

- **Procedimiento N°: PS/00428/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Dña. **A.A.A.** (en adelante, la reclamante) con fecha 22 de julio de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra la Asociación Cámara de la Propiedad Urbana de Burgos y Provincia con NIF G09460338 (en lo sucesivo, la reclamada).

La reclamante manifiesta que sus familiares han recibido llamadas telefónicas requiriéndoles el pago de una deuda suya. Habiendo la reclamada, obtenido y tratado sin consentimiento esos datos.

Añade, que más tarde la parte reclamada remitió a un familiar un documento sobre la citada deuda, y por consiguiente vulnero el deber de confidencialidad.

Y, aporta la siguiente documentación:

WhatsApp de requerimiento enviado al padre de la reclamante.

Listado de llamadas realizadas desde la centralita de la reclamada al padre de la reclamante.

Demostración del número de teléfono perteneciente a la Cámara.

Aviso al padre de la reclamante que se puso en contacto con el vía telefónica y WhatsApp.

Demostración escrita de la llamada de la Cámara a la tía de la reclamante.

SEGUNDO: Se trasladó a la parte reclamada la presente reclamación el 18 de septiembre 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.

Pues bien, el 20 de octubre de este año, la reclamada realizó las siguientes manifestaciones: *“que ante la situación de impago del arrendamiento, el propietario encargó a la reclamada la gestión de la deuda motivo por el cual se pusieron en contacto con los dos arrendatarios, uno de ellos la reclamante, con los que llegaron a un acuerdo de pago el cual fue incumplido.*

Posteriormente, uno de los arrendatarios manifestó que les iban a prestar el dinero para pagar la deuda y facilitó el teléfono de un tercero. Efectuaron llamada a ese

teléfono facilitando otro número de teléfono que resultó ser el del padre de uno de los arrendatarios, con quién contactó la parte reclamada y a petición suya le enviaron información sobre la citada deuda.

Ante la reclamación formulada por los arrendatarios contactaron con los mismos y les informaron de lo anteriormente referido.

Asimismo, la reclamada declara que ha acordado revisar el procedimiento de actuación en relación con los datos personales de los arrendatarios y han redactado un modelo de uso para estos casos (datos no aportados directamente por los interesados) para la mejor salvaguarda de los derechos de los interesados, su intimidad y privacidad, y el cumplimiento del deber de información”.

TERCERO: Con fecha 23 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.

CUARTO: Notificado el citado acuerdo de inicio, la reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba: *“que los hechos tienen su origen en la deuda que, en concepto de alquileres y suministros, mantenía la reclamante con el propietario de la vivienda que venía ocupando, cuya reclamación y gestión fue encomendada por la propiedad a LA CAMARA. Hecho acreditado.*

Es importante aclarar que LA CAMARA, entre otros, presta el servicio de administración y gestión integral de arrendamientos: contratación, mantenimiento, desarrollo, cumplimiento y control de la relación contractual con el arrendatario.

La CAMARA se limitó a dar cumplimiento al encargo recibido de la propiedad, conforme a la información recibida, en aras a evitar mayores perjuicios que se les causarían a la reclamante y su pareja derivados del posible corte del suministro eléctrico. Su intención no fue la de comunicar datos a terceros o causar perjuicio a la reclamante.

Por otra parte, en relación a la protección de los datos desde el diseño y por defecto, LA CAMARA contrato los servicios del despacho de abogados LIFE Abogados, implementando las medidas técnicas y organizativas que se consideraron razonables acordes con el riesgo. Se adoptaron medidas de seguridad encaminadas a salvaguardar la confidencialidad de la información, firmándose los correspondientes documentos de confidencialidad con los empleados y usuarios de los sistemas de LA CAMARA, se les instruyó y entregó instrucciones relativas a sus funciones y obligaciones para la seguridad de los datos, y el documento con la política de uso de las herramientas puestas a disposición de los usuarios, que firmaron todos los empleados.

Conforme al principio de responsabilidad proactiva, tras hacer un mapa de datos y análisis de riesgos, se diseñó la estructura técnica y organizativa de LA CAMARA y medidas razonables acordes al riesgo a fin de restringir el acceso a los datos a

personas no autorizadas (control de usuarios) y que los datos no sean accesibles a un número indeterminado de personas sin la intervención humana y garantizar su seguridad física.

Particularmente, en la gestión de Arrendamientos y tratamiento de los datos personales asociados a los contratos de alquiler, LA CAMARA utiliza el programa informático denominado GESFINCAS, al que acceden solo el personal autorizado. Para ello existe un control de acceso tanto a los equipos como a los recursos compartidos. Los usuarios de LA CAMARA solamente tienen acceso a los recursos y datos que precisan para el desarrollo de sus funciones, control que permite la propia aplicación GESFINCAS.

Como prueba de todo lo anterior, adjuntamos documentos 3 y 4 (documento de confidencialidad al que se une la política de seguridad en el tratamiento de datos personales y política en el uso de las herramientas puestas a disposición de los usuarios. Documento 5, estructura técnica y organizativa de LA CAMARA en el almacenamiento y tratamiento de la información. Como documento 6, informe de responsabilidad proactiva de LA CAMARA (resultado de la adecuación que realizó LA CAMARA a la nueva regulación sobre protección de datos, RGPD).

Por ello, solicitamos el sobreseimiento del presente procedimiento sancionador y archivo de las actuaciones o subsidiariamente, se declara la comisión de una infracción del art. 5.1 f) RGPD tipificada en el art. 83. 5 a) del RGPD, y al amparo del art. 58.2b RGPD se imponga la sanción de apercibimiento. Subsidiariamente a lo anterior, de mantenerse la comisión de dos infracciones, mostramos nuestra conformidad a la sanción de apercibimiento, considerando que, con anterioridad a la incoación de este procedimiento, esta Asociación ya adoptó medidas organizativas complementarias tendentes a corregir los hechos objeto de denuncia y evitar que se repitan en el futuro”.

QUINTO: Con fecha 18 enero de 2021, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas E/07100/2020, así como los documentos aportados por la reclamada.

SEXTO: El 8 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 la Asociación Cámara de la Propiedad Urbana de Burgos y Provincia, con NIF G09460338, 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.
- por la infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 a) del RGPD la sanción que correspondería sería de apercibimiento.

Notificada la propuesta de resolución, la reclamada no ha formulado alegaciones a la misma.

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

HECHOS PROBADOS

PRIMERO: Consta acreditado que la reclamada remitió copia de la reclamación de cantidad de la reclamante a un tercero, al que informó de la deuda contraída por ella.

SEGUNDO: Consta WhatsApp de requerimiento enviado al padre de la reclamante.

Consta listado de llamadas realizadas desde la centralita de la reclamada al padre de la reclamante.

Consta demostración escrita de la llamada de la Cámara a la tía de la reclamante.

TERCERO: La reclamada, ha aportado en el presente procedimiento sancionador las medias que ha adoptado, entre las mismas consta:

Acuerdo de confidencialidad y secreto profesional.

Política en el uso de las Herramientas tecnológicas puestas a disposición de los usuarios.

Política de seguridad del personal para el tratamiento de datos personales funciones y obligaciones de los usuarios.

Informe de responsabilidad proactiva.

Deberes del Teletrabajador en materia de protección de datos.

Consentimiento para utilizar dispositivos personales para el teletrabajo.

Estructura técnica organizativa. Ficheros. Organización. Recursos. Personal. Empresas externas que tratan los datos.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

Se imputa a la reclamada la comisión de una infracción por vulneración de los artículos 5.1 f) y 32 del RGPD.

En el artículo 5 se establecen 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”.

III

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 la reclamada 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 la reclamante a un tercero, al que informa de la deuda contraída por la reclamante.

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”.

IV

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.

No obstante, 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;
(...)”

Por tanto, el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 58.2 b) la posibilidad de acudir al apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones.

De conformidad con las evidencias de las que se dispone, de la documentación aportada se desprende que la parte reclamada remitió copia de la reclamación de cantidad de la reclamante a un tercero, al que informa de la deuda contraída por la reclamante, vulnerando el deber de confidencialidad, lo cual constituye, por parte de la reclamada, de 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.

Estas infracciones podrían ser sancionadas con apercibimiento. De acuerdo con el artículo 58.2.b) del RGPD, y al considerar que las multas administrativas que pudieran recaer con arreglo a lo dispuesto en el artículo 83.5.b) del RGPD constituiría una carga desproporcionada para la reclamada.

En este caso concreto, se ha acreditado en virtud de los documentos aportados con sus alegaciones al acuerdo de inicio que la reclamada ha adoptado una serie de medidas adecuadas para garantizar la seguridad y confidencialidad de los datos.

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 la Asociación Cámara de la Propiedad Urbana de Burgos y Provincia, con NIF G09460338, 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, las sanciones serían de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a la Asociación Cámara de la Propiedad Urbana de Burgos y Provincia.

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