

- **Procedimiento N°: PS/00376/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. **A.A.A.** (en adelante, el reclamante) con fecha 15 de junio de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra ASESORÍA MUNIZ SOLAN, S.L. con NIF B21451364 (en adelante, la reclamada).

Los motivos en que basa la reclamación son que, como Vicepresidente de la Intercomunidad de propietarios a la que pertenece, manifiesta que al solicitar copia de un certificado emitido de reclamación de deuda de un copropietario deudor, pero en lugar de enviarle el correcto, le remitieron copia de un certificado perteneciente a un tercero, vulnerando el deber de confidencialidad.

Se aporta copia del certificado de deuda emitido a nombre de un tercero, de fecha 15 de enero de 2020.

SEGUNDO: Se trasladó al reclamado la presente reclamación el 25 de junio de 2020 y se reiteró el 13 de julio de 2020, requiriéndole para que en el plazo de un mes remitiese a esta Agencia, información sobre las causas que han motivado la incidencia que ha originado la reclamación, Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia, pero la entidad reclamada no ha contestado en el plazo señalado.

TERCERO: Con fecha 16 de octubre de 2020, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra la reclamada.

CUARTO: Con fecha 15 de diciembre de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por las presuntas infracciones de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5 a) y 83.4 a) del RGPD.

QUINTO: Notificado el citado acuerdo de inicio, la reclamada presentó escrito de alegaciones en el que, en síntesis, solicita: *“la anulación del expediente por no ir dirigido a la persona correcta y la anulación del expediente por estar indefenso esta empresa que no ha podido conocer anteriormente que se cocía en este asunto”*.

SEXTO: Con fecha 29 de diciembre de 2020, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, E/05269/2020, así como los documentos aportados por la reclamada.

SÉPTIMO: Con fecha 3 de febrero de 2021, se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a ASESORÍA MUNIZ SOLÁN, S.L., con NIF B21451364, por las infracciones de los artículos 5.1 f) y 32 del RGPD, tipificadas en los artículos 83.5 a) y 83.4 a) del RGPD respectivamente.

- por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 a) del RGPD la sanción que correspondería sería de apercibimiento requiriéndose al reclamado que proceda a adoptar las medidas necesarias para que cese la conducta objeto de esta reclamación, que ha causado la brecha de seguridad denunciada, los efectos de la infracción cometida y su adecuación a las exigencias contempladas en el artículo 32 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.
- por la infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 a) del RGPD la sanción que correspondería sería una multa por un importe de 2.000 euros (dos mil euros) sin perjuicio de lo que resulte de la instrucción.

OCTAVO: Notificada la propuesta de resolución, la parte reclamada presentó escrito de alegaciones ratificándose en las realizadas al Acuerdo de Inicio, solicitando la nulidad del expediente.

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

HECHOS PROBADOS

1.- La parte reclamada a través del Secretario-Administrador D. **B.B.B.**, envió al reclamado, como Vicepresidente de la Intercomunidad de propietarios, copia de un certificado emitido el 15 de enero de 2020 de reclamación de deuda de un copropietario deudor, pero en lugar de enviarle el correcto, le remitieron copia de un certificado perteneciente a un tercero, vulnerando el deber de confidencialidad.

2.- El reclamante aporta copia copia del certificado de deuda emitido a nombre de un tercero, de fecha 15 de enero de 2020.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD y en los art. 47 y 48.1 de LOPDGDD.

II

La valoración conjunta de la prueba documental obrante en el procedimiento trae a conocimiento de la AEPD, una visión de la actuación denunciada que ha quedado reflejada en los hechos declarados probados arriba relatados.

No obstante, en respuesta a las alegaciones presentadas por la entidad reclamada se debe señalar lo siguiente:

Sobre la afirmación que hace la entidad reclamada cuando indica que *“la anulación del expediente por no ir dirigido a la persona correcta”*. Sobre este particular, debemos señalar que consta en el presente procedimiento sancionador un certificado emitido el 15 de enero de 2020 por la reclamada a través del Secretario-Administrador, dirigido al reclamante como Vicepresidente de la Intercomunidad de propietarios sobre una reclamación de deuda de un copropietario deudor, pero en lugar de enviarle el correcto, le remitieron copia de un certificado perteneciente a un tercero, vulnerando el deber de confidencialidad. Por tanto, queda acreditada la responsabilidad de la reclamada en la remisión de la certificación de la deuda.

En relación con *“la anulación del expediente por estar indefenso esta empresa que no ha podido conocer anteriormente que se cocía en este asunto”*. Es importante resaltar que se procedió a su notificación electrónica, tal como establece el artículo 14.2.a) de la Ley 39/2015 LPACAP, y el servicio de Soporte del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada certifica que la fecha de puesta a disposición fue el 25/06/2020 16:05:43 y la fecha de rechazo automático el 06/07/2020 00:00:00. El rechazo automático se produce, de forma general, tras haber transcurrido diez días naturales desde su puesta a disposición para su acceso según el párrafo 2, artículo 43, de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Posteriormente, se notificó por el servicio de correos el 16/07/2020, siendo devuelta el día 28 del mismo mes y año.

El artículo 43 de la Ley 39/2015, en su apartado 3, establece: *“se entenderá cumplida la obligación a la que se refiere el artículo 40.4 con la puesta a disposición de la notificación en la sede electrónica de la Administración u Organismo actuante o en la dirección electrónica habilitada única”*.

Por tanto, se considera que no se puede tomar en consideración la existencia de “un vicio radical de nulidad del presente procedimiento”, tal y como defiende la entidad reclamada.

De esta forma, queda totalmente acreditado que no se ha producido indefensión.

III

El RGPD establece en el artículo 5 los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *“integridad y confidencialidad”*.

El artículo señala que:

*“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»).

A su vez, la seguridad de los datos personales viene regulado en el artículo 32 del RGPD.

El artículo 32 del RGPD “Seguridad del tratamiento”, establece que:

“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”.

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

“4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del

volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

(...)"

Por su parte, la LOPDGDD en su artículo 71, *Infracciones*, señala 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".*

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves"*:

"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:

(...)

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".

IV

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen 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"*.

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse una brecha de seguridad en sus sistemas al remitirse copia de la reclamación de cantidad de un tercero, al reclamante, al que informa de la deuda contraída por el tercero.

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”.

V

De conformidad con las evidencias de las que se dispone y de la documentación aportada se desprende que el reclamante solicitó copia del certificado emitido por el secretario-administrador de su intercomunidad de propietarios de reclamación de deuda de un copropietario deudor, pero en lugar de enviar el correcto, remitieron copia de un certificado perteneciente a un tercero, vulnerando el deber de confidencialidad, lo cual constituye, por parte de la reclamada, dos infracciones, una contra lo dispuesto en el artículo 32 del RGPD y otra contra lo dispuesto en el artículo 5.1 f) del RGPD, que rige los principios de integridad y confidencialidad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento.

VI

El artículo 58.2 del RGPD dispone lo siguiente: “Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

d) 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;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

VII

El artículo 72.1.a) de la LOPDGDD señala que *“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.*

Esta infracción puede ser sancionada con multa de 20 000 000 € 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, de acuerdo con el artículo 83.5 del RGPD.

A tenor de lo dispuesto por el RGPD en su artículo 83.2, al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrán en cuenta los factores agravantes y atenuantes que se relacionan en el artículo señalado, así como cualquier otro que pueda resultar aplicable a las circunstancias del caso.

En consecuencia, se han tenido en cuenta como agravantes:

- En el presente caso estamos ante acción negligente grave (artículo 83.2 b).
- Se encuentran afectados identificadores personales básicos (nombre, apellidos, domicilio), según el artículo 83.2 g).

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos **RESUELVE**:

PRIMERO: IMPONER a ASESORÍA MUNIZ SOLÁN, S.L., con NIF B21451364, por las siguientes infracciones:

- por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 a) del RGPD la sanción sería de apercibimiento requiriéndose a la parte reclamada que proceda, en el plazo de un mes, a adoptar las medidas necesarias para que cese la conducta objeto de esta reclamación, que ha causado la brecha de seguridad denunciada, para que se corrijan los efectos de la infracción cometida y su adecuación a las exigencias contempladas en el artículo 32 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.
- por la infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 a) del RGPD la sanción sería una multa por un importe de 2.000 euros (dos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a ASESORÍA MUNIZ SOLÁN, S.L..

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el

art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

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

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

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

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-131120

Mar España Martí

Directora de la Agencia Española de Protección de Datos