- **Expediente N.º: EXP202309055**

Procedimiento Sancionador N.º PS/00497/2023

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES DE HECHO

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 15 de mayo de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige inicialmente contra ***B.B.B..***

El reclamante manifiesta que se inscribió para participar en una carrera popular organizada por el Ayuntamiento de San Cristóbal de La Laguna, y que con fecha de 20/04/23 recibió un correo desde la dirección de correo electrónico ***EMAIL.1, en cuyo pie de firma constaba el reclamado ***B.B.B.***, bajo el asunto "*Horario recogida dorsales XXII media maratón ciudad de La Laguna 2023*", que "*hizo públicos los correos electrónicos de todos los participantes/inscritos poniendo todos los correos electrónicos en copia en lugar de ponerlos en copia oculta, por lo que he recibido correo de otras personas participantes en la carrera, con lo que queda patente que mi correo electrónico ha sido publicado sin mi consentimiento y cualquiera de los inscritos en la carrera puede hacer uso del mismo. Al ponerme en contacto con él sólo se limitó a pedir disculpas."*

Junto a la notificación se aporta:

- Correo electrónico de 20/04/23 remitido a 493 destinatarios de correo electrónico que aparecen visibles, sobre el "*Horario recogida dorsales XXII media maratón ciudad de La Laguna 2023*", al que se refiere el reclamante.
- Correo electrónico de 23/04/23 en el que el reclamante responde al correo anterior, pidiendo explicaciones al respecto de porqué se ha publicado su correo electrónico.
- Correo electrónico de 24/04/23 contestando al anterior, en el que se piden disculpas, indicando que ha sido un gran error que hay que solucionar.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), y se dio traslado de dicha reclamación a la persona contra la que se dirige la reclamación, que aparece en el pie de firma de los correos electrónicos aportados por el reclamante, D. ***B.B.B.,*** para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, 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), fue recogido en fecha 31/08/2023, como consta en el

acuse de recibo que obra en el expediente, sin que se haya recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 15 de agosto de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante, lo que fue comunicado al mismo.

CUARTO: Con fecha de 8 de mayo de 2024, se expide diligencia para hacer constar y unir al presente procedimiento los siguientes documentos generados por la Subdirección de Inspección de Datos, obtenidos del sitio web del Organismo Autónomo de Deportes del Ayuntamiento de San Cristóbal de La Laguna, www.deportelagunero.com , adjuntados a esta diligencia como Anexo I, II, y III, teniendo por probado el contenido de los mismos a efectos de este expediente:

- Anexo I. Reglamento municipal aplicable a la XXII media maratón de la ciudad de La Laguna.
- Anexo II. Política de privacidad del sitio web.
- Anexo III. Anuncio convocatoria de la XXII media maratón de la ciudad de La Laguna.

En atención a lo anterior, y debido a que el correo electrónico por el que se presenta la reclamación viene referido a aspectos relacionado con el desarrollo práctico de la carrera, cuya organización corresponde al Ayuntamiento de San Cristóbal de La Laguna, dicha identidad, en su condición de responsable, queda identificada como parte reclamada.

QUINTO: Con fecha 13 de mayo de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al Ayuntamiento de San Cristóbal de La Laguna (en adelante, el AYUNTAMIENTO), como responsable del tratamiento de los datos personales de los participantes inscritos en la citada carrera, por la presunta comisión de las infracciones del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificadas en el Artículo 83.5.a) del RGPD y Artículo 83.4.c) del RGPD.

SEXTO: Notificado el citado acuerdo de inicio 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) y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso 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 PROBADOS

PRIMERO: De acuerdo con los correos electrónicos aportados por el reclamante, queda acreditado que con fecha de 20/04/23 se produjo una brecha de confidencialidad de datos personales al remitirse por cuenta del Ayuntamiento de San Cristóbal de La Laguna un correo electrónico que divulgó las direcciones de correo electrónico de 493 personas que proporcionaron sus datos personales al inscribirse en el evento deportivo XXII MEDIA MARATÓN CIUDAD DE LA LAGUNA organizado por el Organismo Autónomo de Deportes de San Cristóbal de La Laguna (en adelante, OAD), que iba a tener lugar el domingo 23 de abril de 2023 a las 09:00 horas.

El citado correo electrónico de 20/04/23 se remitió a 493 destinatarios, desde la dirección de correo electrónico ******EMAIL.1*** y con el pie de firma de ***B.B.B.***. Se observa que las direcciones de correo electrónico de estas 493 personas aparecen como destinatarios del correo, y no en copia oculta. El asunto del correo era informar del "Horario recogida dorsales XXII media maratón ciudad de La Laguna 2023" a los participantes inscritos en la misma, y tenía el siguiente contenido:

"Hola.

IMPORTANTE. Comunicamos los horarios de recogida de dorsales y bolsa del corredor de la XXII MEDIA MARATÓN CIUDAD DELA LAGUNA que tendrá lugar este domingo 23 de abril de 2023 a las 09:00.

Sábado 22 de Abril en la Plaza de la Catedral en horario de 11:00am hasta las 20:00.

Domingo 23 de Abril en la Plaza de la Catedral en horario de 07:00am a 08:00 am .

Rogamos que todo el que tenga fácil desplazarse a La Laguna para recoger su dorsal y bolsa lo haga el sábado para facilitar la recogida el domingo de los que vienen de más lejos.

Muchas gracias a tod@s".

SEGUNDO: El reclamante aporta, así mismo, dos correos electrónicos de 23 y 24 de abril de 2023, en los que queda acreditado que al pedir explicaciones sobre porqué se había publicado y dado a conocer ilícitamente su dirección de correo electrónico a los otros 492 destinatarios del correo, recibió respuesta de la dirección de correo ******EMAIL.1,*** en el que se le pedían disculpas por el error cometido.

TERCERO: Que el responsable del tratamiento de los datos personales de los participantes inscritos en la carrera que fueron desvelados ilícitamente en el mencionado correo electrónico era el Ayuntamiento de San Cristóbal de La Laguna, que a través de su Organismo Autónomo de Deportes, se encargaba de organizar la carrera, determinado los fines y medios del tratamiento de los datos personales de los participantes inscritos en la misma, lo que se ha acreditado mediante la expedición de Diligencia de *18 de mayo de 2024,* por la que se unen al presente procedimiento los siguientes documentos generados por la Subdirección de Inspección de Datos, obtenidos del sitio web del Organismo Autónomo de Deportes del Ayuntamiento de

San Cristóbal de La Laguna, www.deportelagunero.com, adjuntados la misma como Anexo I, II, y III, teniendo por probado el contenido de los mismos a efectos de este expediente:

- Anexo I. Reglamento municipal aplicable a la XXII media maratón de la ciudad de La Laguna.
- Anexo II. Política de privacidad del sitio web.
- Anexo III. Anuncio convocatoria de la XXII media maratón de la ciudad de La Laguna.

CUARTO: Consta acreditado que el Ayuntamiento no ha adoptado ni implementado las medidas técnicas y organizativas apropiadas para garantizar que los datos personales proporcionados por los participantes de la XXII media maratón de la ciudad de La Laguna dispongan de un nivel de seguridad adecuado frente a los riesgos de vulneración de la confidencialidad que concurren cuando su personal o encargados del tratamiento remitan comunicaciones electrónicas masivas o dirigidas a más de un destinatario, como pudiera ser la obligatoriedad de utilizar la funcionalidad de copia oculta para dirigir correos electrónicos a más de un destinatario, o cualquier otra medida que evite la divulgación no autorizada de los correos electrónicos a todos los participantes.

FUNDAMENTOS DE DERECHO

I
Competencia y Procedimiento

De acuerdo con y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 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."*

II
Cuestiones previas

La dirección de correo electrónico se considera un dato personal cuyo tratamiento se somete al régimen previsto en el RGPD, así como a sus disposiciones de desarrollo, de acuerdo con lo previsto en el artículo 4. 1, 2, y 7 el RGPD, que dispone lo siguiente:

"Artículo 4 Definiciones: A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda

persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;(…)

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (…)"

En el presente caso, de acuerdo con lo establecido en el artículo 4, apartados 1, 2 y 7 del RGPD, consta que el Ayuntamiento ha realizado, en su condición de responsable, un tratamiento de datos personales toda vez que ha difundido las direcciones de correo electrónico de 493 personas que las proporcionaron al inscribirse en el evento deportivo XXII MEDIA MARATÓN CIUDAD DE LA LAGUNA organizado por el Organismo Autónomo de Deportes de San Cristóbal de La Laguna (en adelante, OAD), que iba a tener lugar el domingo 23 de abril de 2023 a las 09:00 horas.

De acuerdo con el anuncio del portal web del OAD del Ayuntamiento deportelagunero.com, es el Ayuntamiento de San Cristóbal de La Laguna, a través del citado OAD, el que organiza la carrera, determinando los fines y medios del tratamiento de los datos personales de los participantes de la misma, de acuerdo con las siguientes evidencias que se deducen de sus publicaciones en relación con la referida carrera:

- En primer lugar, la web el OAD deportelagunero.com indica en su política de privacidad que tal ente municipal es el responsable de los datos personales de las personas que se inscriban en sus actos o eventos deportivos, indicando expresamente que: "El OAD *es responsable del tratamiento; sus datos serán tratados conforme dispone la normativa actual para posibilitarle el uso y navegación por esta web y tramitar las específicas solicitudes que nos formule en su ámbito."*

- En el portal web del referido OAD del Ayuntamiento, El XXII Medio Maratón Ciudad de La Laguna se celebrará el 23 de abril (deportelagunero.com) se reconoce que éste es el que organiza la carrera, y reglamenta todas sus

normas. Nótese cómo fija el periodo y forma de inscripción, precios, recorrido de la carrera, categorías y otras normas:

> *"Este miércoles 22 de marzo de 2023 y hasta el próximo 17 de abril, se abren las inscripciones para el XXII Medio Maratón Ciudad de La Laguna, prueba organizada por el Organismo Autónomo de Deportes, que tendrá lugar el venidero 23 de abril. Después de abrir boca con la Carrera Nocturna, esta cita atlética llega para ofrecer una distancia mayor a las y los fondistas. Más allá del recorrido de 21 kilómetros, también se ofertan plazas para 10 y 5, respectivamente. Las inscripciones, que cuentan con un cupo máximo de 1.400, se pueden formalizar a través de www.deportelagunero.com.*
> *Con salida en la Plaza de La Catedral, hasta la 'hermana menor' (5.000 metros) transitará por lugares tan emblemáticos como la Calle la Carrera, La Concepción, Herradores, Trinidad, Viana, Tabares de Cala, etcétera. Un 'track' deportivo que exhibe en todas sus distancias el encanto de una Ciudad Patrimonio de la Humanidad. El 10.000 'toca' lugares como la Avenida República Argentina y los alrededores de Vía de Ronda. Será el mismo recorrido para el Medio Maratón, que dará dos vueltas a ese circuito.*
> *En el reglamento, que se puede consultar en la página de inscripciones (www.deportelagunero.com), se contemplan categorías desde Sub18 a Máster 70, pasando por Diversidad Funcional, que ya se ha hecho un hueco importante en el listado de citas atléticas pasadas. Además, para las y los mejores de la general habrá premios en metálico; se repartirán 1.540 euros.*
> *En lo que respecta a las inscripciones, el precio irá en función de la distancia, resultando de 15, 12 y 10 euros para las de 21, 10 y 5 kilómetros, respectivamente. Además del dorsal, las y los corredoras y corredores contarán con una bolsa en la que dispondrán de camiseta, toalla y 'gymsack'."*

- El Reglamento de inscripción de la carrera publicado por el OAD de La Laguna regula con detalle todas las condiciones referidas a la misma, incluido el cómo se debe proceder a la entrega de dorsales, lo que también supone definir fines y medios del tratamiento de los datos personales a los efectos del artículo 4.7 del RGPD.

De acuerdo con el citado artículo 4.7 RGPD, lo relevante para determinar la responsabilidad por la remisión de este correo sin copia oculta y la falta de medidas que lo impidan, es determinar quién ha fijado los fines y medios del tratamiento. A la vista de estas evidencias, no cabe duda de que el Ayuntamiento, a través del OAD de La Laguna, era el organizador de la carrera, y se declaraba responsable del tratamiento de los datos personales de los participantes inscritos en la carrera, determinando los fines y medios en que debía realizarse el tratamiento, así como las condiciones de la carrera, entre las que se encontraba comunicar el lugar y fecha de recogida de los dorsales.

En el presente supuesto, la reclamación se dirigió contra ***B.B.B.,*** porque el correo electrónico masivo que divulgó los correos electrónicos de 493 participantes de la carrera, entre los que se encontraba el reclamante, fue remitido desde la dirección adelanteventos@gmail.com y en el pie de firma constaba ***B.B.B.***. Sin embargo, ello no implica que la responsabilidad del tratamiento sobre los datos personales que fueron desvelados con dicho correo recaiga en la persona cuyo nombre aparece como

remitente del correo electrónico. Toda vez que el artículo 4.7 del RGPD declara que siempre será responsable del tratamiento el que haya fijado los fines y medios del mismo, y no aquellas personas o entidades que ejecutan las instrucciones que éste ha fijado (ya sean como personal del propio Ayuntamiento, o como encargado del tratamiento contratado por el mismo). Esto es, el responsable del tratamiento responderá de los actos que realicen sus empleados públicos o los posibles encargados que contrate para realizar parte de las funciones competencia del Ayuntamiento que requieran realizar operaciones de tratamiento de datos personales que los interesados hayan proporcionado al responsable (en este caso, al OAD de La Laguna, perteneciente al Ayuntamiento).

Según dilatada jurisprudencia europea, se ha consolidado el criterio en base al cual, en materia de protección de datos personales, el que fija los fines y medios del tratamiento de los datos personales será el único responsable de las operaciones de tratamiento que realicen las personas que actúan siguiendo sus instrucciones, ya sean personal del propio Ayuntamiento, o encargados del tratamiento que gestionen alguno de los trámites o actuaciones necesarias del tratamiento que impliquen acceder y utilizar dichos datos personales. Como en este caso sería el trámite o actuación de comunicar el horario y lugar de entrega de dorsales de la carrera, que se ha realizado mediante el correo electrónico al que se refiere el presente expediente.

Cabe señalar, como ejemplo de esta jurisprudencia, la Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de diciembre de 2023, dictada en el asunto C-683/21 (Nacionalinis visuomenės sveikatos centras), la cual indica:

> *"Dado que, como se ha indicado en el apartado 36 de la presente sentencia, un responsable del tratamiento es responsable no solo por todo tratamiento de datos personales que efectúe él mismo, sino también por los tratamientos realizados por su cuenta, puede imponerse a ese responsable una multa administrativa con arreglo al artículo 83 del RGPD en una situación en la que los datos personales son objeto de un tratamiento ilícito y en la que no es él, sino un encargado al que ha recurrido, quien ha efectuado el tratamiento por cuenta suya"*

De las evidencias obtenidas a través de la expedición de la mencionada Diligencia y los propios correos electrónicos aportados por el reclamante se desprende que en este caso no cabe lugar a dudas de que el ***B.B.B.*** estaba actuando por cuenta del Ayuntamiento cuando remitió el correo de 20/04/23 al que se refiere este expediente, toda vez que:

- El correo electrónico en cuestión tenía por objeto ejecutar parte de las funciones asumidas para la organización de la carrera por el OAD del Ayuntamiento, dado que su finalidad era comunicar los días y lugar de entrega de los dorsales a sus participantes, especificando las fechas, horas y lugar, tal y como se indicaba en el Reglamento de Inscripción de la carrera (22 y 23 de abril de 2023 en la Plaza de la Catedral). Lo que requería acceder a los datos personales de los participantes.
- De la política de privacidad publicada en la sede del OAD de La Laguna, así como de lo dispuesto en el Reglamento y Convocatoria de la carrera, se deduce que los participantes de la carrera le proporcionaron su dirección de

correo electrónico al OAD de La Laguna (y no a “Adelante eventos” ni a ***B.B.B.)***, pues este dato constaba en el formulario de inscripciones y era necesario para poder inscribirse en la carrera, accediendo a la página de inscripciones del OAD del Ayuntamiento (www.deportelagunero.com*)*.

- El remitente del correo no hubiera podido tener acceso a la dirección de correo electrónico de los 493 participantes si el OAD del Ayuntamiento no le hubiera dado acceso a este dato personal de los participantes, al encargarle parte de las funciones de organización de la carrera que le correspondían. En concreto, la dirección de correo electrónico era necesaria para que éste pudiera remitir las comunicaciones que fuera preciso realizar en el marco de la organización de la carrera. Comunicaciones que suponen operaciones de tratamiento de datos personales puesto que precisan recoger/ extraer el dato de la dirección electrónica y/o postal de los participantes, y utilizarlo para remitir los correos mencionados, lo que supone realizar diversas operaciones de tratamiento de datos personales que se someten a los principios y requisitos del RGPD, entre las que están no divulgar ilícitamente los datos personales que un participante ha proporcionado al responsable del tratamiento a otros participantes de la carrera.

Era y es por tanto, el OAD del Ayuntamiento, el responsable de garantizar que no se producen divulgaciones ilícitas de los datos proporcionados por los participantes, por parte de los encargados de tratamiento o personas que se hallen a su servicio, así como de analizar los riesgos derivados del tratamiento de los datos personales que le han proporcionado sus participantes al inscribirse (como su correo electrónico), y prever las medidas organizativas y técnicas de seguridad que sean adecuadas y proporcionadas a estos riesgos, para garantizar que no se vulneran sus derechos y libertades.

En consecuencia, dada la titularidad municipal del OAD, y la personalidad jurídica pública única de la administración local, es el Ayuntamiento de San Cristóbal de La Laguna el presunto responsable al que debe dirigirse el presente procedimiento sancionador de acuerdo con lo previsto en el artículo 70. 1 a) de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (en adelante, LOPPDD):

“Artículo 70. Sujetos responsables.

1. *Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica: a) Los responsables de los tratamientos. b) Los encargados de los tratamientos. c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea. d) Las entidades de certificación. e) Las entidades acreditadas de supervisión de los códigos de conducta. (…)”.*

III

Incumplimiento del Artículo 5.1.f) del RGPD

El artículo 5.1.f) “Principios relativos al tratamiento” del RGPD 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 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad de 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."*

En el presente caso, se ha producido una brecha de seguridad de datos personales, categorizada como una brecha de confidencialidad; como consecuencia del envío de un correo electrónico el 20 de abril de 2023 a la parte reclamante que incluía datos personales de otras muchas personas. En concreto, 493 direcciones de correo electrónico, incluida la del reclamante, que aparecían como destinatarios del correo, siendo visibles para todos ellos, sin utilizar la funcionalidad de copia oculta.

Ello implica una vulneración del Principio de Confidencialidad contenido en el artículo 5.1.f) del RGPD, puesto que el correo electrónico citado ha ocasionado una comunicación no autorizada de las direcciones de correo electrónico de todas las personas que aparecen como destinatarios del correo remitido para comunicar el horario y lugar de entrega de dorsales de la carrera organizada por el Ayuntamiento. Toda vez que los destinatarios que aparecen en tal correo electrónico no han solicitado ni tienen legitimación para conocer las direcciones de correo electrónico de los restantes participantes, más allá de aquellos supuestos regulados por la normativa de protección de datos personales.

En conclusión, de conformidad con los hechos probados en el presente procedimiento, se considera que los hechos expuestos vulneran lo establecido en el artículo 5.1.f) del RGPD, por haber divulgado ilícitamente las direcciones de correo electrónico de los 493 destinatarios que aparecen visibles en el citado correo electrónico.

IV
Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De conformidad con los hechos probados en el presente procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable al reclamado, por vulneración del Principio de Confidencialidad previsto en el artículo 5.1.f) del RGPD.

En concreto, de confirmarse la realidad de los hechos denunciados, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone (el subrayado es nuestro):

"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, cabe aplicar el artículo 72 "Infracciones consideradas muy graves" de la LOPDGDD, que indica (el subrayado es nuestro):

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

V
Incumplimiento del Artículo 32 del RGPD

El Artículo 32 "Seguridad del tratamiento" del RGPD establece 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.

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.

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.

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".

Hay que señalar que el RGPD ha supuesto un cambio de paradigma, que se arbitra en torno a pilares esenciales como los principios de responsabilidad proactiva y gestión de riesgos desde el diseño y por defecto, así como la rendición de cuentas, pilares sobre los que pivota la nueva regulación, con la finalidad de proteger, aún más, los derechos y libertades de los interesados en materia de protección de datos.

En base a esta nueva concepción, 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 son responsables "proactivos" que aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento que realizan (por ser los que conocen el mismo al detalle), 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, cabe destacar que el artículo 32 del RGPD dice expresamente que 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.

Y, 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".*

La responsabilidad del Ayuntamiento respecto al incumplimiento de este precepto viene determinada porque éste es el responsable de tomar decisiones destinadas a adoptar e implementar de manera efectiva las medidas técnicas y organizativas

apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

En el presente caso ha quedado acreditado que en el momento de remitir el correo electrónico al que se refiere el presente procedimiento, el OAD del Ayuntamiento, que recogía los datos personales de los participantes que se inscribieron en la media maratón, no había previsto "*las medidas de seguridad razonables en función de los posibles riesgos estimados*" a las que se refiere el artículo 32 del RGPD, pues entre estos riesgos, se encontraba sin lugar a dudas el riesgo de divulgación no autorizada de las direcciones de correos electrónico de los participantes cuando remita comunicaciones electrónicas a más de un destinatario.

Por lo que, concurriendo tal riesgo de divulgación ilícita, su deber como responsable del tratamiento de estos datos personales era preverlo, y adoptar "*medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo",* que *se* dirijan a impedir que cualquier miembro de la organización (o encargado del tratamiento al que se hayan proporcionado los datos personales de los participantes) pueda remitir correos electrónicos dirigidos a más de un destinatario, sin utilizar la funcionalidad de copia oculta.

En conclusión, a la vista de los hechos probados en el presente procedimiento sancionador, se considera que los hechos conocidos vulneran lo establecido en el artículo 32 del RGPD, por no haber previsto las medidas de seguridad adecuadas al riesgo de divulgación ilícita que supone la remisión de correos electrónicos a múltiples destinatarios sin utilizar la funcionalidad de copia oculta.

VI

Tipificación y calificación de la infracción del artículo 32 del RGPD

En virtud de lo indicado en el fundamento de derecho anterior, de conformidad con los hechos probados en el presente procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción administrativa por vulneración del artículo 32 del RGPD, por no establecer medidas adecuadas de seguridad que evitasen brechas como la producida en este supuesto.

De confirmarse este hecho, la citada infracción del artículo 32 del RGPD podría suponer la comisión de una infracción tipificada en el artículo 83.4 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone lo siguiente (el subrayado es nuestro):

> *"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:*
>
> *5) 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 esta infracción, el artículo 73 "Infracciones consideradas graves" de la LOPDGDD indica:

"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".

VII
Propuesta de sanción

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."*

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone que:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.
2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las

medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016".

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.
3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.
4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

Perteneciendo el responsable del tratamiento a la administración local, una vez confirmada la comisión de las citadas infracciones, corresponde dictar resolución declarando la infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD por parte del Ayuntamiento de San Cristóbal de La Laguna.

VIII
Adopción de medidas correctivas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*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…"*

La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En este caso, la medida consistirá en adoptar y **acreditar ante esta Agencia en el plazo de 1 mes** las medidas técnicas y organizativas necesarias para evitar que la remisión de comunicaciones o correos electrónicos a múltiples destinatarios por parte de personal del Ayuntamiento o de personas o entidades que actúen de acuerdo con

sus instrucciones, se realice sin utilizar la funcionalidad “CCO” o cualquier otra que evite que la dirección de correo de cada destinatario sea desvelada.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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: DECLARAR que **AYUNTAMIENTO DE SAN CRISTÓBAL DE LA LAGUNA**, con NIF **P3802300H**, ha infringido lo dispuesto en el Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, infracción tipificada en el Artículo 83.5.a) del RGPD y Artículo 83.4.c) del RGPD.

SEGUNDO: ORDENAR a ***AYUNTAMIENTO DE SAN CRISTÓBAL DE LA LAGUNA***, con NIF ***P3802300H***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 1 mes desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las siguientes medidas correctivas:

- Adoptar y **acreditar ante esta Agencia en el plazo de 1 mes** las medidas técnicas y organizativas necesarias para evitar que la remisión de comunicaciones o correos electrónicos a múltiples destinatarios por parte de personal del Ayuntamiento o de personas o entidades que actúen de acuerdo con sus instrucciones, se realice sin utilizar la funcionalidad “CCO” o cualquier otra que evite que la dirección de correo de cada destinatario sea desvelada.

TERCERO: NOTIFICAR la presente resolución a ***AYUNTAMIENTO DE SAN CRISTÓBAL DE LA LAGUNA***.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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.

938-16012024

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