- **Procedimiento Nº: PS/00328/2021**

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 11 de marzo de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra Dña. ***B.B.B., con NIF ***NIF.1*** (PISAMUNDO ZARAGOZA) (en lo sucesivo, la reclamada).

El reclamante manifiesta que el 30 de enero de 2020 recibió un correo electrónico sin copia oculta revelando las direcciones de correo electrónico de los demás destinatarios.

Y, aporta la siguiente documentación:

- Correo electrónico donde aparecen cuatro destinatarios sin ocultar.

SEGUNDO: Con carácter previo a la admisión a trámite de esta reclamación, se trasladó al reclamado el día 1 de junio de 2020, de conformidad con lo establecido en el artículo 65.4 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD), en las actuaciones con referencia E/03555/2020. La notificación se realiza electrónicamente, y figura devuelta a origen por no ser retirado el envío de la oficina postal el 18 de junio de 2020.

Posteriormente, se reiteró el día 23 del mismo mes y año, con el mismo resultado, con fecha 9 de julio de 2020.

TERCERO: De conformidad con lo dispuesto en el artículo 65.2 de la Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), en fecha 29 de septiembre de 2020 se firma el acuerdo de admisión a trámite de la reclamación.

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 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

1. En la página web del sitio web www.pisamundo.com, indican como responsable del sitio a Donosti Receptivo, S.L. Según informe de la base de datos de Axesor, esta entidad pertenece a la mercantil Departamento Infraestructuras Turísticas, S.L. (en adelante, Dit Gestión).

2. Realizada solicitud de información a Dit Gestión para que aclarase la relación de esta mercantil con la agencia de viajes reclamada. Con fecha de 26 de octubre de 2020 se recibe en esta Agencia, escrito de alegaciones poniendo de manifiesto que PISAMUNDO ZARAGOZA es un nombre comercial que pertenece a Dña. ***B.B.B.*** según consta en la base de datos de la Oficina Española de Patentes y Marcas.

Añaden que su mercantil no tiene ninguna vinculación con dicho signo distintivo y en consecuencia, no tienen ni han tenido ninguna relación contractual con su legítima propietaria, entendiendo en consecuencia que si alguien es responsable del tratamiento de datos personales correspondiente a dicho nombre comercial será la propietaria del mismo. Aclaran que Dit Gestión si es propietaria del nombre comercial "PISAMUNDO", único nombre comercial cedido en uso a Dña. ***B.B.B.*** mediante el contrato de prestación de servicios.

Adjuntan los siguientes documentos:

- Contrato de prestación de servicio. En este contrato se cede la utilización del nombre comercial "PISAMUNDO" bajo determinadas condiciones mercantiles en el que se reconoce a la agencia de Dña. ***B.B.B.*** como interesada en la venta de servicios de viajes como agente independiente en Zaragoza.
- Acuerdo para la regulación del tratamiento de datos personales. En este acuerdo DIT Gestión ostenta la condición de encargado del tratamiento de los datos de carácter personal necesarios para prestar los servicios descritos en el contrato de colaboración formalizado entre Dit Gestión y Dña. ***B.B.B.***.

3. Realizada solicitud de información sobre la entidad responsable de la agencia de viajes "PISAMUNDO ZARAGOZA" a Dña. ***B.B.B.***, se notifica con fecha de 3 de febrero de 2021.

La reclamada no ha respondido al requerimiento informativo que se envió.

QUINTO: Con fecha 19 de julio de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por las presuntas infracciones de los artículos 5.1f) y 32 del RGPD, tipificadas en los artículos 83.5 a) y 83.4 a) del RGPD respectivamente. Dicho acuerdo fue notificado a través del operador público postal y el tablón edictal único del BOE el 29 de julio y el 9 de agosto de 2021, a la parte reclamada.

SEXTO: Notificado formalmente el acuerdo de inicio, la parte reclamada al tiempo de la presente resolución no ha presentado escrito de alegaciones, por lo que es de aplicación lo señalado en el artículo 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que en su apartado f) establece que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, por lo que se procede a dictar 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: Con fecha 11 de marzo de 2020, la parte reclamante manifiesta que el 30 de enero de 2020 recibió un correo electrónico sin copia oculta revelando las direcciones de correo electrónico de los demás destinatarios.

SEGUNDO: La parte reclamante aporta copia del correo electrónico donde aparecen cuatro destinatarios sin ocultar.

TERCERO: En la base pública de datos de la Oficina Española de Patentes y Marcas, consta que PISAMUNDO Zaragoza, es un nombre comercial que pertenece a Dña. ***B.B.B.***, con fecha de presentación el 11 de agosto de 2016 y estando en vigor.

CUARTO: El emisor del correo electrónico es info.pisamundozaragoza.com, nombre comercial de la entidad y cuya titular responsable es Dña. ***B.B.B..***

QUINTO: El 19 de julio de 2021 se inició este procedimiento sancionador por la presunta infracción del artículo 6 del RGPD, siendo notificado el 9 de agosto de 2021. No habiendo efectuado alegaciones, la parte reclamada, al acuerdo de inicio.

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 arts. 47 y 48.1 de la LOPDPGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

Se imputa a la parte reclamada la comisión de dos infracciones por vulneración de los artículos 5.1 f) y 32 del RGPD.

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".

III

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, 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 enviar un correo electrónico sin copia oculta a cuatro destinatarios, reclamante incluido.

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) dirigir 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 y de la documentación aportada se desprende que de los hechos denunciados, es decir, remitir un correo electrónico sin copia oculta, enviado a otros destinatarios, supone la vulneración del 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, lo cual constituye, por parte del reclamado, 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 son 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 los dispuesto en el artículo 83.5.b) del RGPD constituiría una carga desproporcionada para la reclamada.

Asimismo, a los efectos previstos en el artículo 58.2 del RGPD la medida correctiva que se impone a la parte reclamada consiste en requerirle que tome medidas de seguridad adecuadas para que cuando envíe correos a diferentes destinatarios se utilice la opción de envío con copia oculta para evitar ceder información con datos personales a todos los destinatarios.

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 Dña. ***B.B.B., con NIF ***NIF.1*** (PISAMUNDO ZARAGOZA), dos apercibimientos:

- por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 a) del RGPD un apercibimiento.

- por la infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 a) del RGPD un apercibimiento.

SEGUNDO: REQUERIR a Dña. ***B.B.B., con NIF ***NIF.1*** (PISAMUNDO ZARAGOZA), para que en el plazo de un mes desde la notificación de esta resolución, acredite:

- Las medidas de seguridad adoptadas para evitar que cuando se envíen correos a diferentes destinatarios se utilice la opción de envío con copia oculta para evitar ceder información de datos personales a todos los destinatarios del correo.

TERCERO: NOTIFICAR la presente resolución a Dña. ***B.B.B.***, con ***NIF ***NIF.1*** (PISAMUNDO ZARAGOZA).

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.

938-300320

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