño y por defecto, adoptadas el 20 de octubre de 2020. En las citadas Directrices se indica al respecto que:

"El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del software y hardware y los servicios de tratamiento de datos.

Tomar en consideración la PDDD desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas".

Para ello debe recurrir al diseñar el tratamiento a los principios recogidos en el artículo 5 del RGPD, que servirán para aquilatar el efectivo cumplimiento del RGPD. Así, las citadas Directrices 4/2019 del CEPD disponen que

"61. Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y

responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD".

La Guía de Privacidad desde el Diseño de la AEPD afirma que *"La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada".*

La Guía dispone que "*La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña (…) La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida de los datos".*

Por lo que respecta al caso que nos ocupa, en el transcurso de las actuaciones de investigación realizadas, se ha puesto de manifiesto que no se tuvo en cuenta que los datos de los exclientes deben mantenerse para fines distintos a las existentes durante el tiempo que se encuentra vigente la poliza. Como manifiesta la propia parte reclamada el nuevo fin se limita al cumplimiento de obligaciones normativas tributarias y aseguradoras, entre otras. Según sus manifestaciones no se había tenido en cuenta dichas circunstancias debido a que no tenía los datos separados físicamente, en equipos diferenciados, ni tampoco tenía una separación lógica entre ellos pues figuraban ambos tipos de clientes la misma base de datos, en incluso, la misma tabla (PERSONAS). Ello provocaba, con independencia de la brecha sufrida, que tanto los agentes de seguros como los corredores de seguros, tuvieran acceso a los datos personales de exclientes, a pesar de que estos ya no poseían póliza en vigor. Es decir, se permitía el acceso de datos personales a determinadas personas que ya no estaban autorizadas, pues los titulares de dichos datos ya no tenían la consideración de clientes y, en consecuencia, la finalidad de dicho tratamiento ya había finalizado, limitándose a partir de dicho momento al cumplimiento de determinada normativa exigible.

Dicho hecho, consistente en la posibilidad de acceder a datos de exclientes por personas que ya no se encontraban autorizadas, manifiesta que no se tuvieron en cuenta todas posibles implicaciones en materia de protección de datos en el momento de la creación de la aplicación que tenía como fin el acceso y gestión de los datos de dichos datos. En este sentido, conviene señalar que, a diferencia de lo que ocurría con el incidente producido ***(…)***, en el presente caso la anomalía no se debió a una causa sobrevenida, sino existió desde el inicio, esto es, desde el momento del diseño e implementación de la aplicación. Ello no se desvirtúa por el hecho de que, como consecuencia del incidente, se tuviera conocimiento de dicha circunstancia y se procediera a adoptar por la parte reclamada medidas reactivas con el fin de solventar el problema.

De lo expuesto se desprende que, en el momento del diseño de la aplicación o sistema en cuestión, no se tuvieron en cuenta adecuadamente los principios establecidos en el artículo 5; en particular, el principio de minimización y el principio de limitación de los datos personales.

Así, por lo que se refiere al principio de minimización de los datos personales, tal y como indica el mencionado artículo 5 del RGPD, su cumplimiento exige que dichos datos sean *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)*. Desde la perspectiva de la protección de datos por defecto y desde el diseño supone que, desde las primeras etapas debe considerarse qué datos son realmente necesarios para cumplir con el objetivo previsto y limitar la recopilación y el procesamiento a dichos datos. De igual forma, implementar este principio de forma efectiva requiere una gestión cuidadosa del ciclo de vida de los datos personales, asegurando que se traten solo por el período que sea estrictamente necesario para los fines para los cuales fueron recogidos.

El hecho de que en el momento de creación e implementación del sistema no se tuviera en cuenta la circunstancia de que, ***(…),*** manifiesta que el sistema no fue diseñado teniendo en cuenta el principio de minimización. La consecuencia es que se produce un tratamiento por un tiempo superior al que resultaba necesario para el cumplimiento del fin para el que estaba autorizado en un inicio.

De la misma forma, por lo que se refiere al principio de limitación de datos personales, el apartado b) del citado artículo 5 del RGPD exige "*datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines, …"*. Este principio conlleva que, al diseñar un sistema o proceso, la finalidad de la recogida de datos esté claramente definida y limitada. Ello significa que, desde la fase de conceptualización, se deben establecer claramente los fines para los cuales se recogen los datos. Estos fines deben ser específicos y explícitos, y el sistema debe ser diseñado para soportar solo el tratamiento de datos necesario para lograr esos fines.

De igual forma, los sistemas deben ser diseñados para controlar y restringir el acceso a los datos en función de la finalidad del tratamiento, lo que supone que solo las personas autorizadas para un fin específico puedan tener acceso a los datos relacionados con ese fin. Para ello, los sistemas deben ser capaces de segregar y gestionar datos de acuerdo con sus diferentes fines.

En el caso que nos ocupa, si al diseñar la aplicación no se incorporaron mecanismos ***(…),*** no se está teniendo en cuenta el principio de limitación de datos personales. El sistema debería haber tenido en cuenta los distintos fines existentes a lo largo del ciclo del tratamiento (para la ejecución del contrato, para el cumplimiento de la normativa) y quienes son los autorizados a acceder a dichos datos según se encuentre en la fase correspondiente (mediadores, personal, autoridades…). En caso contrario, se vulnera el principio de limitación de datos personales, pues permite el acceso de datos a personas que ya no se encuentran legitimadas.

Por otro lado, la falta de enfoque de protección de datos desde el inicio y por defecto, también se desprende de la medida reactiva realizada por la propia parte reclamada tras el incidente para resolver el problema y que consistió en ***(…).*** Dicha medida

resultó necesaria, pero su implementación tardía indica una falta de protección de datos por defecto desde el inicio y por defecto. La protección de datos por defecto requiere que las medidas se apliquen automáticamente, sin requerir acciones adicionales del responsable del tratamiento ni del usuario.

Por último, conviene asimismo destacar la naturaleza de la actividad de la parte reclamada, que como entidad aseguradora gestiona un gran volumen de datos personales, recopilando y procesando una cantidad significativa de ellos, incluyendo información sensible relacionada con la salud, finanzas, y otros personales de sus clientes, incluidos menores. El alto volumen de datos, así como su naturaleza, aumenta tanto la complejidad como el riesgo potencial asociado con su tratamiento, lo cual exige una mayor rigurosidad en la necesidad de adoptar un enfoque de protección de datos desde el diseño y por defecto. Debe de tenerse en cuenta que, en tratamientos de datos masivos como ocurre en el presente caso, cualquier fallo en las medidas de protección puede tener implicaciones significativas para un gran número de individuos, por lo que resulta crucial que las entidades que los gestionen implementen sistemas y procesos que incorporen medidas de seguridad desde el inicio.

Por lo expuesto, ***(…),*** a pesar de haberse solventado posteriormente, manifiesta el incumplimiento del artículo 25 del RGPD al no haberse adoptados medidas adecuadas que cumplan los principios de protección de datos desde el diseño y por defecto.

XI Tipificación de la infracción del artículo 25 RGPD

La vulneración del artículo 25 del RGPD se encuentra tipificada en el artículo 83.4 del mismo texto legal, según el cual:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;”

Por lo que se refiere al plazo de prescripción, la infracción señalada en el párrafo anterior se considera como grave y prescribe a los dos años, conforme al artículo 73 d) de la LOPDGDD, que establece que:

“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:
d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.”

XII Sanción por la infracción del artículo 25 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 32 se sancionará, *"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.*

Asimismo, teniendo en cuenta el artículo 82.2 del RGPD y el artículo 76 de la LOPDGDD, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

- Artículo 82.2 b) del RGPD: *"la intencionalidad o negligencia en la infracción;*

De acuerdo con la doctrina jurisprudencialmente anteriormente indicada, esta agravante resulta aplicable asimismo en la presente infracción, pues, de las actuaciones de investigación, se desprende la falta de una debida diligencia por la parte reclamada en el momento del diseño de la aplicación que tenía como fin la gestión por los mediadores de los datos de sus clientes. El hecho de no haber tenido en cuenta los distintos fines del tratamiento y que, como consecuencia, los mediadores pudieran seguir accediendo a datos de sus exclientes manifiesta una negligencia grave en la implementación de la misma, en los términos indicados por la ya citada sentencia de la Audiencia Nacional de 17 de octubre de 2007, número de recurso. 63/2006).

- Artículo 76 b) de la LOPDGDD: *"b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.;*

La concurrencia de la citada agravante es consecuencia de la naturaleza de la actividad de la entidad infractora, la cual como aseguradora, realiza actividades que implican la gestión y tratamiento de grandes volúmenes de datos personales como parte fundamental de su operación. Esta especial vinculación con los datos personales que gestiona implica una mayor responsabilidad de garantizar su protección desde el diseño y, consecuentemente, existe una mayor expectativa de cumplimiento de las normas de dicho ámbito. Por el contrario, el incumplimiento de dichas exigencias supone una amplificación de los posibles riesgos, lo cual justifica la concurrencia de la mencionada agravante.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto en el acuerdo se proponía como sanción una multa de cuantía de **2.000.000 € (DOS MILLONES DE EUROS)**

XIII Sanción por la infracción del artículo 35 del RGPD

El artículo 35, en relación a la Evaluación de impacto relativa a la protección de datos, establece lo siguiente:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para

los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.
4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1.
La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden
relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en

cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

La necesidad de implantar una evaluación de impacto en la protección de datos (EIPD) es consecuencia del principio de responsabilidad proactiva prevista en el propio RGPD, y es una herramienta fundamental para garantizar que entidades que presenten determinadas características en su tratamiento gestionen y traten datos personales de manera responsable, segura y conforme a la normativa en dicha materia, protegiendo de esta forma los derechos de sus titulares y fortaleciendo la confianza en sus operaciones.

La finalidad de la EIPD, como se establece en el citado artículo 35 del RGPD es múltiple y se centra en asegurar la protección de los datos personales de las personas físicas. Entre dichas finalidades podemos destacar:

- Identificar y evaluar los riesgos potenciales para los derechos y libertades de las personas que podrían surgir como resultado del tratamiento de datos personales. Ello es especialmente importante cuando se utilizan nuevas tecnologías o se realizan tratamientos de datos masivos.

- Ayudar a las organizaciones a cumplir con el RGPD, pues permite asegurar que se respetan los requisitos normativos relacionados con la protección de datos desde el diseño y por defecto.

- Implementar medidas de mitigación de los riesgos. Basándose en los riesgos identificados, la EIPD guía a las entidades en la implementación de las

medidas adecuadas para mitigar esos riesgos. Esto puede incluir ajustes en la forma en que se recopilan, almacenan, procesan o comparten los datos personales.

- Prevenir posibles daños y/o violaciones de datos, pues mediante la identificación proactiva y la mitigación de riesgos, la EIPD ayuda a prevenir violaciones de datos y otros daños que podrían resultar del tratamiento inadecuado de los datos personales, lo que puede conllevar consecuencias legales.

En el presente caso, respecto a esta exigencia y tal y como manifestó la propia parte reclamada durante el transcurso de las actuaciones de investigación, se desprende únicamente la existencia un documento donde se realizaba un análisis o descripción general del tratamiento con el propósito de determinar la necesidad de llevar a cabo una evaluación de impacto (EIPD), concluyendo que el tratamiento tiene un nivel de impacto bajo y, que, por tanto, no resultaba necesaria llevar a cabo esta EIPD. Sin embargo, teniendo en cuenta las características de la naturaleza y de las funciones de la parte reclamada, dicho diagnostico devino desacertado y ello en base a las razones que seguidamente se exponen.

En primer lugar, debe destacarse el considerable volumen de clientes que gestiona la parte reclamada, lo cual conlleva, en consecuencia, un tratamiento de los datos personales de dichos titulares a gran escala. En este sentido, cuanto mayor es el volumen de datos que se tratan, mayor es el riesgo potencial de brechas de seguridad y violaciones de datos. Ello se debe, entre otras causas, a la atractiva cantidad de información que supone para los ciberdelincuentes, así como también en el aumento de la complejidad de tratar datos a gran escala de manera segura. De la misma forma, a medida que aumenta el volumen de datos, resulta más complejo garantizar los derechos de los sujetos de datos, como el acceso a sus datos, rectificación, supresión o portabilidad.

En base a dichas circunstancias se deriva la necesidad de una previa elaboración de una EIPD como instrumento fundamental para mitigar los riesgos asociados con el tratamiento a gran escala de datos personales, como ocurre en entidades aseguradoras de ámbito de actuación nacional y/o internacional. En volumen masivos de tratamientos de datos, dicha evaluación permite identificar proactivamente y abordar riesgos antes de que ocurran, desarrollando posibles medidas de mitigación, lo cual es esencial para proteger los derechos y libertades de los individuos en el contexto de tratamientos de datos a gran escala.

En segundo lugar, cabe hacer referencia igualmente al número de datos personales que, en entidades de esta naturaleza, se recopilan de cada cliente. Cuando hablamos de la cantidad de datos personales tratados por una aseguradora por cada cliente o persona, nos referimos a un conjunto potencialmente extenso y detallado de información. En este sentido, las aseguradoras, debido a la naturaleza de sus servicios, recopilan y procesan una amplia variedad de datos personales, que pueden incluir: datos identificativos, información de contacto, datos financieros y bancarios, empleo y educación, de comportamiento y preferencias, de reclamaciones anteriores,

datos derivados y analíticos, entre otras, incluidos los datos de categorías especiales a los que después se hará referencia.

Debe tenerse en cuenta que una gran cantidad de datos detallados sobre individuos aumenta el riesgo de que estos datos sean utilizados de manera indebida, ya sea internamente por la organización o por terceros que puedan acceder a ellos sin autorización. Las grandes bases de datos de información personal, como las que gestionan las aseguradoras, son sumamente atractivas para los ciberdelincuentes, dado que incluyen detalles financieros y de identidad personal, que pueden ser explotados para fraude, robo de identidad, o venta en el mercado negro. Por ello, la vasta cantidad de datos personales tratadas por cliente hace que las EIPD sean esenciales, no solo para cumplir con la exigencia formal, sino también para garantizar la protección efectiva de los derechos y libertades de las personas.

Por último, cabe hacer referencia al tratamiento de categorías especiales de datos personales que se contemplan en el artículo 9 del RGPD. Estas categorías especiales comprenden aquellas que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

La característica principal del tratamiento de este tipo de categorías especiales de datos es la previsión de una mayor protección respecto al resto de los datos, permitiendo únicamente su tratamiento cuando concurra alguna de las circunstancias previstas por el mencionado artículo 9 del RGPD. Teniendo en cuenta esta protección adicional, la realización de una EIPD resulta aún más justificada. De hecho, el apartado tercero del propio artículo 35 del RGPD contempla dentro de los supuestos en los que se prevé que se requiera una EIPD se encuentra aquel "*tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1"*.

En el caso de las entidades aseguradoras, como ocurre con la parte reclamada del presente supuesto, el tratamiento de estas categorías especiales de datos personales afecta principalmente a datos de la salud, dado que este tipo de datos suelen ser recopilados para la adquisición de determinados productos. Este tipo de datos son recogidos, por supuesto, para la concertación de los propios seguros de salud que ofrezca la propia entidad aseguradora. Pero dicha información también es recogida en diversas ocasiones para otro tipo de seguros, con el fin de determinar las primas de manera justa y precisa, basándose en el nivel de riesgo que ha sido valorado tras la obtención de dicha información.

Con independencia de que se encuentre expresamente prevista en el artículo 35, el tratamiento de datos de salud por parte de aseguradoras presenta riesgos significativos que justifican plenamente la realización de una EIPD, pues resulta fundamental para garantizar que se identifican y mitigan adecuadamente los riesgos específicos asociados con estos datos. Dada su naturaleza sensible, el tratamiento de datos de salud lleva consigo riesgos elevados para los derechos y libertades fundamentales de los individuos. Ello incluye el riesgo de discriminación, estigmatización y daño a la reputación personal.

En definitiva, en el caso que nos ocupa y ~~sin perjuicio de lo que resulte de la instrucción del presente procedimiento~~, teniendo en cuenta el volumen de datos tratados, incluidos aquellos con categorías especiales, los cambios tecnológicos que se han producido durante los últimos años, así como los riesgos de que terceros puedan apropiarse de dichos datos de manera ilícita, lleva a la conclusión de que la parte reclamada debió de haber realizado una EIPD. Dicho instrumento persigue conocer mejor los riesgos existentes y los impactos que pueden producirse en los tratamientos e intentar asegurar la confidencialidad, integridad y disponibilidad de los datos personales, minimizando así el riesgo de violaciones de datos y garantizando la protección de los derechos y libertades de los individuos. La no realización de dicha EIPD conlleva, por el contrario, un incumplimiento del citado artículo 35 de RGPD.

XIV Tipificación y calificación de la infracción del artículo 35 del RGPD

De confirmarse, la citada infracción del artículo 35 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone: "*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 este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"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, el artículo 73 "Infracciones consideradas graves" de la LOPDGDD indica: "*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:*

(…) t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible".

XV Posible sanción por la infracción del artículo 35 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 35 se sancionará, *"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*

Asimismo, teniendo en cuenta el artículo 82.2 del RGPD y el artículo 76 de la LOPDGDD, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

- Artículo 82.2 b) del RGPD: *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;*

En el presente caso la gravedad de la infracción se desprende tanto del volumen de datos personales como la naturaleza de los mismos, dado que entre los mismo se encuentran categorías especiales. Tales circunstancias agravan la conducta infractora de no haber realizado la EIPD a pesar de venir obligado a ello, puesto que el incumplimiento de dicha obligación aumenta el riesgo de que los titulares de dichos datos puedan sufrir en sus derechos y libertades.

- Artículo 82.2 b) del RGPD: *"la intencionalidad o negligencia en la infracción;*

De acuerdo con la doctrina jurisprudencialmente anteriormente indicada, esta agravante resulta aplicable asimismo en la presente infracción, pues, de las actuaciones de investigación, se desprende la falta de una debida diligencia al no haber realizado la EIDP a pesar de que la naturaleza de la actividad y de los datos personales tratados se desprendía su necesidad; todo ello en los términos indicados por la ya citada sentencia de la Audiencia Nacional de 17 de octubre de 2007, número de recurso: 63/2006).

- Artículo 76 b) de la LOPDGDD: *"b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.;*

La concurrencia de la citada agravante es consecuencia también de la naturaleza de la actividad de la entidad infractora, la cual como aseguradora, realiza actividades que implican la gestión y tratamiento de grandes volúmenes de datos personales como parte fundamental de su operación Esta especial vinculación con los datos personales que gestiona implica una mayor responsabilidad de garantizar su protección y, en consecuencia, la no realización de la EIPD teniendo en cuenta estas circunstancias agrava la conducta, justificando la concurrencia de la citada agravante.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto, en el acuerdo de inicio se proponía como sanción una multa de cuantía de **1.000.000 € (UN MILLÓN DE EUROS)**

XVI Adopción de medidas

De acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, 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.

En el presente caso, se requiere al responsable para que en el plazo de tres meses a partir de la notificación de la presente resolución notifique a esta Agencia la adopción de las siguientes medidas:

- La realización y superación de la evaluación de impacto de las operaciones de tratamiento en la protección de datos personales prevista en el artículo 35 del RGPD, con el contenido mínimo indicado en dicho artículo, así como el resultado de dicha evaluación.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá 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.

XVII Pago voluntario

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, en el acuerdo de inicio se ofreció a la parte reclamada el reconocimiento de 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 **4.000.000 euros,** resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo, en el citado acuerdo y de acuerdo con el precepto indicado se le permitía, 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 **4.000.000 euros** y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Asimismo, se indicaba que la reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, en cuyo caso, **si procediera aplicar ambas reducciones**, el importe de la sanción quedaría establecido en **3.000.000 euros.**

Tras la presentación de las alegaciones, y antes de que se dictase propuesta de resolución por parte de esta autoridad, la parte reclamada, en fecha 12 de abril de 2024, procedió a realizar el pago voluntario sin reconocer su responsabilidad, acogiéndose a la reducción del 20% y renunciado a cualquier acción o recurso en vía administrativa, manifestando asimismo su intención de impugnar la citada resolución ante la jurisdicción contencioso-administrativa.

Debe de tenerse en cuenta que, de acuerdo con los preceptos de la LPCAP, así como de la jurisprudencia del alto tribunal en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al

procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

En base a las citadas premisas, teniendo en cuenta además que la parte reclamada antes del pago voluntario procedió a interponer las alegaciones que estimó oportunas frente al acuerdo de inicio, la presente autoridad ha procedido a contestar y rebatir cada una de ellas, realizando un análisis pormenorizado y fundamentando jurídicamente la imputación de las infracciones que se confirman en el presente acto, evitando de esta forma cualquier indefensión y permitiendo un mayor comprensión respecto a las cuestiones planteadas por la parte reclamada.

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 Agencia Española de Protección de Datos

RESUELVE:

PRIMERO:
DECLARAR la comisión de las siguientes infracciones y CONFIRMAR 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 las sanciones indicadas en el acuerdo de inicio por la comisión de las citadas infracciones:

Por la infracción del artículo 5.1.f): **1.000.000 € (UN MILLÓN DE EUROS)**

Por la infracción del artículo 32: **1.000.000 € (UN MILLÓN DE EUROS)**

Por la infracción del artículo 25: **2.000.000 € (DOS MILLONES DE EUROS)**

Por la infracción del artículo 35: **1.000.000 € (UN MILLÓN DE EUROS)**

La suma de las citadas cuantías arroja una cantidad total de **5.000.000 € (CINCO MILLONES DE EUROS).**

Tras haber procedido la parte reclamada al pronto pago, aunque sin reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPCAP, a la reducción de un 20 % del total mencionado, lo cual supone la cantidad definitiva de 4.000.000 € (CUATRO MILLONES DE EUROS)

SEGUNDO:
DECLARAR la terminación del procedimiento por el pronto pago realizado por GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS, con NIF A28007268, en virtud de lo dispuesto en el artículo 85 de Ley de Procedimiento Administrativo Común de las Administraciones Públicas.

TERCERO:

REQUERIR a GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS para que, en el plazo de tres meses a partir de la notificación de la presente resolución, notifique a esta Agencia la adopción de las siguientes medidas:

- La realización y superación de la evaluación de impacto de las operaciones de tratamiento en la protección de datos personales prevista en el artículo 35 del RGPD, con el contenido mínimo indicado en dicho artículo, así como el resultado de dicha evaluación.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá 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.

CUARTO:

De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, por parte de la presente autoridad se acepta la renuncia expresamente manifestada por la parte reclamada, no cabiendo en consecuencia la interposición de recurso potestativo de reposición frente a la presente resolución, todo ello sin perjuicio de la posibilidad de acudir a la vía jurisdiccional contencioso-administrativa.

En consecuencia, teniendo en cuenta lo dispuesto en el artículo 90 de la LPACAP, dado que no cabe ningún recurso en vía administrativa al haber renunciado expresamente, la presente resolución será plenamente ejecutiva a partir de la notificación de la misma.

No obstante, 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 Agencia Española de Protección de Datos, 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.

938-16012024

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