- **Expediente Nº: EXP202105644**

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 8 de junio de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **NATURGY ENERGY GROUP, S.A.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202105644

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 4 de noviembre de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra la sociedad **COMERCIALIZADORA REGULADA GAS & POWER, S.A.,** perteneciente a **NATURGY ENERGY GROUP, S.A.** con NIF A08015497 (en adelante, la parte reclamada), de la que es cliente la reclamante.

La reclamante ha tenido conocimiento de que un tercero ha hecho uso de sus datos personales para cambiar el correo electrónico y solicitar que enviaran dos facturas suyas, por lo que interpone reclamación ante la reclamada, y le informan que este cambio se realizó de manera telefónica, facilitando el nombre de este tercero, e indicándole que habían obrado de manera correcta ya que la persona que llamó facilitó el nombre, DNI, dirección y referencia del contrato de la reclamante.

Por lo tanto, el motivo en que basa su reclamación es el cambio de los datos de su contrato con la entidad reclamada, en concreto de su correo electrónico sin su consentimiento.

Junto a la notificación se aporta los correos electrónicos intercambiados con la reclamada exponiendo los hechos, así como contestación a los mismos, detallando en uno de ellos el nombre de la persona que llamó (que no coincide con el nombre de la reclamante) y el correo electrónico facilitado.

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 27 de diciembre 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), fue recogido en fecha 28 de diciembre de 2021 como consta en el acuse de recibo que obra en el expediente.

Con fecha 27 de enero de 2022, se recibe en esta Agencia escrito de respuesta de la entidad reclamada indicando lo siguiente:
"El 4 de octubre de 2021, el servicio de atención al cliente de Comercializadora Regulada recibió una llamada de una persona que se identificó como "familiar" de la reclamante, e indicó que deseaba solicitar un duplicado de la última factura del suministro de electricidad correspondiente al punto de suministro de la reclamante, aportando una dirección de correo electrónico para que le fuera remitida la factura.

Para poder realizar las gestiones demandadas, es necesario superar la política de seguridad de Comercializadora Regulada, para lo que se solicita a la persona que llama determinada información del titular de los contratos de suministro que solo debería conocer dicho titular o persona habilitada por el mismo.

El Peticionario disponía de toda la información necesaria para superar la política de seguridad y realizar las gestiones que solicitaba. Así, en concreto, facilitó el nombre y apellidos, así como el DNI de la reclamante y también los cuatro últimos dígitos de la cuenta bancaria de la reclamante.

Todos estos datos y, en particular, los cuatro últimos dígitos del número de cuenta bancaria, constituyen una información que solamente debería conocer la Reclamante.

De hecho, esos cuatros últimos dígitos de la cuenta bancaria constituyen una información que ni siquiera es visible en los documentos que Comercializadora Regulada genera para sus clientes, pues siempre aparecen ocultos, tanto en las facturas como a través del Área Privada, como medida de seguridad."

Por todo ello, la entidad reclamada considera que su actuación ha sido en todo momento diligente y ajustada a derecho.

TERCERO: Con fecha 4 de febrero de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 ha vulnerado la confidencialidad requerida en el tratamiento de datos personales, ya que pese a la medidas de seguridad indicadas se ha permitido el acceso a los datos personales de un cliente sin su consentimiento, logrando que le enviaran dos facturas del cliente al correo electrónico de dicho tercero alegando para obtener dicha información, la existencia de algún tipo de parentesco con el cliente.

Por lo tanto, se ha vulnerado 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.

Esta Agencia considera además que nos encontramos ante una vulneración del artículo 32 del RGPD, ya que las medidas de seguridad de la entidad reclamada no son adecuadas y deben ser mejoradas tras haber quedado 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

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.
.

VII

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.

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 **NATURGY ENERGY GROUP, S.A.** con NIF A08015497, 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 **NATURGY ENERGY GROUP, S.A.** con NIF A08015497, 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 ***C.C.C.***, 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 50.000 € (cincuenta 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 30.000 € (treinta 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 **NATURGY ENERGY GROUP, S.A.** con NIF A08015497, 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, la primera sanción quedaría establecida en 40.000 €, y la segunda en 24.000€ resolviéndose el procedimiento con la imposición de ambas sanciones.

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, la primera sanción quedaría establecida en 40.000 € y la segunda en 24.000€, 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 la primera sanción quedaría establecido en 30.000 euros y la segunda en 18.000 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 40.000 € o 30.000 € para la primera sanción, o 24.000 € o 18.000€ para la segunda, 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 21 de junio de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **48000 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 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

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 **EXP202105644**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **NATURGY ENERGY GROUP, S.A.**.

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