

- **Expediente N°: PS/00089/2022**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO
VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 23 de febrero de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **FREE SUN ENERGY S.L.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N°: PS/00089/2022

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: **A.A.A.** (en adelante, la parte reclamante) con fecha 28 de marzo de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra **FREE SUN ENERGY S.L.** con NIF B67572669 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

Se ha recibido un correo electrónico en el que se informa de que ya está disponible su factura electrónica, pero la factura que recibe es la de otro cliente, aportando todos sus datos, nombre, apellidos, dirección, NIF, sus datos de consumo, precios e importe.

Se acompaña junto con su reclamación:

- Impresión de correo electrónico de fecha 3 de marzo de 2021 remitido por *****EMAIL.1** hacia *****EMAIL.2** (en adelante, el email de la reclamante) en el que se indica que se adjunta la factura.
- Copia de una factura de “Free energía by NACE” de fecha 25/02/2021 que la reclamante indica que aparecía como adjunto al anterior correo. En esta factura aparece como titular una persona que no es la reclamante.

Los datos que aparecen en esta factura, entre otros, son los siguientes: nombre y apellidos del titular, NIF, dirección de suministro, CUPS, tarifa de acceso, número de contador, forma de pago, datos de consumo e IBAN sin los cuatro últimos dígitos.

- Impresión de correo electrónico de fecha 26 de marzo de 2021 remitido por el email de la reclamante hacia *****EMAIL.3** en el que informa de que ha recibido la factura de otro cliente y solicita ejercer su derecho del artículo 15 de la ley orgánica 3/2018 (que es el derecho de supresión) debido a que ha recibido la factura de otro cliente.

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, 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 16/05/2021 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 23 de julio 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

El 22 de febrero de 2022, la entidad reclamada presenta las siguientes manifestaciones:

La parte reclamante recibió el correo del 3 de marzo de 2021 que indica en su reclamación debido a un error en la asignación automática del identificador de facturas, que generó dos facturas con el mismo identificador para dos clientes y CUPS distintos.

El origen de la incidencia está en la actualización de la aplicación que realiza las funciones de facturación, que repitió algunos números de facturación hasta que se detectó el incidente y se solucionó mediante una actuación en la base de datos.

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.

La entidad reclamada considera que las medidas de seguridad implantadas por PARTNERTEC S.L., que es la empresa que presta el servicio de software CRM (*Customer Relationship Management* o Gestión de la Relación con Clientes), pese a

ser adecuadas, no sirvieron para evitar el incidente debido a que se produjo por un cambio en el aplicativo.

Se aporta contrato de licencia de software que incluye la implantación, integración y *hosting* entre PARTNERTC S.L. y VISALIA ENERGÍA S.L.U. de fecha 14 de mayo de 2019, y acuerdo de confidencialidad entre los mismos de fecha 22 de junio de 2018. Y se indica que este contrato aplica a FREE ENERGÍA al ser una empresa del grupo empresarial VISALIA ENERGÍA S.L.U.

La entidad reclamada manifiesta que tras evaluar este incidente, 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.

La entidad reclamada hace notar que no se tiene constancia de otros incidentes similares.

Finalmente adjunta impresión de correo electrónico de fecha 17 de febrero de 2022 remitido por *****EMAIL.2** al email de la reclamante con un documento adjunto, que se indica que tiene el siguiente contenido:

“Atendiendo a su solicitud de protección de datos, le informamos que, de conformidad con la misma, FREE ENERGÍA ha procedido a tramitar la supresión de sus datos personales.

Sin perjuicio de lo anterior, y de conformidad con lo establecido en el artículo 17.3 RDPG, procederemos a conservar sus datos para el cumplimiento de las obligaciones legales que puedan derivarse de su relación jurídica con la empresa, así como en su caso, dar cumplimiento a requerimientos judiciales.

Por todo ello, y dado que FREE ENERGÍA, quiere respetar escrupulosamente el ejercicio de sus derechos, le informamos que quedamos a su disposición para cualquier aclaración que precise.”

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 en el presente momento, y sin perjuicio de lo que resulte de la instrucción de este procedimiento sancionador, se considera que la entidad reclamada al remitir por correo electrónico una factura de otro cliente al reclamante, donde se incluyen datos personales como nombre y apellidos del titular, NIF, dirección de suministro, CUPS, tarifa de acceso, número de contador, forma de pago, datos de consumo e IBAN sin los cuatro últimos dígitos, se está vulnerando 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 además, 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 por PARTNERTEC S.L., que es la empresa que presta el servicio de software CRM (*Customer Relationship Management* o Gestión de la Relación con Clientes), pese a ser adecuadas, no sirvieron para evitar el incidente debido a que se produjo por un cambio en el aplicativo.

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, sin perjuicio de lo que resulte de la instrucción, 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

Esta infracción 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.

VII

Por lo tanto, a tenor de lo anteriormente expuesto,

Por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a **FREE SUN ENERGY S.L.**, con NIF B67572669, por la presunta infracción de conformidad con lo previsto en el artículo 58.2.b) del RGPD, por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD.

SEGUNDO: INICIAR PROCEDIMIENTO SANCIONADOR a **FREE SUN ENERGY S.L.**, con NIF B67572669, de conformidad con lo previsto en el artículo 58.2.b) del RGPD, por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD.

TERCERO: NOMBRAR como instructor a **B.B.B.** y, como secretario, a (...), indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

CUARTO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por la Subdirección General de Inspección de Datos durante la fase de investigaciones, así como el informe de actuaciones previas de Inspección.

QUINTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, le

correspondería una sanción de 5.000 € (cinco mil euros), por la infracción del artículo 5.1 f) del RGPD, sin perjuicio de lo que resulte de la instrucción.

SEXTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, le correspondería una sanción de 5.000 € (cinco mil euros), por la infracción del artículo 32 del RGPD, sin perjuicio de lo que resulte de la instrucción.

SEPTIMO: NOTIFICAR el presente acuerdo a **FREE SUN ENERGY S.L.**, con NIF B67572669, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, cada sanción quedaría establecida en 4000 €, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, cada sanción quedaría establecida en 4000 € y su pago implicará la terminación del procedimiento.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida

en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de cada sanción quedaría establecido en 3.000 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente 4.000 € o 3.000 € cada sanción, lo cual implicaría un total de 8.000 € o 6.000 € respectivamente, deberá hacerlo efectivo mediante su ingreso en la cuenta 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., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-260122

Mar España Martí

Directora de la Agencia Española de Protección de Datos

>>

SEGUNDO: En fecha 11 de abril de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **6000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO: El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

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 registrarán 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

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica *“Terminación en los procedimientos sancionadores”* dispone lo siguiente:

“1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente.”

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DECLARAR la terminación del procedimiento **PS/00089/2022**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **FREE SUN ENERGY 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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

936-240122

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