- **Expediente N.º: EXP202104139**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 28 de septiembre de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***JAÉN SENTIDO Y COMÚN*** con NIF ***G23798606*** (en adelante, la parte reclamada o JSyC). Los motivos en que basa la reclamación son los siguientes:

El reclamante expone que en fecha 26/09/2021 ha recibido un correo electrónico remitido a 241 destinatarios con las direcciones de todos ellos visibles, sin haber hecho uso de la funcionalidad de "con copia oculta CCO". Junto con el escrito de reclamación aporta copia de la comunicación recibida, remitida por JAÉN, SENTIDO Y COMÚN convocando a la asamblea abierta de fecha 30/09/2021 de JSy C.

El 28/09/2021 el reclamante se dirige a la formación política, solicitando que se acredite la autorización para la utilización de ese email para estas comunicaciones porque su participación en el grupo municipal fue en XXXX en el proceso de candidaturas para la alcaldía en la que concurrían varias organizaciones políticas, y sospecha que se podría haber producido un tratamiento o cesión de datos sin su autorización. También solicitaba la vía de contacto con el DPD.

Expone que ha recibido una contestación evasiva y que se le informa de que procedían a la eliminación de su dirección de correo electrónico de su lista de contactos.

El reclamante expone que él solicitó información sobre el tratamiento realizado con su correo electrónico y no se ha contestado.

Junto a la reclamación se aporta copia del correo electrónico remitido donde figuran 241 destinatarios con las direcciones de todos ellos visibles.

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), se dio traslado de dicha reclamación a la parte reclamada/ALIAS, 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), no fue recogido por el responsable; reiterándose el traslado en fecha 01/12/2021 por correo postal certificado, fue nuevamente devuelto por “ausente”.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 23 de diciembre de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 18 de marzo de 2022, 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 83.4 del RGPD.

QUINTO: 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: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 28 de septiembre de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirigió contra ***JAÉN SENTIDO Y COMÚN*** con NIF ***G23798606*** (en adelante, la parte reclamada o JSyC). Los motivos en que basa la reclamación son los siguientes:

El reclamante en fecha 26/09/2021 recibió un correo electrónico remitido a 241 destinatarios con las direcciones de todos ellos visibles, sin haber hecho uso de la funcionalidad de "con copia oculta CCO". Junto con el escrito de reclamación aporta copia de la comunicación recibida, remitida por JAÉN, SENTIDO Y COMÚN convocando a la asamblea abierta de fecha 30/09/2021 de JSy C.

El 28/09/2021 el reclamante se dirigió a la formación política, solicitando que se acreditase la autorización para la utilización de ese email para estas comunicaciones porque su participación en el grupo municipal fue en XXXX en el proceso de candidaturas para la alcaldía en la que concurrían varias organizaciones políticas, y sospecha que se podría haber producido un tratamiento o cesión de datos sin su autorización. También solicitaba la vía de contacto con el DPD.

El reclamante recibió una contestación evasiva y en la que se le informó de que procedían a la eliminación de su dirección de correo electrónico de su lista de contactos.

El reclamante solicitó información sobre el tratamiento realizado con su correo electrónico y no ha recibido respuesta.

FUNDAMENTOS DE DERECHO

I

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*."

II

Los hechos denunciados se concretan en el envío de una convocatoria de Asamblea a una serie de destinatarios, sin ocultar sus respectivas direcciones de correo electrónico, vulnerando el principio de confidencialidad.

Dicho tratamiento podría ser constitutivo de una infracción del 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»).

(…)"

La documentación obrante en el expediente ofrece indicios evidentes de que la parte reclamada vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al revelar a terceros, datos de carácter personal (en concreto la dirección de correo electrónico), al remitir sin copia oculta una convocatoria de asamblea._Ello por carecer de las medidas adecuadas de seguridad, conforme se motiva en el apartado siguiente.

III

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;

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

b) 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."

Los hechos puestos de manifiesto suponen que no consta acreditado en el expediente la existencia de medidas técnicas y organizativas adecuadas conforme a lo exigido en el RGPD, al revelar información y datos de carácter personal a terceros, con la consiguiente falta de diligencia por el responsable, al haberse enviado un correo electrónico sin copia oculta a 241 destinatarios, facilitándose así a cada destinatario el acceso al correo electrónico del resto de los destinatarios, lo que supone una revelación de datos de carácter personal a terceros.

IV

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 241 destinatarios, entre ellos el reclamante, en el que se convoca a una Asamblea, 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".

V

El artículo 83.5 del RGPD 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."*

Establece el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, 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:*

(…)

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

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."

(…)

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves",* 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

VI

Esta infracción del artículo 32.1. del RGPD puede ser sancionada con multa de 10.000.000,00 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 10% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo {83.4, del RGPD.

Esta infracción del artículo 5.1.f) del RGPD puede ser sancionada con multa de 20.000.000,00 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 20% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5 del RGPD.

VII

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar para su corrección (configuración del envío de correos de forma que se puedan enviar con copia oculta cuando se dirija a una pluralidad de interesados), sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien

conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a ***JAÉN SENTIDO Y COMÚN***, con NIF ***G23798606***, una:

- Sanción de 500 euros (quinientos euros), por la infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4 del RGPD y considerada “grave” a efectos de prescripción en el artículo 73.f) de la LOPDGDD.

- Sanción de 1.500 euros (mil quinientos euros), por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD y considerada “muy grave” a efectos de prescripción, en el artículo 72.1.a) de la LOPDGDD.

SEGUNDO: REQUERIR, en virtud de los poderes correctivos que el artículo 58.2 del RGPD otorga a las autoridades de control, que el responsable configure el envío de correos de forma que se puedan enviar con copia oculta cuando se dirija a una pluralidad de interesado, como medida que procede adoptar para que cese la conducta infractora analizada, se corrijan los efectos de la infracción cometida y se adecúen los tratamientos a las exigencias contempladas en los artículos 5.1.f) y 32 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido, en el plazo de 10 días hábiles desde el siguiente a la recepción de la notificación de la presente resolución.

TERCERO: NOTIFICAR la presente resolución a ***JAÉN SENTIDO Y COMÚN***.

CUARTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.

938-050522
Mar España Martí
Directora de la Agencia Española de Protección de Datos