- **Expediente N.º: EXP202302073**

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

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

ANTECEDENTES

PRIMERO: ***A.A.A.***, ***B.B.B.*** *y* ***C.C.C.*** (en adelante, las partes reclamantes) presentaron respectivamente con fechas 5, 6 y 10 de enero de 2023, sendos escritos de reclamación ante la Agencia Española de Protección de Datos. Las reclamaciones se dirigían contra ***D.D.D.*** con NIF ******NIF.1*** (en adelante, la parte reclamada).

Dichos reclamantes manifestaban en sus escritos la recepción de un correo electrónico en fecha 4 de enero de 2023, desde la dirección ******EMAIL.1***, constando como destinatarios una pluralidad de direcciones de correo electrónico, entre las cuales se incluían las de los propios reclamantes y en el que se podían visualizar las direcciones de correo electrónicos del resto de los destinatarios a los que iba dirigido. Afirman que las mencionadas direcciones de correo electrónico aparecen visibles debido a que no se ha utilizado la funcionalidad CCO en el citado correo electrónico que permite ocultar los destinatarios.

Junto a dichas reclamaciones destaca la aportación de la copia del mencionado correo electrónico de fecha 4 de enero de 2023, donde constan como destinatarios unas 151 direcciones de correo electrónico, incluidas las direcciones de correo electrónico de los reclamantes, con el asunto "COMUNICADO REEMPLAZO ESPECTÁCULO SHEA COULEÉ BARCELONA" y remitido desde la dirección ******EMAIL.1.***

SEGUNDO: Con fecha 17 de febrero de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

TERCERO: 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:

- Teniendo en cuenta el remitente del correo electrónico objeto de las reclamaciones, se procede a consultar la titularidad del dominio (...)**,** extrayéndose que el mismo fue registrado en IONOS CLOUD S.L.U., en fecha 28 de enero de 2020, y que se encuentra asociado a un servicio de Alojamiento web denominado "MyWebsite Creator", por el cliente de IONOS cuyos datos corresponden a la parte reclamada ***D.D.D. con NIF ***NIF.1*** *con domicilio en* ******DIRECCIÓN.1.***

- En virtud de tal información, en fecha 4/5/2023 se solicitó por la Inspección de Datos a la parte reclamada información y documentación en relación con los hechos expuestos en la reclamación, respondiendo ésta a través de escrito presentado en fecha 16/5/2023, del cual destaca lo siguiente:
  - Que, en su condición de trabajadora autónoma, realiza la actividad de organización y gestión de eventos, bajo la marca (…).
  - Afirma, que en el marco de su actividad colaboró en la organización en un evento que debía celebrarse en el año 2020, el cual, por las medidas adoptadas en virtud del Covid-19, tuvo que posponerse. Al establecerse posteriormente nueva fecha para el evento aplazado, resultó necesario comunicar la misma a todos los clientes que habían comprado previamente sus entradas. Para ello, el organizador principal del evento, WEEZEVENT SAS, le solicitó que enviara la comunicación a los clientes dado que, por problemas técnicos, no podía remitirlas.
  - Con fecha 4/1/2023 procedió a remitir dos correos electrónicos a los citados clientes con las direcciones de correo ocultas, cuyas copias aporta, para comunicarles la nueva fecha del evento; uno remitido desde la dirección ***(…)*** y otro desde la dirección ******EMAIL.1***. Este segundo correo se remitió con el objetivo de que los clientes tuvieran una dirección de correo a la que contestar o solicitar información adicional. Afirma que, sin embargo, el correo remitido desde ******EMAIL.1***, reportó error, al indicar que el correo no había podido ser entregado a los destinatarios, de lo cual aporta copia a efectos acreditativos.
  - Tras dichas circunstancias, manifiesta que preparó un tercer email desde ******EMAIL.1***, el cual es objeto de las reclamaciones presentadas, y el que, por error, debido a la preocupación de que los clientes finalmente pudieran recibir la información, colocó las direcciones en el área “CC” en lugar de “CCO”, lo que permitió visualizar el correo del resto de los destinatarios.
  - Expone que, horas más tarde, del envío del correo, recibió respuesta de tres clientes informando del error cometido advirtiendo que se había enviado el correo en copia visible. Detectado dicho hecho, contestó de manera individual a los clientes que le habían notificado el error, ofreciendo sus disculpas individuales a cada uno, aportando copia de dos de estos correos como acreditación de dicho hecho. Asimismo, posteriormente preparó y remitió un correo, cuya copia también aporta, colocando esta vez las direcciones en copia oculta a todos los destinatarios, solicitando disculpas a todos ellos y lamentando el error cometido.
  - Manifiesta que los hechos tuvieron lugar como consecuencia de un error humano, cometido de forma involuntaria, añadiendo que no forma parte de su actividad realizar este tipo de comunicaciones masivas, siendo, de hecho, la primera vez que lo realizaba.
  - Por su parte, afirma que no tiene conocimiento de la utilización por terceros de los datos personales obtenidos, consistentes en las direcciones de correo electrónicos.
  - Respecto a la seguridad de los tratamientos de datos de carácter personal, aporta copia del análisis de riesgos de fecha 15/9/2022, que incluye el tratamiento objeto de reclamación, en el que se previó el riesgo del envío de

comunicaciones masivas, valorándose la amenaza inherente al envío de comunicaciones a varios destinatarios. Se determinó en el análisis que, dado que esta actividad no se realizaba, el riesgo inicial fue bajo. En las medidas se recoge la obligación del uso de copia oculta, y la de contratar en su caso una herramienta de mail-marketing que mitigara riesgo de errores si esta actividad debía repetirse o pudiera considerarse habitual.

- Respecto a las medidas adoptadas para evitar que se repita el incidente acredita la contratación de una herramienta mailmarketing para el envío de comunicaciones para en el caso de que su actividad se viera forzada a realizar con urgencia una comunicación similar, pudiendo garantizar así el envío en copia oculta.

QUINTO: Con fecha 15 de septiembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de apercibimiento a la parte reclamada, por la presunta infracción de los artículos 5.1.f) y 32 del RGPD, tipificados en los artículos 83.5 y 83.4 del RGPD, respectivamente. En dicho acuerdo se le otorgaba un plazo de diez días hábiles para que formulase las alegaciones y presentase las pruebas que considerase convenientes.

SEXTO: La notificación del citado acuerdo de iniciación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), tuvo lugar de forma electrónica en fecha 15/09/2023, tal y como consta en el acuse de recibo que obra en el expediente.

SÉPTIMO: En fecha 26/09/2023 se recibió por esta autoridad escrito de la parte reclamada a través del cual manifestaba su conformidad con lo expuesto por la AEPD, así como su compromiso de cumplir con las medidas de seguridad ya implantadas, así como adoptar todas aquellas medidas técnicas y organizativas apropiadas para garantizar un tratamiento no autorizado.

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: De la instrucción del presente procedimiento, así como de las actuaciones de investigación y de los documentos que obran en el mismo resulta acreditado la remisión de un correo electrónico en fecha 4 de enero de 2023, desde la dirección ******EMAIL.1***, dirección que iba destinado a una pluralidad de destinatarios, entre los cuales se encontraban las partes reclamantes y en el cual se podían visualizar las direcciones de correo electrónicos del resto de los destinatarios a las que iba dirigido. Las direcciones de correo electrónico aparecen visibles debido a que no se hizo uso la funcionalidad CCO en el citado correo electrónico, la cual permite ocultar a cada uno de ellos el resto de los destinatarios.

TERCERO: Asimismo, resulta acreditado que la mencionada dirección ******EMAIL.1*** a través de la cual se remitió el correo objeto del presente procedimiento, se encuentra

vinculada al dominio ***(...)***, cuya titularidad corresponde a la parte reclamada, a través de un servicio de alojamiento web.

SEGUNDO: Tales hechos han sido confirmados además por la parte reclamada, la cual ha afirmado durante la instrucción del presente procedimiento que los mismos tuvieron lugar debido a un error humano, de carácter involuntario.

CUARTO: Durante las actuaciones de investigación, la parte reclamada ha afirmado haber tomado medidas con el fin de evitar que los mencionados hechos se reiteren. De forma concreta, se acredita la contratación de una herramienta *mailmarketing* que tiene como objeto el envío de comunicaciones y que permite garantizar el envío en copia oculta.

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 y 64.3 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
Obligaciones incumplidas

El artículo 5 del RGPD establece los principios relativos al tratamiento, indicando, entre otras cuestiones, que 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»)."

De la misma forma, el artículo 32 del RGPD se refiere de forma expresa a la seguridad del tratamiento:

"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."

En el presente supuesto, ha quedado acreditado que la parte reclamada remitió un correo electrónico con una pluralidad de destinatarios sin ocultar las direcciones de estos, lo que permitió que se pudiera visualizar las del resto, lo cual conlleva la vulneración del principio de confidencialidad previsto en el mencionado artículo 5.1 f) RGPD respecto al tratamiento de los datos personales.

En este sentido, para garantizar dicho principio, la parte reclamada debió de adoptar las pertinentes previas medidas técnicas u organizativas, de todo tipo, que garantizasen un adecuado tratamiento y evitase un tratamiento no autorizado o ilícito.

Por otro lado, la parte reclamada, como responsable del tratamiento de dichos datos, debió de haber adoptado medidas técnicas y organizativas que garantizasen un nivel de seguridad adecuado al riesgo y que, sin embargo, no se realizaron. La ausencia de medidas para garantizar el nivel de seguridad manifiesta el incumplimiento de la previsión del artículo 32 RGPD, puesto que el número considerable de destinatarios a los que iba destinado el correo suponía la existencia un riesgo que implicaba la adopción de medidas adecuadas con el fin de evitar una brecha de datos personales, como ocurrió en el presente caso.

III

Tipificación y calificación de las infracciones

Por un lado, el incumplimiento del principio de confidencialidad previsto en el mencionado artículo 5.1.f) del RGPD es constitutivo de la infracción, imputable a la parte ***D.D.D.,*** prevista en el artículo 83.5 de la misma norma, el cual dispone expresamente:

"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 efectos del plazo de prescripción de las infracciones, dicha infracción prescribe a los tres años, conforme al artículo 72.1. a) de la LOPDGDD, que califica de muy grave la siguiente conducta:

"a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679."

Por otro lado, el incumplimiento de adoptar las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo previsto en el artículo 32 RGPD es constitutivo de la infracción prevista en el artículo 83.4, según el cual, *"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 imputada prescribe a los dos años, conforme al artículo 73 f) de la LOPDGDD, que califica de grave la siguiente conducta:

"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]"

IV
Apercibimiento

Sin perjuicio de lo dispuesto en el apartado artículo 83 del RGPD, el citado Reglamento dispone en el apartado 2.b) del artículo 58 "*Poderes*" 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 un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento; (…)"

Asimismo, el artículo 64 de la LOPDGDD que regula la "*Forma de iniciación del procedimiento y duración"*, en su apartado tercero dispone que:

"3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la

Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.
El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.
Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo."

En este caso, atendidas las circunstancias resultantes de la instrucción del presente procedimiento y siguiendo el criterio de las disposiciones indicadas, por los hechos objeto de las infracciones señaladas anteriormente, se estima por la presente autoridad proceder a dirigir un apercibimiento a la parte reclamada.

V
Adopción de medidas

Teniendo en cuenta que, tal y como se señala en los hechos probados, la parte reclamada ha acreditado la adopción de medidas técnicas y organizativas para evitar que se reiteren los hechos objeto del presente procedimiento, no se estima por la presente autoridad la imposición de nuevas medidas a la parte reclamada, sin perjuicio del mantenimiento por ésta de las ya adoptadas.

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 UN APERCIBIMIENTO a ***D.D.D.***, con NIF ******NIF.1***, por una infracción del artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, así como del artículo 32 RGPD, tipificado en el artículo 83.4 de la misma norma.

SEGUNDO: NOTIFICAR la presente resolución a ***D.D.D.***.

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.

1403-021023

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