- **Expediente N.º: EXP202209203**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 3 de octubre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202209203

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 4 de julio de 2022, ***A.A.A.*** en representación de ***B.B.B.*** (en adelante, la parte reclamante) presentó reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra **MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.** con NIF A28141935 (en adelante, MAPFRE o la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante es avalista en un contrato de alquiler suscrito por su hija.

Los propietarios de la vivienda (para protegerse frente a posibles impagos) realizan (con la parte reclamada) un seguro de alquiler, en virtud del cual, la parte reclamada solicita a la parte reclamante la aportación de sus tres últimas nóminas y documento que certifique el carácter indefinido del contrato de trabajo, documentación que es aportada.

No obstante, y tras la entrega de dicha documentación, la parte reclamada solicita, además, la entrega de copia de la declaración del IRPF de la parte reclamante, así como su vida laboral.

A raíz de lo solicitado, la parte reclamante solicita (en fecha 17 de junio de 2022) conocer la finalidad del tratamiento de los datos solicitados, así como los destinatarios de sus datos y las posibles cesiones de los mismos, recibiendo respuesta de la parte reclamada (en fecha 17 de junio de 2022) indicando, por un lado, que la parte reclamante no es cliente de la entidad y, por otra parte, que la información la solicita el propietario de la vivienda.

En consecuencia, la parte reclamante, presenta reclamación ante esta Agencia por considerar que la parte reclamada solicita a la parte reclamante (avalista) sus datos personales sin garantizar la protección de los mismos, alegando que los datos los solicita el propietario de la vivienda.

Junto a la reclamación se aporta intercambio de e-mails con la parte reclamada relativos a los requerimientos de documentación, a la solicitud de información en relación el tratamiento de los datos y copia de la respuesta recibida a la solicitud de acceso, en la que se indica lo siguiente:

"El avalista no es nuestro cliente, y la documentación que nos remiten queda archivada en el sgo y si se emite la póliza la adjuntamos en un archivo especial para que desde SSCC las revisen puesto que hay operación de protecciones que nos auditan. Gracias Saludos".

Asimismo, se aporta copia de una hoja informativa entregada en otra oficina de la parte reclamada, en donde se recogen los documentos a aportar en los seguros de impago.

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), con fecha 7 de septiembre de 2022, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

Una vez realizado traslado de la reclamación a la parte reclamada, con fecha de 7 de octubre de 2022 se recibe en esta Agencia escrito remitido por esta parte manifestando que dado que la parte reclamante solicita información relativa al tratamiento de sus datos personales, se le ha remitido una nueva comunicación por la que se le informa sobre las circunstancias relativas al tratamiento de sus datos, así como en la forma en que dicha información ya se ha incorporado a la documentación de la póliza entregada al tomador del seguro que es quien, en definitiva, ha contactado y solicitado al avalista la entrega de la documentación necesaria para formalizar la póliza de Seguro de Protección de Alquileres.

La parte reclamada añade que en el contexto de la suscripción de las pólizas de seguro de protección de alquileres, y tal y como se establece en el documento de NORMAS DE EMISIÓN y SUSCRIPCIÓN de la entidad, es el tomador o arrendador quien se relaciona con la entidad desde el momento de la solicitud del seguro y es

quien, a partir del cuestionario para la conclusión del contrato declara a mi representada todas las circunstancias e información necesaria para la valoración del riesgo, entre las que se encuentra la de verificar la capacidad de pago del inquilino y de almacenar la documentación que acredita dicha capacidad, incluida, en su caso, la de la persona del avalista.

En consecuencia, la obligación y compromiso de verificar la capacidad de pago suficiente del inquilino y aportar a la entidad toda la documentación económica del inquilino o su avalista que lo acredite en el momento de la formalización del contrato, corresponde al arrendador tomador de la póliza.

Concluyen por lo tanto, que los documentos señalados en la reclamación para la evaluación del riesgo (nómina, contrato, etc.) son recabados por el tomador del seguro, el cual, mediante su adhesión a la solicitud o contrato, ha reconocido y garantizado a la entidad *"haber recabado y contar con el consentimiento previo de los mismos para la comunicación de sus datos y haberles informado, con carácter previo a su inclusión en el presente documento, de las finalidades del tratamiento, comunicaciones y demás términos previstos en el mismo y en la Información Adicional de Protección de Datos."*

No obstante, según manifestaciones de la parte reclamada, al recibir el traslado de la reclamación, interpretaron que el arrendador no había informado apropiadamente a la parte reclamante sobre el tratamiento de sus datos personales y remitieron una comunicación el 7 de octubre de 2022 por correo electrónico a la parte reclamante informándole de lo establecido en el artículo 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo, RGPD).

Y adjuntan la siguiente documentación relevante:

- Normas de emisión, suscripción y tarifas protección de alquileres 2022.
- Condiciones Particulares Seguro Protección de alquileres
- Solicitud y Cuestionario del Seguro de Protección de Alquileres
- Copia de correo electrónico con fecha de 7 de octubre de 2022 remitido por la parte reclamada a la parte reclamante informando del tratamiento de sus datos personales.

TERCERO: Con fecha 4 de octubre de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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

Respecto a los datos recabados.

Se comprueba que en el documento “IT. ATNV. PP. NORMAS DE EMISIÓN, SUSCRIPCIÓN Y TARIFAS PROTECCIÓN DE ALQUILERES 2022 - Producto Seguro Protección de Alquileres - RAMO 027” (folio 10) se establece en el epígrafe 2.2 letra A que las opciones de documentación requerida para una persona física trabajadora por cuenta ajena o funcionario es, de forma alternativa:

- Última nómina donde figure la antigüedad y el tipo de contrato (en caso de que no quede detallado expresamente se debe adjuntar certificado de la empresa que lo acredite, copia del contrato de trabajo o vida laboral) y última declaración de la renta. No obstante, sin que exista condicionante alguno, se ofrecen las siguientes alternativas:
- Aval bancario por el importe mínimo de tres mensualidades de renta.
- Aval personal de un fiador con capacidad de pago suficiente acreditada con la documentación indicada en el primer punto de esta relación.

En el caso que nos ocupa, y según la presente reclamación, se eligió la primera opción.

Solicitado al DPD de la parte reclamada informe sobre el producto “Seguro de Alquiler”, con fecha de 30 de noviembre de 2022 se recibe en esta Agencia, el informe requerido manifestando que *“los documentos indicados para demostrar la solvencia del inquilino son alternativos y su selección se hace en consonancia con la calidad de arrendatario, la cual conoce exclusivamente el tomador del seguro porque es él quien tiene en su poder los documentos del arrendatario, por lo tanto, el agente comercial cumple una función orientadora de información sobre las opciones documentales que estipula la entidad.”*

Examinada la documentación obrante en el expediente, se comprueba que entre las condiciones de contratación consta que la obligación de recabar estos documentos recae en el arrendador/tomador del seguro.

En este sentido, se constata en el documento “Solicitud y Cuestionario del Seguro de Protección de Alquileres” (Plantillas y formularios Perdidas Pecuniarias 5-2019, folio 2) el párrafo *“El solicitante en su calidad de arrendador de la vivienda descrita declara que ha recibido y obran en su poder alguno de los siguientes documentos aportados por el/los arrendatario/s o fiador/es en caso de aval personal, a efectos de justificar la capacidad de pago del arrendatario/s […]”* y en el apartado de observaciones de las Condiciones Particulares Seguro, folio 2 firmado por el tomador del seguro *“El tomador en su calidad de arrendador de la vivienda descrita declara que: ha recibido y obran en su poder algunos de los siguientes documentos aportados por los arrendatarios o fiadores en caso de aval personal, […]”*.

Respecto al deber de informar

En el informe emitido por el DPD de la entidad reclamada acerca del producto “Seguro de Alquiler” se declara que *“El inquilino es un tercero, con el que MAPFRE ESPAÑA no tiene relación jurídica alguna. Es, por tanto, el propietario/arrendador que quiere contratar la protección de su alquiler, el que solicita a su futuro inquilino, los datos, y le informa de la finalidad con van a ser tratados.”*, así mismo en este informe el DPD manifiesta que la obligación de informar al arrendatario recae sobre el arrendador/tomador del seguro.

De acuerdo con estas manifestaciones, se comprueba en los documentos Solicitud y Cuestionario del Seguro de Protección de Alquileres (documento Plantillas y Formularios, folio 3) y Condiciones Particulares Seguro, folio 5 (firmado este último por

el tomador del seguro, la existencia del párrafo *"en caso de que los datos personales facilitados se refieran terceras personas, el tomador del seguro reconoce y garantiza "haber recabado y contar con el consentimiento previo de los mismos para la comunicación de sus datos y haberles informado, con carácter previo a su inclusión en el presente documento, de las finalidades del tratamiento, comunicaciones y demás términos previstos en el mismo y en la Información Adicional de Protección de Datos".*

Requerido al arrendador documento en el que se informara a la parte reclamante del tratamiento de sus datos personales, con fecha de 31 de mayo de 2023 se recibe en esta Agencia, escrito de respuesta manifestando que no posee ningún documento en el que se pueda verificar que informó correctamente a la parte reclamante del tratamiento de sus datos personales porque esta información se produjo verbalmente.

La parte reclamada aportó, entre otra, la siguiente documentación:

- Copia del contrato de arrendamientos de 11 de junio de 2022
- Informe de evaluación de cumplimiento seguro de protección de alquiler
- Condiciones particulares del seguro de protección del alquiler de 29 de junio 2021 firmado por Mapfre y el tomador del seguro
- Documento denominado "IT.ATNV.PP.NORMAS DE EMISIÓN, SUSCRIPCIÓN Y TARIFAS PROTECCIÓN DE ALQUILERES 2022
- Plantilla de solicitud y cuestionario del seguro de protección de alquileres

FUNDAMENTOS DE DERECHO

I

De acuerdo con lo dispuesto en los artículos 58.2 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2 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

El artículo 4 *"Definiciones"* del RGPD define los siguientes términos a efectos del Reglamento:

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

"2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

En el presente caso, a tenor del artículo 4.1 del RGPD, se produce un tratamiento de datos personales, tanto del tomador del seguro como de terceras partes (en este caso, el avalista) que tienen que aportar información que incluye datos personales, para la celebración del contrato de seguro.

MAPFRE realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

En nada influye, como se verá más adelante, que MAPFRE, en relación con sus obligaciones de información, establezca en sus condiciones generales de contratación que será el tomador del seguro el que se encuentre obligado a "*"haber recabado y contar con el consentimiento previo de los mismos para la comunicación de sus datos y haberles informado, con carácter previo a su inclusión en el presente documento, de las finalidades del tratamiento, comunicaciones y demás términos previstos en el mismo y en la Información Adicional de Protección de Datos".*

III
Artículo 5.1.c) del RGPD

El artículo 5 del RGPD establece que *"los datos personales serán:*

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

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

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

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

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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»).

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

En relación con el principio recogido en la letra c) anterior (“minimización de datos”) de la reclamación recibida en esta Agencia y la investigación llevada a cabo, se deduce lo siguiente:

A la parte reclamante se le requirió por MAPFRE la aportación de sus tres últimas nóminas y de un documento que certifique el carácter indefinido del contrato de trabajo, documentación que es aportada. No obstante, y tras la entrega de dicha documentación, la parte reclamada solicita, además, la entrega de copia de la declaración del IRPF de la parte reclamante, así como su vida laboral.

La parte reclamada ha aportado un documento denominado “NORMAS DE EMISIÓN, SUSCRIPCIÓN Y TARIFAS PROTECCIÓN DE ALQUILERES”. Pues bien, en el mismo se relaciona la documentación que, en caso de mediar aval, debe proporcionarse por el avalista:” *Última nómina donde figure la antigüedad y el tipo de contrato (en caso de que no quede detallado expresamente se debe adjuntar certificado de la empresa que lo acredite, copia del contrato de trabajo o vida laboral) y última declaración de la renta*.”

A este respecto debe recordarse que la parte reclamante afirmó haber aportado, aparte de las tres últimas nóminas, un certificado que acreditaba el carácter indefinido del contrato de trabajo. Dado que ese documento se exige alternativamente a la copia del contrato o la vida laboral, una vez aportado no sería necesaria la aportación de ninguno de los otros dos.

Por ello, esta Agencia, examinando los hechos denunciados, considera que exigir la vida laboral para la formalización del contrato de seguro de alquiler, después de haber sido aportada un documento que certificaba el carácter indefinido del contrato laboral, podría suponer la vulneración del principio de minimización de datos personales que

exige que su tratamiento sea adecuado, pertinente y limitado a lo necesario en relación con los fines para los que son tratados.

IV
Tipificación de la infracción del artículo 5.1.c) 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 por la infracción del artículo 5.1.c) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- *b) la intencionalidad o negligencia en la infracción;*

En este mismo 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. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. **[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]**

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

Como agravantes:

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

MAPFRE es una gran empresa cuyo objeto social es, en relación con los hechos, enjuiciados, la realización de operaciones de seguros y reaseguros en todos los ramos y modalidades de cobertura de riesgos. Forma parte de su actividad diaria y continua el tratamiento a gran escala de datos de carácter personal para el normal desarrollo de sus actividad.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.c) del RGPD, permite fijar inicialmente una sanción de 70.000 € (SETENTA MIL EUROS).

VI
Infracción del artículo 13 del RGPD

El artículo 13 del RGPD establece la información que deberá facilitarse cuando los datos personales se obtengan del interesado, indicando lo siguiente:

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

Esta Agencia examinando los hechos denunciados considera que en este supuesto la parte reclamada solicita a la parte reclamante (avalista) sus datos personales sin facilitarle la información exigida según la normativa de protección de datos, cuando estos se obtienen del titular de los datos personales, alegando la parte reclamada en

su defensa que tales datos personales los solicita el propietario de la vivienda y que ellos los recaban en su nombre, lo que no sucedió en este caso que se examina, pues los datos se solicitaron directamente por MAPFRE al reclamante.

De este modo, la parte reclamada pretende escudarse en el hecho de que, conforme a la documentación que adjunta a sus alegaciones, sería el tomador del seguro (arrendador del inmueble) el que estaría obligado a facilitar la información relativa al tratamiento, así como de recabar la documentación necesaria al arrendatario o avalista. Pero lo cierto es que, conforme a la reclamación recibida, (y estos hechos no son negados por la parte reclamada), en el supuesto que nos ocupa MAPFRE se dirigió directamente al avalista para recabar la documentación, siendo así que no le proporcionó la información a que está obligado, como responsable del tratamiento que recaba los datos, conforme al artículo 13 del RGPD, que establece las obligaciones de información cuando los datos personales se obtienen del interesado.

Por lo tanto, como MAPFRE, en este caso concreto, requirió directamente la documentación del reclamante, el momento en que debió informar al reclamante fue en el de la recogida de datos y no en el momento de la contratación del seguro, y al no hacerlo vulnera el artículo 13 del RGPD.

Así las cosas, de conformidad con los indicios de los que se dispone en el presente momento de acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, los hechos descritos, en este caso concreto, supondrían una infracción de lo dispuesto en el artículo 13 del RGPD,

VII
Tipificación de la infracción del artículo 13 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:

b) los derechos de los interesados a tenor de los artículos 12 a 22; […]"

A efectos del plazo de prescripción de las infracciones, la infracción señalada en el párrafo anterior se considera como muy grave y prescribe a los tres años, conforme al artículo 73 h) de la LOPDGDD, que establece que:

"Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83, del Reglamento (UE) 2016/679 y, en particular, las siguientes:

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

VIII
Sanción por la infracción del artículo 13 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

b) la intencionalidad o negligencia en la infracción;

En este mismo 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. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. **[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]**

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "Sanciones y medidas correctivas" de la LOPDGDD:

Como agravante:

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

MAPFRE es una gran empresa cuyo objeto social es, en relación con los hechos, enjuiciados, la realización de operaciones de seguros y reaseguros en todos los ramos y modalidades de cobertura de riesgos. Forma parte de su actividad diaria y continua el tratamiento a gran escala de datos de carácter personal para el normal desarrollo de sus actividad.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 13 del RGPD, permite fijar inicialmente una sanción de 70.000 € (SETENTA MIL EUROS).

IX
Infracción 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."

Por otro lado, ha de indicarse que el artículo 14 del RGPD, relativo a la información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado establece lo siguiente:

"1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en

cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez. 4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

En el presente caso, hay que tener en cuenta que MAPFRE es el responsable, al establecer los medios y los fines para el tratamiento de los datos personales que concurren en la celebración y ejecución de los contratos de seguro, y por lo tanto debe garantizar la información a todos los titulares de los datos que participan en el contrato.

En el contrato de seguro de garantía del alquiler que nos ocupa se desplaza al tomador las obligaciones de obtención de documentación e información sobre la protección de datos personales. Esto consta así en diferentes documentos:

- En el documento “SOLICITUD Y CUESTIONARIO DEL SEGURO DE PROTECCIÓN DE ALQUILERES”, figura la cláusula “*El solicitante en su calidad de arrendador de la vivienda descrita declara que ha recibido y obran en su poder alguno de los siguientes documentos aportados por el/los arrendatario/s o fiador/es en caso de aval personal, a efectos de justificar la capacidad de pago del arrendatario/s para la contratación del seguro y que la situación laboral del inquilino es la que se indica (marcar con X las casillas que correspondan):”*

- En el mismo documento, y en relación con la información a terceros intervinientes, como el avalista, se indica lo siguiente "*En caso de que los datos facilitados se refieran a terceras personas físicas distintas del Tomador/Asegurado/Afectado, éste garantiza haber recabado y contar con el consentimiento previo de los mismos para la comunicación de sus datos y haberles informado, con carácter previo a su inclusión en el presente documento, de las finalidades del tratamiento, comunicaciones y demás términos previstos en el mismo y en la Información Adicional de Protección de Datos."*

Este desplazamiento en la responsabilidad de informar a terceros como el avalista sobre la protección de sus datos personales, es corroborado el propio Delegado de protección de datos de la parte reclamada, que en su informe aportado junto con las alegaciones de la parte reclamada y que no lleva fecha, afirma lo siguiente en el apartado "Deber de información":

(…).

.

Con ello, tanto de la documentación aportada como del informe del Delegado de Protección de Datos de MAPFRE, se deduce claramente que, aun siendo la obligación de información sobre protección de datos del responsable del tratamiento (en este caso MAPFRE), cuando se produce la aportación de datos personales por parte de terceras personas, como podría ser el arrendador y tomador del seguro, distintas al titular de los datos, la obligación de información (que se encuadraría en el artículo 14 del RGPD al no haberse obtenido los datos del interesado) no se ejerce por el propio responsable, sino que contractualmente se traslada al tomador del seguro.

Aparte de lo anterior, como se observa fácilmente en las alegaciones de la parte reclamada, se produce un traslado de la responsabilidad de proporcionar información sin que por parte de MAPFRE se establezca mecanismo ni procedimiento alguno que garantice que por parte del tomador se proporcione una adecuada información a los terceros. A mayor abundamiento debe señalarse que en este caso no se le proporcionó la información por parte del tomador a la parte reclamante y MAPFRE, al no tener un procedimiento diseñado para garantizar el suministro de la información, no hizo nada al respecto hasta que recibió la queja de la parte reclamante.

Al amparo de una atribución meramente formal de la responsabilidad de informar (que MAPFRE otorga al tomador del seguro), en el fondo la parte reclamada se desentiende de las obligaciones de información que le impone el artículo 14 del RGPD. No existe ninguna precaución o mecanismo de control que haga que la parte reclamada garantice que la información es realmente proporcionada. A este respecto debe insistirse en que el RGPD impone esta obligación al responsable del tratamiento, en este caso MAPFRE.

El principio de privacidad desde el diseño es una muestra del paso de la reactividad a

la proactividad y manifestación directa del enfoque de riesgos que impone el RGPD. Parte de la responsabilidad proactiva, impone que, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Así, y respecto de los riesgos que pueden estar presentes en el tratamiento, el responsable del tratamiento llevará a cabo un ejercicio de análisis y detección de los riesgos durante todo el ciclo de tratamiento de los datos, con la finalidad primera y última de proteger los derechos y libertades de los interesados, y no sólo cuando efectivamente se produce el tratamiento. 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:

> *"35. 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.*
>
> *36. 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 ello, la privacidad desde el diseño, obligación del responsable del tratamiento que nace antes de que el sistema esté en funcionamiento, no son meros añadidos que se van asentando sobre un sistema construido de espaldas al RGPD. Ligado a la edificación de una verdadera cultura de protección de datos en la organización, implica también por mor de la responsabilidad proactiva la capacidad de documentar todas las decisiones que se adopten con un enfoque "privacy design thinking", demostrando el cumplimiento del RGPD también en este aspecto.

El enfoque de riesgos hace referencia directa e inmediata a un sistema preventivo tendente a visualizar, respecto de un tratamiento de datos personales, los riesgos en los derechos y libertades de las personas físicas. En relación con los riesgos en esos derechos y libertades, han de identificarse los riesgos, evaluar su impacto y valorar la probabilidad de que aquellos se materialicen. Se protegen pues, no los datos, sino a las personas que están detrás de ellos.

Los riesgos para los derechos y libertades de las personas físicas, derivados del tratamiento de datos personales, pueden ser de gravedad y probabilidad variables y provocar daños y perjuicios físicos, materiales o inmateriales, consecuencias tangibles o intangibles, en los derechos y las libertades de las personas físicas. El considerando 75 del RGPD y el artículo 28.2 de la LOPDGDD recopilan ejemplificativamente algunos de los considerados por el legislador, mas no son los únicos. Dependerá del tratamiento y el contexto en el que este se realiza, de los datos personales tratados, de las personas involucradas, de los medios utilizados, etc.

A este respecto, la parte reclamada ha aportado, en relación con el derecho de información a que se refiere este expediente, determinada documentación que se limita a desplazar al cualquier tomador del seguro de garantía de alquiler la responsabilidad de informar a terceros intervinientes. Y ya hemos comentado que el principio de privacidad desde el diseño es una muestra del paso de la reactividad a la proactividad y es un reflejo del enfoque de riesgos que impone el RGPD.

Con la documentación aportada por MAPFRE se produce un mero desplazamiento formal de la obligación, pero no se protegen los derechos y libertades de los intervinientes, que es la finalidad última que persigue el RGPD a través de la protección de datos desde el diseño. MAPFRE no cuenta, por lo tanto, con un procedimiento para el cumplimiento del principio de responsabilidad proactiva (artículo 5.2 RGPD), ya que para ello debería haberse partido del mencionado análisis de riesgos que llevara a la adopción de medidas técnicas y organizativas, de todo tipo, para la protección de los

derechos y libertades, a partir siempre del diseño del tratamiento. No existe ningún mecanismo que establezca la parte reclamada que garantice que un posible incumplimiento por parte del tomador de la obligación de informar sea subsanada por parte del responsable. De este modo, no se controla ni garantiza ninguno de estos extremos:

- Si se ha informado o no al titular de los datos
- El contenido de dicha información
- La exactitud de la información transmitida

Desde esta óptica, en la ya mencionada Guía de Privacidad desde el diseño de la AEPD se establecen diversas orientaciones, que no se cumplen en el supuesto que nos ocupa:

"Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños. Una política de PbD se caracteriza por la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar los riesgos en lugar de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos. Es decir, la PbD huye de la "política de subsanar" y se adelanta a la materialización del evento de riesgo".

La privacidad como configuración predeterminada:

"La PbD persigue proporcionar al usuario el máximo nivel de privacidad dado el estado del arte y, en particular, que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio. La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. En el caso de que el sujeto no tome ninguna acción de configuración, su privacidad debe estar garantizada y mantenerse intacta, pues está integrada en el sistema y configurada por defecto.

Privacidad incorporada en la fase de diseño:

"*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. Para garantizar que la privacidad se tiene en cuenta desde las primeras etapas del diseño se debe:*
• Considerar como un requisito necesario en el ciclo de vida de sistemas y servicios, así como en el diseño de los procesos de la organización.
• Ejecutar un análisis de los riesgos para los derechos y libertades de las personas y, en su caso, evaluaciones de impacto relativas a la protección de datos, como parte integral del diseño de cualquier nueva iniciativa de tratamiento.
• Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque "privacy design thinking".

Así, los procedimientos de contratación de productos financieros de la parte reclamada requieren, en materia de protección de datos, de un correcto análisis de los riesgos en los derechos y libertades de los clientes, de una adecuada planificación, del establecimiento de medidas de seguridad evitativas de los riesgos, de un mantenimiento, actualización y control de aquellas desde la revisión continua de los riesgos, incluyendo la demostración del cumplimiento (observancia del principio de responsabilidad proactiva), especialmente, en el caso que nos atañe, en relación con el derecho de información. Y ello con el objeto de que se garantice el Derecho Fundamental a la Protección de Datos de los clientes, que incluye la efectiva disposición de los datos personales por los interesados, así como garantizar la información de los interesados cuyos datos están siendo objeto de tratamiento El cumplimiento de esta obligación impuesta por el RGPD al responsable del tratamiento se logra a través de la privacidad desde el diseño.

De la documentación aportada por MAPFRE en la investigación de este procedimiento se constata la inobservancia de la obligación impuesta por el artículo 25 del RGPD, sin que las medidas adoptadas por esta entidad puedan suponer el cumplimiento de lo dispuesto en dicho artículo, que exhorta a la protección de los derechos y libertades de los ciudadanos en el tratamiento de sus datos, no a la mera imposición formal de obligaciones a otros sujetos.

Los documentos aportados no contienen ningún análisis de este riesgo y, con ello, no arbitraban medidas técnicas u organizativas que podrían evitar la lesión del derecho fundamental a la protección de datos, y junto a él, los bienes y derechos de información de que son titulares los clientes de la entidad bancaria.

A este respecto, debe recordarse que conforme al artículo 25 del RGPD:

"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."

Es decir, la protección del derecho fundamental a la protección de datos no consiste en una mera espera "reactiva" a que pueda producirse un problema que lo lesione, sino que los responsables del tratamiento deben diseñar ("protección de datos desde el diseño") con carácter previo al inicio del tratamiento, las políticas adecuadas para la protección de dicho derecho fundamental. Y ello incluye todos los aspectos regulados en el RGPD, comenzando por las obligaciones de transparencia, el respeto al ejercicio de los derechos establecidos en el Reglamento, y el establecimiento de todas medidas técnicas y organizativas necesarias para garantizar el cumplimiento de dicha norma. Y todo ello debe estar planificado e implementado con carácter previo al inicio del tratamiento por el responsable.

Derivado de las actuaciones de inspección llevadas a cabo por esta Agencia, así como del resto de documentación y alegaciones presentadas por MAPFRE en este procedimiento, ha podido constatarse que dicho principio (y en consecuencia el artículo 25 del RGPD) no se cumplían por la parte reclamada. No existía un procedimiento que evite los riesgos de falta de información a terceros intervinientes en los procedimientos de contratación.

A este respecto, el análisis de riesgo es una pieza clave del principio de privacidad desde el diseño, ya que es lo que permite el establecimiento de medidas técnicas y organizativas que los eviten o, en caso de producirse, los palíen. Como se ha señalado, el artículo 25 hace especial referencia a "los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas", como presupuesto para el establecimiento de dichas medidas.

Se ha comprobado que ni el riesgo estaba establecido ni con ello las medidas implantadas. Y todo ello queda corroborado a través de la documentación del procedimiento facilitada por la reclamada.

Así las cosas, esta Agencia considera que la entidad reclamada podría haber vulnerado el artículo 25 del RGPD en relación con el artículo 14 del RGPD, que regula la protección de datos desde el diseño y por defecto, donde se exige al responsable del tratamiento la obligación de aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección 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.

Sin perjuicio de lo que resulte de la instrucción, los hechos descritos supondrían una infracción de lo dispuesto en el artículo 25 del RGPD.

X

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 que 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 efectos del plazo de prescripción de las infracciones, 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."

XI
Sanción por la infracción del artículo 25 RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

> *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;*

A este respecto conviene destacar dos aspectos concurrentes: por una parte, el número de afectados, ya que la infracción, al referirse al procedimiento establecido para garantizar el derecho de información, afecta a todas las personas físicas que intervengan en la celebración de contratos de seguro de garantía del alquiler

Y aparte, los afectados sufren un perjuicio por la infracción, toda vez que se ha visto lesionado su derecho a recibir información sobre el tratamiento de sus datos personales, abarcando aspectos tan importantes como la determinación del responsable del tratamiento, el período de conservación de los datos o su derecho a presentar una reclamación.

b) la intencionalidad o negligencia en la infracción;

En este mismo 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. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y

abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. **[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]**

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "Sanciones y medidas correctivas" de la LOPDGDD:

Como agravante:

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

MAPFRE es una gran empresa cuyo objeto social es, en relación con los hechos, enjuiciados, la realización de operaciones de seguros y reaseguros en todos los ramos y modalidades de cobertura de riesgos. Forma parte de su actividad diaria y continua el tratamiento a gran escala de datos de carácter personal para el normal desarrollo de sus actividad.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 25 del RGPD, permite fijar inicialmente una sanción de 1.000.000 € (UN MILLÓN DE EUROS).

XII

Imposición de medida

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

La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En tal caso, en la resolución que se adopte, esta Agencia podrá requerir a la entidad responsable para que, en el plazo que se determine, adecúe a la normativa de protección de datos personales las operaciones de tratamiento que realiza, con el alcance expresado en los Fundamentos de Derecho del presente acuerdo y sin perjuicio de lo que resulte de la instrucción.

En particular, se podrá ordenar el establecimiento por el responsable de un procedimiento que garantice que cuando los datos personales no sean recogidos directamente por el responsable, se garantice el suministro de información desde el

principio de privacidad desde el diseño y con los elementos que este implica, con la finalidad de otorgar la información en los términos del artículo 14

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.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones,

Por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a **MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.** con NIF A28141935, por las presuntas infracciones de los artículos 5.1c), 13 y 25 del RGPD, tipificadas en el artículo 83.5 y 83.4 de la citada norma.

SEGUNDO: NOMBRAR como instructora a ***C.C.C.*** y, como secretario, a ***D.D.D.***, indicando que podrán ser recusados, 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, y sin perjuicio de lo que resulte de la instrucción, las sanciones que pudieran corresponder serían:

- Por la presunta infracción del artículo 5.1 c) del RGPD por ser excesivo exigir la vida laboral para la celebración del contrato de seguro de alquiler, si ya se ha aportado certificado sobre el contrato de trabajo: SETENTA MIL EUROS (70.000€).

- Por la presunta infracción del artículo 13 del RGPD, ya que la entidad reclamada al formalizar no solo el contrato que nos ocupa, sino que con carácter general, cuando celebra un contrato de seguro de alquiler, no tiene ningún mecanismo para garantizar que se informa al tercero sobre el tratamiento de sus datos: SETENTA MIL EUROS (70.000€).

- Por la presunta infracción del artículo 25 del RGPD, por no informar al reclamante del tratamiento de sus datos personales en el momento de la recogida de los mismos: UN MILLÓN DE EUROS (1.000.000€).

Ello hace un total de UN MILLÓN CIENTO CUARENTA MIL EUROS (1.140.000€)

QUINTO: NOTIFICAR el presente acuerdo a **MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.** con NIF A28141935, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

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

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 912.000 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 912.000 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 684.000 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 (912.000 euros o 684.000 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

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

El procedimiento tendrá una duración máxima de 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.

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.

935-170223

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

>>

SEGUNDO**:** En fecha 26 de octubre de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **684000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

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

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

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el Acuerdo de inicio.

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."

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

PRIMERO: DECLARAR la terminación del procedimiento **EXP202209203**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a **MAPFRE ESPAÑA COMPAÑÍA DE SEGUROS Y REASEGUROS, S.A.** para que en el plazo de 9 meses 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 **MAPFRE ESPAÑA 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.

1259-121222

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