- **Expediente N.º: PS/00101/2022**

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 17 de mayo de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra ***RESTEXPERIENCE, S.L.*** con NIF ***B88260609*** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La reclamante expone que solicitó el 7 de abril de 2021 al director de Operaciones y EXPANSIÓN DEL GRUPO RESTEXPERIENCE su certificado de retenciones.

El 5 de mayo de 2021 el director de operaciones envió por correo electrónico a la reclamante y a otros 11 destinatarios un fichero PDF en el que consta el certificado de retenciones de 36 trabajadores de la empresa.

Junto a la reclamación aporta el correo remitido el 5 de junio de 2021 junto al fichero anexado.

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), el 14 de junio de 2021, se dio traslado de dicha reclamación a la parte reclamada, 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) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 25 de junio de 2021 como consta en el certificado que obra en el expediente.

TERCERO: Con fecha 7 de septiembre de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de 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:

(…).

Se ha solicitado información y documentación a la entidad responsable, y de la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos y acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

(…).

(…).

Respecto de las causas que hicieron posible la brecha

(…).

Respecto de los datos afectados

(…).

Respecto del contrato de encargado del tratamiento

(…).

Respecto de las medidas de seguridad implantadas:

(…).

(…):

(…).

(…):

(…)

(…)

(…)

(…):

- ***(…).***
- ***(…).***

- ***(…)***

(…)

Respecto de la notificación con posterioridad a las 72 horas

(…)

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo

(…)

QUINTO: Con fecha 31 de mayo de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

SEXTO: Con fecha 10 de junio de 2022, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que *"esta parte reconoce la responsabilidad que se le está imputando y por ello solicita que se proceda a la reducción oportuna de la sanción. Así mismo, pone en conocimiento de la AGEPD que la intención de la empresa sería abonar en el plazo oportuno el pago voluntario de la sanción impuesta, no obstante, la situación económica negativa en la que se encuentra la misma no lo permite".*

SEPTIMO: Con fecha 6 de julio de 2022, el instructor del procedimiento acordó dar por reproducidos a efectos probatorios la reclamación interpuesta por ***A.A.A.*** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por ***RESTEXPERIENCE, S.L.,*** y la documentación que a ellas acompaña.

OCTAVO: Con fecha 15 de julio de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a ***RESTEXPERIENCE, S.L.***, con NIF ***B88260609***, por una infracción del artículo 5.1.f) del RGPD y por una segunda infracción del artículo 32 del RGPD, tipificadas respectivamente en los artículos 83.5 a) y 83.4 a) del RGPD, con una multa de 3.000 euros (tres mil euros) y 2.000 euros (dos mil euros) respectivamente.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: La entidad reclamada ha enviado por correo electrónico a la reclamante y 11 personas más, el certificado de retenciones de 36 personas, vulnerando la confidencialidad requerida en el tratamiento de datos personales, así como el principio de integridad y confidencialidad, para que los datos sean tratados de tal manera que se garantice una seguridad adecuada de los datos personales.

SEGUNDO: La entidad reclamada reconoce las infracciones cometidas y solicita la doble reducción por reconocimiento de la infracción y pronto pago, pero alega que no puede proceder al mismo.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

Los principios relativos al tratamiento de datos de carácter personal, se regulan en el artículo 5 del RGPD donde se establece que *"los datos personales serán:*

"a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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 responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

El artículo 72.1 a) de la LOPDGDD señala que “*en función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

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

III

La seguridad en el tratamiento de datos personales viene regulada en el artículo 32 del RGPD donde se 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.*

***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."*

El artículo 73.f) de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves dispone:

"En función del artículo 83.4 del Reglamento (UE) 2016/679 se considerarán graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel, y en particular los 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

IV

De conformidad con las evidencias de las que se dispone, corroboradas con las alegaciones aportadas por la parte reclamante el 10 de junio de 2022, al indicar que reconoce los hechos que le son imputados, pero que no puede proceder al pronto pago por la situación económica actual, se considera que la entidad reclamada al remitir por correo electrónico a la reclamante y a otros 11 destinatarios un fichero PDF en el que consta el certificado de retenciones de 36 trabajadores de la empresa, ha vulnerado la confidencialidad requerida en el tratamiento de datos personales, y con ello se contraviene el artículo 5.1 f) del RGPD, que rige el principio de integridad y confidencialidad, para que los datos sean 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.

Ha de hacerse notar, que la entidad reclamada ha manifestado que este incidente no fue identificado como brecha de seguridad hasta que se recibió el traslado de esta reclamación y, por este motivo, no se informó a la delegada de protección de datos ni se analizó su alcance para valorar la notificación a los interesados ni a la AEPD.

Asimismo, la entidad reclamada considera que las medidas de seguridad implantadas son auditadas cada dos años en materia de protección de datos, donde específicamente se revisen los procedimientos de envío de documentación que contenga datos personales.

La entidad reclamada considera que no existe un riesgo para los derechos y libertades de los afectados, y que no consta la utilización de los datos por terceros aparte de la presentación de esta reclamación ante la AEPD.

Pese a lo indicado, esta Agencia considera que la existencia de un solo caso es suficiente para denotar que las medidas de seguridad de la entidad reclamada no eran adecuadas en el momento de producirse el incidente objeto de reclamación y deben

ser mejoradas porque queda constatado que no han sido suficientes para evitar los hechos denunciados.

Así las cosas, esta Agencia considera que la entidad reclamada, ha infringido los artículos 5.1 f) y 32 del RGPD, al violar el principio de integridad y confidencialidad, así como no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de sus clientes.

V

El artículo 58.2 del RGPD dispone lo siguiente: "Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

d) 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;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

VI

A fin de determinar las multas administrativas a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias."

"*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Respecto al apartado k) del artículo 83.2 del RGPD, la LOPDGDD, artículo 76, "*Sanciones y medidas correctivas",* dispone:

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

VII

La infracción del artículo 5.1 f) del RGPD puede ser sancionada con multa de 20 000 000 € 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, de acuerdo con el artículo 83.5 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD, considerando como agravante según el artículo 76.2 b) LOPDGDD, la vinculación del responsable con el

tratamiento de datos personales, y el número de afectados, al haberse remitido datos personales de 36 personas.

VIII

La infracción del artículo 32 del RGPD puede ser sancionada con multa de 10 000 000 € 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, de acuerdo con el artículo 83.4 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD, considerando como agravante según el artículo 76.2 b) LOPDGDD, la vinculación del responsable con el tratamiento de datos personales y el número de afectados, al haberse remitido datos personales de 36 personas.

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 ***RESTEXPERIENCE, S.L.***, con NIF ***B88260609***, por una infracción del artículo 5.1.f) del RGPD y por una segunda infracción del artículo 32 del RGPD, tipificadas respectivamente en los artículos 83.5 a) y 83.4 a) del RGPD, una multa de 3.000 euros (tres mil euros) y otra de 2.000 euros (dos mil euros) respectivamente.

SEGUNDO: NOTIFICAR la presente resolución a ***RESTEXPERIENCE, S.L.***

TERCERO: 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.

938-120722

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