Expediente N.º: EXP202301331

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 enero de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **TOTALENERGIES CLIENTES, S.A.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202301331

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 18 de diciembre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **TOTALENERGIES CLIENTES, S.A.** con NIF A95000295 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que se ha llevado a cabo un cruce de datos al dar de alta el servicio de suministro del gas en su vivienda con la parte reclamada. Afirma que se han asociado sus datos persones con el de un tercero que estaba llevando a cabo el mismo trámite. Señala que los datos personales del tercero (nombre, apellidos, dirección postal y cuenta bancaria) figuran en el contrato suscrito para el suministro de gas del domicilio de la reclamante, donde los únicos datos correctos, son la dirección del suministro, DNI, teléfono y correo electrónico.

A efectos acreditativos, se acompaña al escrito de reclamación el contrato celebrado con la compañía reclamada, en el cual figuran tanto datos de la un reclamante como de un tercero, así como un correo electrónico dirigido por la parte reclamada al tercero.

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 07/02/2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 07/03/2023 se recibe en esta Agencia escrito de respuesta de la parte reclamada. La respuesta de la entidad en cuestión indica que no constan datos de la parte reclamante en relación con el contrato de suministro de gas mencionado. Además, señalan que no comercializan gas natural y, por lo tanto, no podrían haber establecido un contrato de suministro de este servicio con la reclamante. Afirman que, tras recibir el requerimiento de información y realizar investigaciones pertinentes, la entidad envió una carta a la parte reclamante para informar sobre las acciones realizadas y confirmar la ausencia de datos sobre el contrato de suministro de gas en sus sistemas. Adjuntan una copia de esta carta como documento de referencia.

TERCERO: Con fecha 18 de marzo de 2023, 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 extremos que seguidamente se exponen.

La reclamante expuso un problema de cruce de datos personales con los de un tercero al contratar el servicio de suministro de gas en su domicilio con la compañía reclamada, ocurrido el 12 de diciembre de 2022. En dicho escrito manifiesta que, al darse de alta en el servicio, sus datos personales se mezclaron con los de otro cliente en proceso similar. En el contrato presentado junto a la reclamación, constan datos erróneos como el nombre, apellidos, dirección postal y cuenta bancaria de un tercero, manteniéndose correctos únicamente su dirección de suministro, DNI, teléfono y correo electrónico.

Por su parte, la entidad reclamada, en su respuesta inicial a la presente autoridad, negó la existencia de datos incorrectos en sus sistemas, argumentando que no comercializan gas natural. Sin embargo, tras una investigación más profunda, reconocieron un error humano en el proceso de carga manual de datos, que resultó en el mencionado cruce de información. Señalan que, aunque los datos del tercero se asociaron erróneamente con el perfil de la reclamante, no se activó ningún contrato para el tercero y, por tanto, no tuvo acceso a los datos de la reclamante. Afirman que

la entidad procedió a enviar una carta a la reclamante explicando las razones del incidente y las acciones tomadas para solucionarlo. Asimismo, incluyen detalles sobre la actualización de la facturación del suministro de gas y servicio de mantenimiento, procediendo a anular las facturas erróneamente emitidas y emitiéndolas nuevamente con los datos correctos.

Se tiene constancia por la presente autoridad que, con anterioridad a la presentación de la reclamación, la reclamante había presentado otra reclamación ante la Oficina Municipal de Información al Consumidor del Ayuntamiento de ******LOCALIDAD.1***, trasladada a la parte reclamada el 24 de enero de 2023 y respondida el 17 de febrero de 2023. En la respuesta a dicho traslado, la entidad detalló las acciones realizadas para resolver el incidente y expresó disculpas por las molestias causadas.

Como documentación adicional presentada por la parte reclamada se incluye un registro de las interacciones entre ésta y la parte reclamante. De la misma se observa que la reclamante había contactado a la entidad en varias ocasiones, comenzando el 7 de noviembre de 2022, para informar sobre la incidencia consistente en la discrepancia en los datos y expresar su descontento con la lentitud de las gestiones. Es mediante esta primera comunicación, a través de la cual la parte reclamada tuvo conocimiento de la incidencia sufrida por la parte reclamante. La compañía mantuvo comunicación regular con la reclamante, tanto telefónicamente como electrónicamente, para confirmar datos y actualizar la situación.

Finalmente, el 13 de febrero de 2023, la entidad realizó la corrección de los datos erróneos en sus sistemas internos, asegurando la desvinculación entre los datos del tercero y los de la reclamante, así como la exactitud de los datos en el área de cliente de la reclamante, resolviendo de esta forma la incidencia.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad TOTALENERGIES CLIENTES, S.A. es una gran empresa, y con un volumen de negocios de 1.700.272.000 € millones en el año 2022

FUNDAMENTOS DE DERECHO

I
Competencia

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, 48.1, 64.2 y 68.1 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
Obligación incumplida del artículo 5.1 f) RGPD

De acuerdo con el apartado 1.f) del artículo 5 RGPD los datos deben ser *"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»)"*

De la misma forma, el Considerado 39 RGPD dispone que: "*Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."*

El principio de confidencialidad, según el mencionado artículo 5.1 f) del RGPD, exige la protección de datos personales contra accesos, usos y divulgaciones no autorizados. Dicho principio resulta esencial para garantizar la seguridad de los datos personales, constituyendo un pilar clave en la protección del derecho fundamental en dicho ámbito. Por el contrario, la violación de este principio puede tener consecuencias no deseadas, reflejando su importancia en el marco normativo de la protección de datos.

En el presente caso, de las actuaciones de investigación realizadas se observa un incidente consistente en el hecho de que los datos personales de la reclamante fueron entrecruzados con los de un tercero en un contrato durante el proceso de alta en un servicio de suministro realizado por la parte reclamada. Dicha situación, sin perjuicio de lo que resulte a lo largo de la instrucción del procedimiento, representa una presunta vulneración de los principios de integridad y confidencialidad de los datos personales, tal como se estipula en el citado artículo 5.1 f) del RGPD y en los términos que seguidamente se exponen.

En primer lugar, conviene indicar que el artículo 4 define como datos personales "*a toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."*

El hecho consistente en asociar erróneamente datos personales de un tercero, como nombre, apellidos, dirección postal y cuenta bancaria, al contrato y perfil de la parte reclamante conlleva que determinados datos hayan sido expuestos por personas no autorizadas. En el presente caso, el cruce indebido de información involucró la exposición no autorizada de los datos personales de un tercero. En este sentido, la gravedad del incidente en este caso reside en las implicaciones que ha supuesto, tanto para la parte reclamante como para el tercero.

En el caso de la parte reclamante, la aparición de datos de un tercero en su contrato no solo generó confusión, sino que también puso en riesgo la propia seguridad de sus

datos personales, al tratarse de información errónea y potencialmente comprometedora. La circunstancia de que, tal y como afirma la parte reclamada, no se produjera finalmente una afectación de sus datos no desvirtúa el hecho de que los mismos se encontraron en riesgo de ser indebidamente tratados en un determinado período de tiempo. Conviene recordar que fue la propia parte reclamante y no la reclamada quien informó de la incidencia producida, lo que conllevo la subsanación de la incidencia de la misma y, en consecuencia, a la mitigación o cese del riesgo.

Por lo que se refiere al tercero afectado, la incorporación sin su consentimiento de sus datos personales en el contrato de otra persona supuso, en consecuencia, una presunta vulneración del principio de confidencialidad, dado que, tuvo conocimiento de dichos datos personales la parte reclamante, la cual no estaba legitimada para acceder a estos, tal y como indica en la propia reclamación y se deduce de las actuaciones previas realizadas por esta entidad.

En conclusión, el incidente en cuestión representa una presunta vulneración del principio de confidencialidad, tal como se define en el artículo 5.1 f) del RGPD. La confidencialidad de los datos personales es un pilar fundamental de la protección de datos, y su infracción en este caso se manifiesta en la exposición no autorizada y el uso indebido de un tercero tras incorporarse erróneamente en el contrato de la parte reclamada.

III

Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, 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:

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

IV
Sanción por la infracción del artículo 5.1.f) del RGPD

Según el artículo 83.2 del RGPD "*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".

De la misma forma, el artículo 76 de la LOPDGDD establece una serie de criterios para graduar la posible sanción, siguiendo lo dispuesto en el apartado k) del anterior artículo:

"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."

Teniendo en cuanta dichos preceptos, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

Posible agravante prevista en el apartado a) del artículo 83.2 del RGPD:

"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;"

La concurrencia de la posible agravante se manifiesta en la naturaleza de la infracción, dado que los hechos han afectado a determinados datos, como información bancaria y de contacto, cuya exposición aumentaba el riesgo de uso indebido y fraude. Además, la infracción se ve agravada por el contexto en el que se produce, puesto que tuvo lugar en un entorno contractual, donde los individuos confían en la entidad para el manejo seguro de su información personal, habiéndose erosionado la confianza y expectativas de los afectados respecto al tratamiento de sus datos personales.

Posible agravante prevista en el apartado b) del artículo 76 del LOPDGDD:

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

La aplicación de esta posible agravante deriva del sector en el que opera la parte reclamada, consistente en el suministro de energía, lo cual conlleva la gestión de una cantidad significativa de datos personales de sus clientes, incluyendo información sensible y detallada relacionada con la facturación y el consumo. Dicha circunstancia amplifica el potencial impacto negativo y el riesgo para los individuos afectados cuyos datos han sido expuestos.

No se aprecia la concurrencia de circunstancias atenuantes.

En función de las mencionadas circunstancias, de acuerdo con lo dispuesto en el artículo 83.5 del RGPD, y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se considera adecuado fijar como posible sanción una multa de cuantía de 140.000 € (CIENTO CUARENTA MIL EUROS)

V
Artículo 32 del RGPD

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”.

Resulta necesario señalar que el citado precepto no establece un listado de medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen 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, determinando aquellas medidas técnicas y organizativas adecuadas 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 debe tener 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.

Por su parte, 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".*

En el presente caso, la producción de la incidencia consistente en el cruce de datos personales entre la parte reclamante y un tercero implica una posible la falta de adopción técnicas y organizativas efectivas para garantizar un adecuado nivel de seguridad. Debe tenerse en cuenta que los datos que son susceptibles de tratamiento por la parte reclamada implican información sensible y personal, incluyendo numerosos datos identificativos, direcciones y detalles bancarios. La naturaleza de tales datos requiere un alto nivel de protección debido a su potencial impacto en los derechos de las personas. Por el contrario, la no adopción de medidas adecuadas expone a los individuos a riesgos significativos, como el fraude o el robo de identidad.

En este sentido, el responsable del tratamiento de los datos personales debe de tener en cuenta los riesgos específicos asociados con la alteración, pérdida, acceso no autorizado, o cruces de datos personales como ocurrió en el presente caso. La falta de medidas para prevenir el cruce de datos indica un posible fallo en la evaluación de riesgos, debiendo la parte reclamada haber evaluado y mitigado estos riesgos.

Por otro lado, es esencial considerar la naturaleza de las operaciones de la entidad reclamada y su impacto en el cumplimiento de las obligaciones de protección de datos, teniendo en cuenta que la misma trata de forma periódica una cantidad considerable de datos personales. Esta perspectiva resulta relevante debido a la escala y regularidad del tratamiento de datos personales, lo que incrementa el riesgo y, en consecuencia, las expectativas de cumplimiento por la entidad responsable. La regularidad con la que la empresa trata datos personales requiere un sistema robusto y actualizado de protección de datos, puesto que cualquier fallo puede tener efectos repetidos o prolongados y ello con independencia de que el fallo sea de origen humano o de cualquier otra naturaleza.

A tal respecto, con el fin de prevenir errores humanos en el manejo de datos personales, como ocurre en el presente caso, una entidad puede adoptar diversas medidas efectivas de distinta índole. Así, sin ánimo de ser exhaustivo, la formación y concienciación continuas del personal, la verificación y validación automatizadas de datos al momento de su entrada, la implementación de procedimientos de doble

verificación para tareas, la tecnología de detección de anomalías que alerte automáticamente sobre incoherencias o irregularidades, junto a otras que resulten adecuadas e implementadas de manera integral, pueden fortalecer significativamente la protección de datos personales y el cumplimiento del RGPD.

Por último, conviene destacar la forma en que tuvo conocimiento de la incidencia la parte reclamada, la cual provino directamente de la persona afectada, y no a través de sus propios sistemas de detección o procedimientos de control interno. Dicho hecho subraya aún más la falta de adopción de medidas de seguridad adecuadas al riesgo. La incapacidad de la parte reclamada para identificar y abordar proactivamente el error por sí misma manifiesta una carencia significativa en sus mecanismos de supervisión y auditoría interna, lo cual refuerza la necesidad de implementar sistemas de revisión y control continuo, no solo para prevenir errores, sino también para detectarlos y rectificarlos de manera oportuna, asegurando así el cumplimiento del RGPD.

En definitiva, el fallo humano consistente en un cruce de datos personales podría haberse evitado si la entidad hubiera adoptado las medidas de seguridad adecuadas. Por el contrario, la producción de la incidencia objeto de la reclamación pone en evidencia la falta adopción de medidas técnicas y organizativas pertinentes y efectivas con el fin de garantizar un nivel de seguridad adecuada el riesgo, lo cual conlleva un presunto incumplimiento del citado artículo 32 del RGPD, sin perjuicio de lo que resulte a lo largo del presente procedimiento.

VI
Tipificación y calificación de la infracción del artículo 32 del RGPD

De confirmarse, 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.

VII
Posible sanción por la infracción del artículo 32 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 32 se sancionará, *"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"*

Asimismo, en el presente supuesto se considera que procede graduar la sanción a imponer de acuerdo con los criterios anteriormente establecido:

Como posible agravante se prevé la prevista en el apartado b) del artículo 76 LOPDGDD:
Posible agravante prevista en el apartado b) del artículo 83.2 del RGPD:

b) la intencionalidad o negligencia en la infracción;

En este caso cabe apreciar una negligencia grave por la parte reclamada. En este sentido, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. En la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, dado que la actividad de la recurrente es de constante y abundante gestión de datos de carácter personal es exigible un mayor rigor y exquisito cuidado con el fin de ajustarse a las previsiones legales.

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

En el presente caso, teniendo en cuenta el volumen de datos personales que gestiona la parte reclamada debido al sector donde opera, conlleva una mayor responsabilidad en cuanto a la implementación de sistemas de seguridad. El no haber establecido medidas de seguridad adecuadas en dicho ámbito amplifica el riesgo significativo de acceso no autorizado, manipulación o pérdida de datos, de lo cual se desprende la concurrencia de esta posible agravante.

No se aprecia la concurrencia de circunstancias atenuantes.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se propone como posible sanción una multa de cuantía de 60.000 € (SESENTA MIL EUROS).

VIII

Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*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…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En el presente supuesto, se podrá requerir al responsable para que en un plazo de tres meses se notifique a esta autoridad la adopción de las siguientes medidas:

- Adoptar las medidas organizativas y técnicas adecuadas para garantizar un nivel de seguridad adecuado el riesgo con el fin de evitar futuros errores humanos, incluyendo mecanismos de detección que permitan identificar y corregir rápidamente cualquier error humano que en su caso pudiera producirse para, de esta forma, minimizar su impacto.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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 **TOTALENERGIES CLIENTES, S.A.**, con NIF A95000295, por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructor/a a ***B.B.B.*** y, como secretario/a, a ***C.C.C.***, indicando que podrán ser recusados, 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).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: 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, la sanción que pudiera corresponder sería, sin perjuicio de lo que resulte de la instrucción:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía **140.000,00 euros**

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía **60.000,00 euros**

La suma de ambas cuantías hace un total de **200.000 € (DOSCIENTOS MIL EUROS).**

QUINTO: NOTIFICAR el presente acuerdo a **TOTALENERGIES CLIENTES, S.A.**, con NIF A95000295, 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 expediente 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 sanción quedaría establecida en **160.000,00 euros**, 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, la sanción quedaría establecida en **160.000,00 euros** y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

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 sanción quedaría establecido en **120.000,00 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.

Asimismo, con el fin de prevenir ulteriores infracciones de la misma naturaleza, el reconocimiento de responsabilidad y la consiguiente aplicación de la mencionada reducción implicará la aceptación, en su caso, de las medidas a adoptar propuestas e indicadas por esta entidad en el presente acuerdo.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (160.000,00 euros o 120.000,00 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00 0000 0000 0000 0000 0000 (BIC/Código SWIFT: XXXXXXXXXXX)*** 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 doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo sin que se haya dictado y notificado resolución se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

De conformidad con lo establecido en el artículo 76.4 de la LOPDGDD y si el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta.

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.

935-30102023

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

>>

SEGUNDO**:** En fecha 31 de enero de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **120000 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.

CUARTO: En el Acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá “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…”.

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el Acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

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, 48.1, 64.2 y 68.1 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
Terminación del procedimiento

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 **EXP202301331**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a **TOTALENERGIES CLIENTES, S.A.** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del Acuerdo de inicio transcrito en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a **TOTALENERGIES CLIENTES, 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.

1259-16012024

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