- **Expediente N.º: EXP202213514**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 21 de mayo de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<
Expediente N.º: EXP202213514

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: Con fecha 27 de octubre de 2022 ***A.A.A.*** (en adelante, la parte reclamante) con fecha 27 de octubre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A. con NIF A28007748 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que el 1 de junio de 2022, recibió un e-mail de su expareja en el que adjuntaba un documento relativo a los datos de la póliza de automóvil suscrita por la parte reclamante con la parte reclamada, así como un informe de la Dirección General de Tráfico, "extraídos de los sistemas de la compañía aseguradora a la que accedió sin estar autorizada".

Añade que dicha documentación fue aportada en el marco de un procedimiento judicial de modificación de medidas paternofiliales."

Junto a la reclamación aporta copia de los mensajes de correo electrónico recibidos, así como pantallazo relativo a los datos asociados a la póliza "Auto todo riesgo" como resultado de una búsqueda en la web de la parte reclamada y pantallazo relativo a un Informe del vehículo de la DGT.

SEGUNDO: Esta reclamación fue presentada por el reclamante ante la AEPD el 8 de agosto de 2022, dando origen al expediente EXP202210372. En el marco del citado expediente, en fecha 4 de octubre de 2022 se comunica a la parte reclamante que su reclamación registrada no ha sido admitida a trámite, IT/06061/202.

TERCERO: En fecha 27 de octubre de 2022 el reclamante reitera la reclamación presentada el 8 de agosto de 2022, expediente EXP202210372, dando lugar a la apertura de un nuevo expediente, el actual expediente EXP202213514. En el marco del actual expediente, se comunica a la parte reclamante que su reclamación presentada con fecha 27 de octubre de 2022 no ha sido admitida a trámite, IT/08015/2022.

CUARTO: En fecha 18 de enero de 2023, la parte reclamante presenta recurso de reposición contra la resolución de la Agencia Española de Protección de Datos (en adelante, AEPD o Agencia) dictada en fecha 20 de diciembre de 2022. En fecha 31 de marzo de 2023, en el procedimiento RR/00030/2023, la AEPD acuerda estimar el recurso de reposición interpuesto, admitir a trámite la reclamación formulada de acuerdo con lo establecido en el artículo 65 de la LOPDGDD, AT/01642/2023, y llevar a cabo las actuaciones previas de investigación AI/00109/2023 en relación con los hechos reproducidos anteriormente.

QUINTO: 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.

SEXTO: En fecha 24 de enero de 2024 la directora acuerda declarar la caducidad de las actuaciones previas de investigación AI/00109/2023, abrir nuevas actuaciones de investigación, AI/00063/2024, e incorporar a estas nuevas actuaciones la documentación que integra las actuaciones declaradas caducadas.

SEPTIMO: La Subdirección General de Inspección de Datos concluye sus actuaciones de investigación AI/00063/2024, el 19 de marzo de 2024, a través de las cuales ha tenido conocimiento de los siguientes extremos:

.-1-. Respecto a las evidencias aportadas en las reclamaciones.

La parte reclamante ha presentado dos reclamaciones, ambas por los mismos hechos, la primera fue de fecha 8 de agosto de 2022, -expediente EXP202210372- , y la segunda de fecha 20 de diciembre de 2022, que da lugar al actual expediente EXP202213514.

La parte reclamante aporta junto a su escrito de denuncia contra la parte reclamada, mensajes de correo electrónico remitidos a la parte reclamante por parte de su expareja con fecha 1 de junio de 2022 en los que su expareja adjunta dos capturas de pantalla:

(a) Captura de pantalla de los datos relativos a la póliza suscrita entre la parte reclamante y reclamada.

(b) Informe de la Dirección General de Tráfico.

Analizando estos anexos se extrae la siguiente información:

(a) Póliza ******POLIZA.1***
Tomador: A.A.A.

Esta captura de pantalla incluye los datos personales del tomador asegurado y es, presumiblemente, una captura de pantalla de la aplicación interna de gestión de clientes de la parte reclamada.

(b) Informe DGT del vehículo ******MATRICULA.1***: Informe con fecha 30/05/2022
Dato titular: ***B.B.B.***.
ID Vehículo: Matrícula, marca, bastidor, etc.
Dato seguro: Allianz

El informe incluye (i) el historial de titulares junto con la información sobre fecha inicio/fecha fin/ tipo particular y (ii) el historial de ITVs.

La persona solicitante del informe es ***C.C.C.*** con Fecha 30/05/2022 y a través del Canal Internet.

Al buscar información sobre dicha persona en internet se revela que existe una abogada con dicho nombre especializada en divorcios con sede en A Coruña.

Con fecha 19 de julio de 2023 se consulta la sede electrónica de la Dirección General de Tráfico en lo relativo a la solicitud de informes de vehículos, de la que se obtiene la siguiente información:

.- Anexo 1. - INFORME DE UN VEHÍCULO. ¿Qué debes saber?

"*Salvo el caso del informe de 'vehículos a mi nombre', que necesitas ser el titular del vehículo o una tercera persona autorizada en su nombre para descargarlo, el resto de informes están disponibles para cualquier persona, sea o no el titular del vehículo*."

.- Anexo 2. - INFORME DE UN VEHÍCULO. ¿Qué tipos de Informes puedo obtener?

"*Informe completo: Incluye toda la información administrativa, identificación del titular, municipio donde está domiciliado el vehículo, historial de ITV, kilometraje, número de titulares, cargas… así como datos técnicos, puntuación EuroNCAP y mantenimiento respecto al vehículo solicitado*."

.- Anexo 3. - Ejemplo de informe completo de un vehículo.

Consultada la parte reclamante por el nombre de la abogada de su expareja, se confirma que coincide con el nombre de la persona que aparece en el anexo como solicitante del informe del vehículo a través del canal de internet.

Por lo tanto, esta evidencia no está facilitada por la parte reclamada, sino que el informe lo solicitó directamente la abogada de la expareja de la parte reclamante en la sede electrónica de la Dirección General de Tráfico, ya que es un informe público.

Con fecha 6 de marzo de 2024 se graba de nuevo diligencia en el sistema SIGRID con la información anterior y la actualización de los enlaces de la sede electrónica de la Dirección General de Tráfico donde se puede obtener dicho informe:

- https://sede.dgt.gob.es/es/vehiculos/informacion-de-vehiculos/informe-de-un-vehiculo/

- https://sede.dgt.gob.es/export/sites/dgt/.galleries/ayuda/informe-completo.pdf

.-2-. Respecto a la información aportada en las respuestas a los requerimientos de información

.-2.A-. Con fecha 24 de julio de 2023 se realiza un requerimiento de información a la parte reclamada solicitándole, entre otros puntos, confirmación de que la captura de pantalla pertenece al programa de gestión de clientes de ALLIANZ y el Protocolo de acceso a los datos de las pólizas.

La parte reclamada responde a este requerimiento de información con fecha de registro 11 de agosto de 2023, proporcionando la siguiente documentación en su escrito de respuesta:

.- Copia de la póliza que acredita la titularidad de la parte reclamante durante el tiempo en que estuvo vigente dicha póliza.

.- Guía rápida sobre la calidad de la llamada, en la que se describe el procedimiento seguido por la Compañía a los efectos de verificar la identidad de la persona que realiza la llamada y comprobar que el que llama es el tomador y no un tercero.

.- Diagrama de acceso por parte de los usuarios a los distintos aplicativos que conforman el programa de gestión de clientes de la Compañía.

.- Movimientos producidos en la póliza de la parte reclamante.

.-2.B-. Con fecha de registro 18 de septiembre de 2023, la parte reclamada remite a esta Agencia un Escrito adicional a la contestación requerimiento de información, en el que proporciona la siguiente documentación en su escrito de respuesta:

.- Escrito de contestación a dicho Requerimiento de Información

.- Justificante de la brecha comunicada por parte de la parte reclamada ante el registro electrónico de la AEPD.

.- Código de conducta del grupo ALLIANZ, de obligado cumplimiento para todos los empleados

.- Captura de pantalla de las últimas formaciones recibidas por la empleada causante de la incidencia.

.-2.C-. Con fecha 1 de febrero de 2024 se realiza un requerimiento de información a la parte reclamada de solicitándole, entre otros puntos, la justificación de la necesidad de que la empleada que originó la brecha tuviera permisos de acceso a los datos de la parte reclamante y la acreditación de las instrucciones que ALLIANZ comunicó previamente a dicha trabajadora sobre el tratamiento de los datos de los clientes.

La parte reclamada responde a este requerimiento de información con fecha de registro 15 de febrero de 2024, proporcionando la siguiente documentación en su escrito de respuesta:

.- Inscripción de Delegada de Protección de Datos ante la lista de Delegados de Protección de Datos

.- Código de Conducta del grupo ALLIANZ, de obligado cumplimiento para todos los empleados

.- Norma (interna) de uso aceptable de los activos

.- Norma (interna) de clasificación de la información

.- Capturas de la pantalla de inicio de los cursos disponibles en la actualidad en materia de protección de datos y confidencialidad

.- Historial de las formaciones realizadas por la empleada

.- Procedimiento de definición y mantenimiento de roles y accesos

.- Procedimiento de gestión de certificados ID (ID Certification Management Procedure)

.- Confirmaciones por los responsables de cada unidad de Allianz en el ámbito de la auditoría y revisión llevada a cabo de los permisos de cada usuario

.- Informe emitido por el Delegado de Protección de Datos de Allianz en fecha 13 de septiembre de 2023 acerca los hechos que causaron la brecha

.- Copia del Registro de Actividades del tratamiento donde se ha producido el incidente

.- Análisis de riesgos para la seguridad de las referidas actividades del tratamiento llevado a cabo por Allianz de conformidad con el artículo 32 del RGPD

.- Copia de la información que consta en el registro de incidentes en relación con dicha brecha, donde fue registrada en fecha 24 de julio de 2023

.- Captura de pantalla de la página de inicio del portal “Protección de datos en Allianz y la Comunidad Privada de Allianz” ubicado dentro de la Intranet de Allianz

.- Copia del documento Estándar de privacidad del Grupo Allianz

.-2.1-. Respecto el caso particular de la parte reclamante

.-2.1.1-. Respuesta al primer requerimiento de información

La parte reclamada, en su escrito de respuesta proporciona la siguiente información y manifestaciones:

.- Confirma y aporta evidencias acerca de que el titular de la Póliza era la parte reclamante e indica que dicha Póliza no se encuentra en la actualidad vigente al haber sido solicitada su anulación por parte del titular en fecha 30 de junio de 2022 como consecuencia de la venta del vehículo y habiendo procedido la Compañía a anular dicha póliza con efectos a 5 de julio de 2022;

.- Confirma que *“la imagen del anexo incorporado al requerimiento de información requerido se corresponde con el aplicativo “consultas generales” del programa de gestión de clientes de la Compañía”*

.- Indica que no dispone de los accesos a dicha Póliza entre las fechas 31 de mayo de 2022 y 2 de junio de 2022 ***(…)***. *Es por ello no podemos facilitarles la información solicitada al no disponer de ella*”.

.- Confirma y aporta evidencias que en fecha 1 de junio de 2022 no se ha producido ninguna modificación en dicha Póliza;

.- Informa que a fecha de presentación del escrito no es conocedora de ninguna incidencia ni de ningún acceso no autorizado por parte de terceras personas a los datos de la Póliza, por lo que no dispone de ninguna información adicional a aportar, si bien comunica que *“la Compañía ha iniciado una investigación como consecuencia de su requerimiento de información que aún se encuentra en curso y de la que les informaremos oportunamente de su resultado una vez finalizada la misma en el supuesto que como resultado de dicha investigación tuviésemos conocimiento de la existencia de cualquier incidencia o de cualquier acceso no autorizado por parte de terceras personas.”*

.-2.1.2-. Ampliación de información de la respuesta al primer requerimiento de información

Como resultado de la investigación interna iniciada a consecuencia del requerimiento de información, la parte reclamada indica en que el origen de la incidencia es una empleada del Centro de Tramitación de Siniestros (CTS) de la Compañía ***(D.D.D.)*** *“quien, incumpliendo las políticas en materia de protección de datos de la Compañía y el código de conducta aplicable a todos los empleados de la Compañía que recoge el deber de confidencialidad que tienen todos los empleados en relación con los datos de*

carácter personal a los que puedan acceder para el ejercicio de sus funciones, procedió en junio de 2022 a realizar una captura de imagen de la información que consta en el aplicativo "consultas generales" del programa de gestión de clientes de la Compañía de la póliza que se corresponde con la imagen sobre la que en el Requerimiento de Información se solicitó confirmación por parte de la Compañía que correspondía a su programa de gestión de clientes, y procedió a facilitarle a la exesposa del titular de la Póliza con quien la referida empleada mantenía una relación de amistad para que esta pudiera probar que su exesposo era titular de dicha Póliza en el marco del procedimiento judicial de divorcio existente entre el titular de la póliza y la exesposa. Dicha comunicación no autorizada, que fue realizada por parte de la empleada de forma intencionada y a sabiendas de su ilicitud, supone una brecha de la confidencialidad de datos personales que la Compañía ha procedido a comunicar el pasado 14 de septiembre dentro del plazo de setenta y dos (72) horas desde que se tiene conocimiento de la misma establecido por la normativa vigente."

(Nota: el subrayado ha sido incorporado por la Agencia)

La parte reclamada aporta Código de conducta de la Compañía, de obligado cumplimiento para todos los empleados, donde se refleja el deber de confidencialidad; y Captura de pantalla de las últimas formaciones recibidas por la empleada causante de la incidencia en materia de protección de datos.

ALLIANZ comunica que, "*ante la conducta realizada por la referida empleada que supone un flagrante incumplimiento del deber de confidencialidad*" ha procedido "*a informar de dichos hechos al Comité de Integridad de la Compañía para que, siguiendo los procedimientos internos establecidos, decida las acciones (incluidas, en su caso, acciones disciplinarias) a emprender contra la empleada ante tal flagrante incumplimiento*."

.-2.1.3-. Respecto a la necesidad de la empleada para poder acceder a los datos en el ejercicio de sus funciones

Revisado el documento, diagrama de acceso por parte de los usuarios a los distintos aplicativos que conforman el programa de gestión de clientes de la Compañía (ver apartado 2.2 del presente informe) y el escrito de respuesta, se confirma que la empleada causante de la incidencia estaba autorizada a acceder los datos para el desarrollo de sus funciones ya que pertenece al Centro de Tramitación de Siniestros (CTS) de ALLIANZ.

.-2.1.4-. Respecto a las instrucciones comunicadas a la empleada que originó la brecha sobre el tratamiento de los datos de los clientes

La parte reclamada especifica en su escrito de respuesta los códigos y normas internas, de aplicación a todos los empleados de la Compañía, que recogen las instrucciones para garantizar la confidencialidad de los datos personales de sus clientes (ver apartado 2.4 del presente informe) y aporta como evidencia el historial de las formaciones realizadas por la empleada.

.-2.1.5-. Respecto a los Informes técnicos o recomendaciones elaborados por el Delegado de Protección de Datos respecto del incidente ocurrido

En su escrito de respuesta, la parte reclamada proporciona el informe emitido por el Delegado de Protección de Datos de Allianz en fecha 13 de septiembre de 2023 acerca los hechos que causaron la brecha, sus consecuencias para el reclamante, las acciones llevadas a cabo para solventar la misma, incluyendo el análisis sobre la necesidad de comunicar la misma a la autoridad de control (comunicación que se realizó en fecha 14 de septiembre de 2023) y, en su caso, al reclamante, así como sobre la suficiencia de los controles existentes para evitar futuras brechas similares

Se observa que la Compañía concluye "*que las medidas implementadas por la Compañía con carácter previo al incidente son suficientes para evitar futuras brechas similares en el futuro, siendo conscientes que tal y como ha reconocido el Comité Europeo de Protección de Datos en el caso núm. 8 de su Guía 1/2021 sobre ejemplos en relación con la comunicación de brechas de datos adoptada el 14 de enero de 2021, este tipo de brechas son las más difíciles de evitar por parte de los responsables del tratamiento*."

Aporta, además, copia de la información que consta en el registro de incidentes en relación con dicha brecha, donde fue registrada en fecha 24 de julio de 2023.

.-2.2-. Respecto al protocolo de acceso a los datos de las pólizas

La parte reclamada, en su escrito de respuesta, proporciona la siguiente información y manifestaciones:

.- Indica que "*los tomadores de nuestras pólizas pueden acceder a los datos que constan en sus pólizas a través de su mediador, a través de la aplicación móvil e-cliente, a través de llamada telefónica al servicio de atención al cliente de la Compañía, así como físicamente a través de las distintas oficinas que la Compañía tiene abiertas en todo el territorio español*". ALLIANZ adjunta, guía rápida sobre la calidad de la llamada, en la que se describe el procedimiento seguido por la Compañía a los efectos de verificar la identidad de la persona que realiza la llamada y comprobar que el que llama es el tomador y no un tercero.

.- Informa que, respecto al personal de la Compañía, únicamente tienen acceso a los datos de las pólizas de sus asegurados aquellas personas que necesitan acceder a los mismos para el desarrollo de sus funciones y, con carácter general, el personal del Servicio de Atención al Cliente (SAC), de la Oficina de Soporte de Negocio (OSN), del Centro de Tramitación de Siniestros (CTS), de los servicios centrales de la Compañía, así como de la red de ventas y sucursales de la Compañía, si bien en dicho caso los agentes y corredores únicamente tienen acceso a los datos de las pólizas de las que constan como mediadores y que constituyen su cartera, indicándose las distintas tipologías de perfiles de usuario del aplicativo "consultas generales" del programa de gestión de clientes de la Compañía. Aporta, diagrama de acceso por parte de los usuarios a los distintos aplicativos que conforman el programa de gestión de clientes de la Compañía.

.-2.3-. Respecto a las medidas implementadas por la Compañía para evitar que se produzcan incidencias similares

Una vez conocida la incidencia que ha motivado la reclamación, la parte reclamada indica en su escrito de respuesta las medidas implementadas para evitar que un empleado comunique a terceros no autorizados fuera de la Compañía datos personales de los que la Compañía es responsable y a los que necesita acceder para el desarrollo de sus funciones:

"(…)"

ALLIANZ expresa que ha aprovechado para acelerar e impulsar la siguiente medida que tenía previsto llevar a cabo, consistente en enviar a todos los empleados de la Compañía un catálogo de las principales conductas de riesgo en materia de protección de datos y prohibidas por la misma en la que se incluirá el presente supuesto.

La parte reclamada aporta, copia del Registro de Actividades del tratamiento donde se ha producido el incidente, de conformidad con el artículo 30 del RGPD; y Análisis de riesgos para la seguridad de las referidas actividades del tratamiento llevado a cabo por ALLIANZ de conformidad con el artículo 32 del RGPD

.-2.4-. Respecto a las instrucciones específicas dadas por la Compañía a sus empleados con el objeto de garantizar la confidencialidad de los datos personales de sus clientes

En su escrito de respuesta, la parte reclamada indica los códigos y normas internas, de aplicación a todos los empleados de la Compañía, que recogen las instrucciones para garantizar la confidencialidad de los datos personales de sus clientes:

.- El Código de Conducta del grupo ALLIANZ, que recoge en su apartado "Gestión Responsable de Datos" el compromiso de confidencialidad que tienen los empleados respecto a los datos personales a los que puedan acceder en el desempeño de sus funciones y que establece de forma expresa la prohibición de compartirlos con terceros que no estén autorizados.

.- La Norma interna de uso aceptable de los activos, que establece en sus apartados 5.1 y 5.2 la obligación de los trabajadores de ALLIANZ de hacer un uso responsable, guardar secreto profesional y a la máxima reserva, así como estableciendo el deber de no divulgar ni utilizar directamente ni a través de terceros, los datos de carácter personal conforme lo establecido en el RGPD a los que accedan en el desempeño de sus funciones.

.- La Norma interna de clasificación de la información, que establece de forma expresa en su apartado 5.1 la obligación de todos los empleados de Allianz de no divulgar o revelar información clasificada con los niveles de Confidencial o Estrictamente Confidencial a ningún otro usuario (empleado o tercero), a menos que esté explícitamente autorizado por el propietario del activo o sea necesario para el ejercicio de sus funciones.

La parte reclamada continúa explicando que "*la normativa interna es completada por el plan de formación en materia de protección de datos y confidencialidad diseñado por la Compañía para todos sus empleados, que incluye una serie de cursos relacionados con dicha materia"*, y proporciona, capturas de la pantalla de inicio de los cursos disponibles en la actualidad en materia de protección de datos y confidencialidad.

.-2.5-. Respecto a las auditorías que ALLIANZ realiza periódicamente sobre los accesos realizados por sus trabajadores, para llevar un control de los accesos y detectar conductas que puedan ser sospechosas

La parte reclamada señala en su escrito de respuesta que "*cuenta con un Procedimiento de definición y mantenimiento de roles y accesos, para la determinación de los roles y accesos de los usuarios en los activos de la Compañía, en aras a garantizar la protección los activos de información y su confidencialidad, basando los accesos a dicha información en la necesidad legítima de los usuarios para el desarrollo de su actividad profesional.* ***(…)***."

En este sentido, aporta los documentos, Procedimiento de definición y mantenimiento de roles y accesos; Procedimiento de gestión de certificados ID (ID Certification Management Procedure); y Confirmaciones por los responsables de cada unidad de Allianz en el ámbito de la auditoría y revisión llevada a cabo de los permisos de cada usuario

OCTAVO: La AEPD ha tenido acceso al informe de auditoría de cuentas anuales emitido el 30 de marzo de 2023 por un auditor independiente, que ha facilitado el Localizador de Recursos Uniforme, es decir la ULR siguiente, ******URL.1***

Dicho documento permite determinar el volumen de negocio de la parte reclamada, utilizando la cifra del indicador "Primas devengadas – seguro directo". No obstante, como sus cuentas están divididas en "no-vida" y "vida" hay que sumar las dos:

- "no vida", primas devengadas seguro directo: 2.236.771 miles de euros (página 19)

- "vida", primas devengadas seguro directo 367.249 miles de euros (página 21).

Por lo tanto, de dicho documento se desprende que a diciembre de 2022 el volumen de negocio de la parte reclamada alcanzaba el importe de 2.604.020 miles de euros,

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

Cuestiones previas

En el presente caso, nos encontramos ante una reclamación presentada debido a la filtración de datos personales de la parte reclamante consistentes en número de póliza, matrícula de vehículo, así como nombre y apellidos del reclamante.

La parte reclamante proporciona dos capturas de pantalla como evidencias de la filtración de información.

La reclamante denuncia que su expareja ha tenido acceso a sus datos del seguro.

La parte reclamada reconoce que los datos personales de la parte reclamante fueron extraídos y filtrados por una empleada suya, que los pasó a la expareja de la parte reclamante.

No obstante, la parte reclamada afirma que esa empleada, tramitadora de siniestros de la compañía ALLIANZ, es decir, de la parte reclamada, estaba legitimada por sus funciones a tener acceso a las pólizas de los clientes entre los que se encuentra la parte reclamante.

La parte reclamada reconoce que no hay trazabilidad de accesos, y de esa falta de trazabilidad se deduce una falta medidas de seguridad.

Hay que tener en cuenta que la trazabilidad es un instrumento que precisamente permite controlar la posibilidad de existencia de accesos indebidos, sin perjuicio de que existan perfilados.

Además, en este caso se ha extraído un pantallazo de la aplicación, pese a que hay aplicaciones que impiden la captura de pantallazos de las aplicaciones para evitar un posible filtrado de información.

Se ha confirmado que la primera evidencia es una captura de pantalla de la aplicación interna de gestión de clientes de la parte reclamada y la segunda evidencia es una captura de pantalla del informe público que se puede obtener a través de la sede electrónica de la Dirección General de Tráfico.

La parte reclamada ha iniciado una investigación interna como consecuencia del requerimiento de información y, como resultado, ha comunicado que el origen de la incidencia fue una empleada del Centro de Tramitación de Siniestros (CTS) de la Compañía (***D.D.D.***) que realizó en junio de 2022 una captura de imagen de la información que consta en el aplicativo “consultas generales” del programa de gestión de clientes de la Compañía respecto a la póliza de la parte reclamante y procedió a facilitar a la exesposa del titular de la Póliza, con quien la referida empleada mantenía una relación de amistad.

Las actuaciones de investigación han permitido constatar que la empleada causante de la incidencia estaba autorizada a acceder los datos para el desarrollo de sus funciones ya que pertenecía al Centro de Tramitación de Siniestros (CTS) de ALLIANZ

A través de dichas actuaciones de investigación se ha evidenciado que la parte reclamada proporcionó instrucciones sobre el tratamiento de los datos de los clientes a todos los empleados de la compañía, en particular a la empleada que originó la brecha de seguridad, ya que la parte reclamada ha facilitado el historial de las formaciones realizadas por la empleada en materia de protección de datos y confidencialidad.

Asimismo, mediante la investigación previa realizada se ha comprobado que el Delegado de Protección de Datos elaboró un informe respecto del incidente ocurrido, en el que se concluye la necesidad de comunicar la brecha de confidencialidad a la autoridad de control (comunicada en fecha 14 de septiembre de 2023).

Además, la parte reclamada ha proporcionado el protocolo de acceso a los datos de la póliza tanto para los tomadores (proporciona un documento que describe el procedimiento seguido por la Compañía a los efectos de verificar la identidad de la persona) como para el personal de la parte reclamada.

Finalmente, la parte reclamada ha detallado las medidas implementadas por la Compañía para evitar que se produzcan incidencias similares, para de esta manera proporcionar evidencias de las auditorías que realiza anualmente respecto a la gestión de certificación de la identidad.

III

Artículo 5.1.f) del RGPD

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

“Artículo 5 Principios relativos al tratamiento:

1. Los datos personales serán:

(…)

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

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

“[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento”.

El artículo 5.1 f) del RGPD, determina el cauce a través del cual ha de lograrse el mantenimiento de la confidencialidad e integridad cuando explicita “*mediante la aplicación de medidas técnicas y organizativas apropiadas*”, que no son estrictamente de seguridad.

La reclamante ha denunciado ante la AEPD que su expareja ha tenido acceso a los datos obrantes en la póliza de seguro que tiene contratada con la parte reclamada.

La parte reclamada ha reconocido que los datos personales de la parte reclamante fueron extraídos y filtrados por una empleada suya, tramitadora de siniestros, y facilitados por a la expareja de la parte reclamante.

La parte reclamada se justifica indicando que su empleada para realizar el ejercicio de sus funciones ha de tener acceso a los datos personales de la parte reclamante.

Ni lo anteriormente indicado, ni la supuesta relación de amistad entre la trabajadora de la compañía reclamada y la expareja de la parte reclamante a la que se han cedido los datos, permiten justifican ni legitimar los hechos objeto de denuncia, es decir, que se haya dado acceso a los datos personales de la parte reclamante a su expareja sin su consentimiento.

De conformidad con las evidencias de las que se dispone en el presente momento, y sin perjuicio de lo que resulte de la instrucción, se podría considerar que los hechos denunciados consistentes en que una empleada de la entidad reclamada, haya dado acceso a los datos personales de la parte reclamante, a una tercera persona sin contar con el consentimiento del titular de dichos datos personales, podría implicar que la parte reclamada como responsable última del tratamiento de los datos personales de la parte reclamante, habría vulnerado la confidencialidad exigidas en la normativa de protección de datos de carácter personal, por carecer de las medidas técnicas y organizativas apropiadas en el tratamiento de los datos personales de los que es responsable.

Por lo tanto, existen indicios claros de un tratamiento contrario a la normativa de protección de datos personales por parte de la entidad reclamada, porque se habría vulnerado el artículo 5.1 f) del RGPD, precepto donde se establece el principio de integridad y confidencialidad en el tratamiento de datos personales.

IV

Tipificación 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. (…)"

V

Sanción del artículo 5.1f) del RGPD

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

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

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

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para 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,

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

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

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

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

a) El carácter continuado de la infracción.

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

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

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

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

f) La afectación a los derechos de los menores.

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

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

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

Como agravantes:

Artículo 83.2 e) RGPD: "toda infracción anterior cometida". El 10 de mayo de 2021 se impuso a la parte reclamada una sanción de 30.000 euros (treinta mil euros), por realizar un tratamiento ilegítimo de los datos personales, en el PS/00123/2021

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

reclamada realiza para el desarrollo de su actividad, un elevado volumen de tratamiento de datos personales.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 140.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad.

VI

Artículo 32 del RGPD

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

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

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

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".

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el 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, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse 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 se tendrán 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.

En este mismo sentido 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".

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad adoptadas, con las peculiaridades que presenta, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

Por lo tanto, esta Agencia considera que también podría haberse vulnerado el artículo 32 del RGPD, al no haberse cumplido por parte de la entidad reclamada, con la

obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar en este caso concreto.

Para valorar el alcance de tales hechos eje del presente procedimiento sancionador, hay que tener en cuenta que la trazabilidad es un instrumento que permite controlar la posibilidad de existencia de accesos indebidos.

La parte reclamada manifiesta que, respecto al personal de la Compañía, únicamente tienen acceso a los datos de las pólizas de sus asegurados aquellas personas que necesitan acceder a los mismos para el desarrollo de sus funciones y, con carácter general, el personal del Servicio de Atención al Cliente (SAC), de la Oficina de Soporte de Negocio (OSN), del Centro de Tramitación de Siniestros (CTS), de los servicios centrales de la Compañía, así como de la red de ventas y sucursales de la Compañía, si bien en dicho caso los agentes y corredores únicamente tienen acceso a los datos de las pólizas de las que constan como mediadores y que constituyen su cartera, indicándose las distintas tipologías de perfiles de usuario del aplicativo "consultas generales" del programa de gestión de clientes de la Compañía. Aporta, diagrama de acceso por parte de los usuarios a los distintos aplicativos que conforman el programa de gestión de clientes de la Compañía.

Señala además que una vez conocida la incidencia que ha motivado la reclamación, ha aprovechado para acelerar e impulsar una medida que tenía previsto llevar a cabo, consistente en enviar a todos los empleados de la Compañía un catálogo de las principales conductas de riesgo en materia de protección de datos y prohibidas por la misma en la que se incluirá el presente supuesto.

La parte reclamada aporta los códigos y normas internas, de aplicación a todos los empleados de la Compañía, que recogen las instrucciones para garantizar la confidencialidad de los datos personales de sus clientes:

La parte reclamada continúa explicando que "*la normativa interna es completada por el plan de formación en materia de protección de datos y confidencialidad diseñado por la Compañía para todos sus empleados, que incluye una serie de cursos relacionados con dicha materia"*, y proporciona, capturas de la pantalla de inicio de los cursos disponibles en la actualidad en materia de protección de datos y confidencialidad.

La parte reclamada señala que "*cuenta con un Procedimiento de definición y mantenimiento de roles y accesos, para la determinación de los roles y accesos de los usuarios en los activos de la Compañía, en aras a garantizar la protección los activos de información y su confidencialidad, basando los accesos a dicha información en la necesidad legítima de los usuarios para el desarrollo de su actividad profesional.* ***(…)***"

En este sentido, la parte reclamada aporta los documentos, Procedimiento de definición y mantenimiento de roles y accesos; Procedimiento de gestión de certificados ID (ID Certification Management Procedure); y Confirmaciones por los responsables de cada unidad de Allianz en el ámbito de la auditoría y revisión llevada a cabo de los permisos de cada usuario

La AEPD considera que a raíz de las actuaciones previas de investigación se ha comprobado que la parte la parte reclamada carecía de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presenta el tratamiento de datos personales en una compañía de seguros como la de parte reclamada, pues entre estos riesgos, se encontraba el riesgo de captura de las pantallas con los datos personales contenidos en las pólizas.

Por lo que, concurriendo tal riesgo de captación ilícita, su deber como responsable del tratamiento de estos datos personales era preverlo, y adoptar "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", que se dirigieran a impedir que cualquier miembro de la organización pueda captar esos datos personales y transmitirlos fuera de la organización.

Por lo tanto, de conformidad con las evidencias de las que se dispone en el presente momento y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

VII
Tipificación 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."

VIII
Sanción del artículo 32 del RGPD

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

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

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

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para 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,

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

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

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

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

a) El carácter continuado de la infracción.

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

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

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

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

f) La afectación a los derechos de los menores.

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

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

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

Como agravantes:

Artículo 83.2 e) RGPD: "toda infracción anterior cometida". El 10 de mayo de 2021 se impuso a la parte reclamada una sanción de 30.000 euros (treinta mil euros), por realizar un tratamiento ilegítimo de los datos personales, en el PS/00123/2021

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

reclamada realiza para el desarrollo de su actividad, un elevado volumen de tratamiento de datos personales.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 60.000 € por infracción del artículo 32 del RGPD, respecto a la seguridad del tratamiento de los datos personales.

IX
Responsabilidad

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

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

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

X
Medidas

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

En concreto en este caso las medidas consistirían en notificar en el plazo de tres meses desde la recepción de la resolución dictada, que la entidad responsable del tratamiento de datos personales se ajusta a las disposiciones del presente Reglamento, garantizando el principio de integridad y confidencialidad de los datos personales tratados, de conformidad con el artículo 5.1 f) del RGPD, la adopción de medidas técnicas y organizativas oportunas para garantizar la trazabilidad de los accesos a los datos personales de sus clientes, para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, así como la capacidad para restaurar la disponibilidad y el acceso a los datos personales tras un incidente como el que nos ocupa, así como contar con un adecuado proceso de verificación, evaluación y valoración de la eficacia de tales medidas, de conformidad con el artículo 32 del RGPD.

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

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

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A., con NIF A28007748, por la presunta infracción del [por las presuntas infracciones de los artículos 5.1. f) y 32 del RGPD, tipificadas conforme a lo dispuesto en los artículos 83.5 del RGPD, respecto de la infracción del artículo 5.1 f) del RGPD calificada como muy grave y a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD, y de conformidad con el artículo 83.4 del RGPD, respecto de la infracción del artículo 32 del RGPD calificada como grave y a efectos de prescripción en los artículos 73 f) de la LOPDGDD.

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

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

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de 140.000€ (ciento cuarenta mil euros) por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad, y de 60.000 € (sesenta mil euros) por infracción del artículo 32 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales, sin perjuicio de lo que resulte de la instrucción, lo que supone una multa total de 200.000€ (dos cientos mil euros)

QUINTO: NOTIFICAR el presente acuerdo a ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A., con NIF A28007748, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de expediente que figura en el encabezamiento de este documento.

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

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 160.000 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en [Introduzca el texto correspondiente a 160.000 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 120.000 euros.

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

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente 160.000 o 120.000 euros, deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

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

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

En cumplimiento de los artículos 14, 41 y 43 de LPACAP, se advierte que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica por comparecencia en la sede electrónica del Punto de Acceso General de la Administración o a través de la Dirección Electrónica Habilitada única y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a

disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

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

935-18032024

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

SEGUNDO**:** En fecha 4 de junio de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **160000 euros** haciendo uso de una de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente. Por tanto, no ha quedado acreditado el reconocimiento de responsabilidad.

TERCERO**:** El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere el Acuerdo de Inicio.

CUARTO: En el Acuerdo de inicio transcrito anteriormente se señalaba que podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".

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

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

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

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

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

Habiéndose procedido al pago de la sanción de carácter pecuniario, de conformidad con el apartado 2 de este artículo, el pago voluntario implica la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada. Por tanto, procede la imposición de las medidas necesarias para que cese la conducta o se corrijan los efectos de la infracción.

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

PRIMERO: DECLARAR la terminación del procedimiento **EXP202213514**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a ***ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.*** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del Acuerdo de inicio transcrito en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a ***ALLIANZ COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.***.

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

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

1309-16012024

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