- **Expediente Nº: PS/00084/2021**

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 16 de octubre de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AURORA ENERGY SUPPLY S.L. con CIF B17657719 (en adelante AURORA) Los motivos en que basa la reclamación son los siguientes:

"Ayer 15 de octubre, recibí 160 mails procedentes de la compañía ASICXXI, a la que mi compañía eléctrica Aurora Energy Supply tiene contratado como proveedor de servicios informáticos de la empresa. Estos correos electrónicos iban dirigidos a todos los clientes, y en dichos mails se puede leer las direcciones de correo electrónico de los clientes, entre ellas la mía, quedando al descubierto información privada de todos los clientes"

Junto a la reclamación aporta copia de uno de los correos electrónicos en el que figuran las direcciones de correo electrónico de una pluralidad de clientes.

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 AURORA 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.

Con fecha 12/01/2021 se recibe en esta Agencia escrito de respuesta indicando:

-En fecha 15/10/2020 detectaron un intento de estafa a sus clientes, mediante llamada telefónica, amenazando con cortar el suministro eléctrico si no cedían sus datos personales y bancarios.

-Ante ese hecho, decidieron contactar con sus clientes mediante correo electrónico, que fue enviado a la mercantil ASIC XXI S.L., con CIF B99276917, (en adelante, ASIC), empresa con la que tienen contrato de servicios informáticos, siendo uno de ellos el envío de comunicaciones a los clientes. En fecha 15/10/2021, ASIC procedió al envío del correo electrónico cometiendo el error de no poner en copia oculta a los destinatarios, provocando el envío de un correo masivo.

-En fecha 16/10/2021, ASIC envía correo electrónico a AURORA comunicando el error cometido y asumiendo su responsabilidad.

TERCERO: Con fecha 16 de enero de 2021 se produjo la admisión a trámite de la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 2 de diciembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ASIC, por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

QUINTO: Con fecha 13 de enero de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a ASIC XXI, S.L., con CIF B99276917, con un APERCIBIMIENTO por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, y con un APERCIBIMIENTO por una infracción del Artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

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: Consta acreditado que ASIC envió un correo electrónico a clientes de AURORA ENERGY SUPPLY S.L., cometiendo el error de no poner en copia oculta a los destinatarios, provocando el envío de un correo masivo.

SEGUNDO: Consta acreditado, según manifiesta ASIC, que éste hecho se debió a un error de carácter aislado, y que se han tomado medidas para impedir que pueda volver a producirse en el futuro.

## 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

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que ASIC realiza, entre

otros tratamientos, la utilización de los siguientes datos personales de personas físicas, tales como: nombre, dirección de correo electrónico, etc. ASIC realiza esta actividad en su condición de encargado del tratamiento, dado que trata estos datos personales por cuenta de AURORA ENERGY SUPPLY S.L., que es la responsable de este tratamiento en cuestión, todo ello en virtud del artículo 4.8 del RGPD.

III

Se imputa a ASIC la comisión de una infracción por vulneración del artículo 5.1.f) del RGPD, y por vulneración del artículo 32 del RGPD.

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

*"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 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:

> *"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 este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece 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*".
>
> A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:
>
> *"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:*

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

Dado que se ha demostrado a lo largo de la instrucción del procedimiento que ASIC ha difundido datos personales de la parte reclamante y de otras 160 personas, sin su consentimiento, al enviar al menos, según la documentación obrante en el expediente, un correo electrónico masivo sin copia oculta, permitiendo así que cada uno de los receptores tuviera acceso a la dirección de correo electrónico del resto, queda acreditada la infracción al artículo 5.1.f) del RGPD.

IV

Sin perjuicio de lo dispuesto en el 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; (…)"*

Por su parte, el considerando 148 del RGPD indica:

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

V

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

*"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 citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD, que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

*"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 este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece 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*".

A efectos del plazo de prescripción, 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.*

De la instrucción llevada a cabo en el presente procedimiento, se considera que ASIC ha incumplido lo dispuesto en el artículo 32 del RGPD, al no contar con las medidas organizativas y técnicas apropiadas para impedir el envío de un correo electrónico sin copia oculta. Queda, por tanto, acreditada, la infracción al citado artículo.

VI

Sin perjuicio de lo dispuesto en el 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; (…)"*

Por su parte, el considerando 148 del RGPD indica:

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

VII

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 ASIC XXI, S.L., con CIF B99276917, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, un apercibimiento.

Dirigir a ASIC XXI, S.L., con CIF B99276917, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, un apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a ASIC XXI, S.L.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el

día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-100322

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