- **Expediente N.º: PS/00285/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 11 de diciembre de 2020, tuvo entrada en la Agencia Española de Protección de Datos (AEPD), escrito de reclamación presentado por D. ***A.A.A.***, en el que manifiesta su disconformidad con la recepción de un mensaje electrónico remitido por la entidad EXIPAGO, S.L., en el que se le exigía el pago de una deuda de la que es acreedora la entidad ******ENTIDAD.1.*** Según manifestaba, el mensaje fue enviado a 88 destinatarios sin ocultar las direcciones de estos, que de este modo habrían tenido acceso a la dirección de correo electrónico de los otros destinatarios, así como a su presunta condición de morosos. Junto a la reclamación no se aportaba copia del mensaje recibido.

SEGUNDO: En fecha 21 de enero de 2021, tras analizarse la documentación que obraba en el expediente, se dicta resolución por la Directora de la AEPD, por la que se acuerda inadmitir la reclamación, al no apreciarse indicios racionales de la existencia de una infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

TERCERO: Contra la mencionada resolución, en fecha 21 de febrero de 2021, el reclamante interpuso recurso de reposición, aportando copia del mensaje referido en la reclamación.

CUARTO: En fecha 22 de marzo de 2021, la Directora de la Agencia Española de Protección de Datos resolvió estimar el recurso de reposición interpuesto.

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

"Primera. - Detalle de las causas que han motivado la incidencia que ha originado la reclamación.

(...).

Segunda. - Descripción detallada del procedimiento seguido para la remisión de este tipo de comunicaciones con los deudores.

(…).

Tercera. - Posible sucesión de otros incidentes similares.

(…).

Cuarta. - Acciones tomadas con objeto de minimizar los efectos adversos de este incidente y sobre las medidas adoptadas para su resolución final.

(…).

Quinta. - Información sobre la notificación de la brecha de seguridad a los afectados.

(…).

Sexta. - Medidas técnicas y organizativas adoptadas.

(…).

Séptima. - Contrato de prestación de servicios suscrito con el responsable del tratamiento.

(…).

Octava. - Comunicación de la brecha al responsable del tratamiento.

(…).

SEXTO: En fecha 1 de septiembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 y 83.4 del RGPD, respectivamente.

SÉPTIMO: Notificado el acuerdo de inicio, el reclamado presentó escrito de alegaciones en el que, en síntesis, manifestaba que la causa que motivó la incidencia fue un error humano en el envío de una comunicación electrónica, que la metodología para la remisión de comunicaciones electrónicas a los deudores se basa en la necesidad de poner en copia oculta (CCO) a todos los destinatarios, que los empleados en el momento de su incorporación a la compañía y con anterioridad al desempeño de sus funciones reciben formación en este sentido, que se procedió de inmediato a notificar la brecha de seguridad al responsable del tratamiento, que dicho empleado fue amonestado, que se han tomado medidas preventivas para evitar este tipo de incidentes en el futuro y solicita que se proponga sanción de apercibimiento.

OCTAVO: En fecha 3 de diciembre de 2021 se formuló propuesta de resolución, proponiendo:

<<Que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento a EXIPAGO, S.L., con CIF B65984262, por una infracción del artículo

5.1. f) del RGPD, conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 i) de la LOPDGDD y por una infracción del artículo 32 del RGPD, conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción en el artículo 73 apartado f) de la LOPDGDD >>

NOVENO: En fecha 10 de diciembre de 2021, la parte reclamada presenta escrito en el que, en síntesis, manifiesta que está conforme con la citada Propuesta de Resolución.

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

PRIMERO: En fecha 11 de diciembre de 2020, la parte reclamante interpuso escrito reclamación ante la Agencia Española de Protección de Datos (AEPD), en el que manifestaba su disconformidad con la recepción de un correo electrónico remitido por la entidad reclamada, en el que se le exigía el pago de una deuda. El mensaje fue enviado a 88 destinatarios sin ocultar sus direcciones, teniendo acceso a la dirección de correo electrónico de los otros destinatarios, así como a su presunta condición de morosos.

SEGUNDO: Comprobada la documentación aportada y que se encuentra incorporada al expediente, consta que en fecha 11 de diciembre de 2020, a las 14:56 horas, el reclamante recibió correo electrónico desde la dirección***: ***EMAIL.1***, en nombre de EXIPAGO, S.L., sin copia oculta, junto con otras 88 direcciones de correo electrónico, entre las que se hallaba la dirección del reclamante y a través del cual se reclamaba una deuda que debía ser pagada o se emprenderían las oportunas acciones judiciales.

TERCERO: La parte reclamada reconoce que el incidente objeto de la reclamación fue debido a un error humano y expone que ha procedido a implantar las medidas correctoras adecuadas para evitar la repetición de hechos similares en el futuro.

FUNDAMENTOS DE DERECHO

PRIMERO: 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 y 48.1 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*."

SEGUNDO: Los hechos probados en el procedimiento evidencian la divulgación de las direcciones de correo electrónico al ser remitido al reclamante un correo electrónico sin copia oculta con quebrantamiento de las medidas técnicas y organizativas y vulnerando la confidencialidad de los datos.

En el presente caso, se imputa al reclamado la infracción del artículo 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD.

TERCERO: El artículo 5 del RGPD, *Principios relativos al tratamiento*, que establece 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»).

(…)"

El artículo 5, *Deber de confidencialidad*, de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en lo sucesivo LOPDGDD), señala que:

"1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, en relación con el artículo 5 de la LOPGDD, *deber de confidencialidad*, al revelar a terceros, datos de carácter personal, al remitir sin copia oculta una reclamación de deuda.

Este deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de estos.

Por tanto, ese deber de confidencialidad es una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional.

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

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

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

QUINTO: Establece el artículo 4.12 del RGPD que se considera "*violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione 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, al remitirse un correo electrónico sin copia oculta a 88 destinatarios, entre ellos el reclamante, en el que se reclamaba una deuda, revelando información y datos de carácter personal a terceros.

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".

SEXTO: La infracción se tipifica en el artículo 83.5 del RGPD, que dispone lo siguiente:

"5. 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;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" determina lo siguiente: "*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 de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente: *"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:*

(…)

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica."

La vulneración del artículo 32 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."

(…)

A efectos del plazo de prescripción de las infracciones, el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves",* establece lo siguiente:

"*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una*

vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD.

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

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

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

OCTAVO: Sin perjuicio de lo establecido en el artículo 83.5 apartados a) y b) del RGPD, en su art. 58.2 b) dispone la posibilidad de dirigir un apercibimiento, en relación con lo señalado en el Considerando 148:

"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante."

En el presente caso, atendiendo a la diligencia llevada a cabo por la entidad reclamada en lo referente a informar a esta Agencia de las circunstancias en las que se produjo el incidente que propició la reclamación, así como las medidas a adoptar a fin de evitar que hechos como el reclamado vuelvan a producirse en el futuro, considerando que la respuesta ha sido razonable, reconociendo los hechos y, no teniéndose constancia de otras reclamaciones por parte de las personas afectadas, permite considerar una disminución de la culpa en los hechos, por lo que se considera conforme a Derecho, no imponer sanción consistente en multa administrativa y sustituirla por un apercibimiento, de conformidad con el artículo 76.3 de la LOPDGDD, en relación con el articulo 58.2 b) del RGPD que señala lo siguiente*:*

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

"b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento."

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: DIRIGIR a EXIPAGO, S.L., con CIF B65984262, por una infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 y 83.4 del RGPD, respectivamente, un apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a EXIPAGO, S.L.

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.

938-270122

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