- **Expediente N.º:**

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 agosto de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***ENDESA ENERGÍA, S.A.U.*** (en adelante la parte reclamada). Notificado el acuerdo de inicio y tras analizar las alegaciones presentadas, con fecha 14 de noviembre de 2022, se emitió la propuesta de resolución que a continuación se transcribe:

<<

Expediente N.º: EXP202200455

PROPUESTA DE RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***D. A.A.A.*** (en adelante, la parte reclamante), en fecha 21 de diciembre de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ENDESA ENERGÍA, S.A.U. con NIF A81948077 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

El reclamante manifiesta que, en fecha 16 de diciembre de 2021, recibió en su domicilio la factura del contrato que mantiene desde hace años con la entidad reclamada, a nombre de una tercera persona (su sobrina) y que, tras contactar con la reclamada, se le informó que un tercero había cambiado la titularidad del contrato, sin su consentimiento.

Junto a la reclamación aporta factura de diciembre de 2021 dirigida a su sobrina y extracto bancario, de noviembre de 2021, con el cargo en su cuenta bancaria.

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), mediante notificación electrónica, fue recibido en fecha 18 de enero de 2022, como consta en el certificado que obra en el expediente.

En respuesta a la solicitud de ampliación del plazo de un mes que le fue otorgado para que procediera al análisis de la reclamación presentada, en fecha 3 de febrero de 2022, se acordó su ampliación hasta un máximo de 10 días hábiles.

En fecha 4 de marzo de 2022, se recibe en esta Agencia escrito de respuesta en el que se indica que en fecha 16 de diciembre de 2021, el reclamante recibió en su domicilio la factura de un contrato con Endesa Energía, a nombre de una tercera persona, asociado al punto de suministro en el que su padre, ***B.B.B.*** y en cuyo nombre actúa ***A.A.A.***, era titular de un contrato con la sociedad Energía XXI Comercializadora de referencia S.L.U. (en adelante, "Energía XXI"), de cuyo pago era titular el propio ***A.A.A..***
Manifiesta que tal y como aparece reflejado en los sistemas internos de Endesa Energía, con fecha 21 de octubre de 2021, el canal de venta de Endesa Energía "Agentes Comerciales" contactó telefónicamente con ***C.C.C.***, a través del proveedor Energía Andalucía Oriental, S.L.U. (en adelante, "EAO"), quien, bajo un contrato de prestación de servicios de telemarketing y actuando en calidad de encargado del tratamiento, realiza llamadas de captación a potenciales clientes que previamente han prestado su consentimiento expreso para ello, mediante la oferta de productos y servicios de Endesa Energía y Endesa X.

Expone que Endesa Energía ha detectado un comportamiento anómalo por parte de su empleada ya que, según ha podido averiguarse, la operadora no aportó el SMS correcto con la confirmación de contratación de ***C.C.C.***, puesto que no se correspondía con el número de teléfono confirmado en la llamada por ***C.C.C..*** En el presente caso, la operadora llevó a cabo un cambio de titularidad y de compañía comercializadora, en un punto de suministro del que no era titular la persona en cuyo nombre se dio de alta el contrato y, además, aportó un SMS certificado no válido, como aceptación de la contratación.

Por último, se indica que, si bien la incidencia fue ocasionada por el proceder individual de una operadora que se apartó del procedimiento, desde la Oficina del Delegado de Protección de Datos de Endesa se ha instado a Endesa Energía a que, sin perjuicio de las auditorías ordinarias que lleva a cabo, refuerce, aún más, los controles respecto a las acciones llevadas a cabo por el proveedor EAO. Asimismo, se ha recomendado a Endesa Energía que envíe una amonestación a EAO indicando la gravedad de los hechos ocurridos y el perjuicio ocasionado al interesado.

TERCERO: En fecha 21 de marzo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: En fecha 8 de agosto de 2022***,*** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en

adelante, LPACAP), por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

El acuerdo de inicio fue enviado, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibido en fecha 10 de agosto de 2022, como consta en el certificado que obra en el expediente.

QUINTO: En respuesta a la solicitud de ampliación del plazo para presentar alegaciones, en fecha 11 de agosto de 2022, se acordó su ampliación hasta un máximo de 5 días.

En respuesta al escrito solicitando copia del expediente referenciado, en fecha 19 de agosto de 2022, se dio acceso al mismo.

SEXTO: Notificado el citado acuerdo de inicio 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), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que no cabe apreciar antijuricidad en la conducta de Endesa Energía por cuanto se limitó a atender las distintas solicitudes de contratación de ***C.C.C.,*** entre la que se encontraba la correspondiente a la vivienda sita en ******DIRECCION.1***, y a facilitar los trámites correspondientes para permitir el cambio de titularidad del contrato de acceso, siguiendo con los protocolos establecidos, sin que ello conllevara permitir el acceso a los datos personales del titular original del contrato de acceso.

Señala que las medidas de seguridad que Endesa Energía desplegó para garantizar la protección de los datos personales de los interesados, funcionaron correctamente puesto que ningún dato personal de ningún tercero fue revelado, y el hecho de que se produjera una incidencia en la tramitación de la contratación al aportarse un SMS certificado de confirmación no válido y la venta siguiera su curso, no implica que Endesa Energía carezca de protocolos o procedimientos de actuación y que las medidas de seguridad no hayan sido adecuadas para garantizar la protección de los datos de carácter personal de sus clientes, significa, simple y llanamente, que una operadora se apartó del procedimiento establecido, aportando un SMS certificado correspondiente a un número de teléfono de otra venta, sin que ello, en cualquier caso, haya ocasionado que ningún dato personal de los clientes se hayan visto desprotegidos.

Subsidiariamente, para el supuesto de que no se atienda la petición principal, solicita, una reducción de la sanción inicialmente fijada, teniendo en cuenta las circunstancias atenuantes, concretamente, las medidas adoptadas para paliar cualquier posible perjuicio en el reclamante o en la persona en cuyo nombre actúa, así como para evitar que se produzcan sucesos similares en el futuro; y la gravedad y carácter episódico de la presunta infracción, toda vez que se iniciaron los trámites necesarios para facilitar la reposición del contrato de suministro de electricidad de la vivienda en cuestión con la anterior compañía comercializadora, así como la anulación de las tres facturas emitidas por el consumo de energía durante el tiempo en que el contrato objeto de reclamación estuvo activo.

Por último, señala que se han reforzado los protocolos de actuación del canal de venta “Agentes Comerciales” y que los hechos reclamados responden a un acontecimiento aislado y puntual, en el que sólo se ha visto afectada una persona que además mantuvo el suministro de electricidad, sin tener que abonar factura alguna por la energía consumida y que se ha producido un fallo en el trámite de la contratación, al aportar un SMS certificado de confirmación no válido.

Se aporta grabación de la llamada telefónica realizada por el proveedor Energía Andalucía Oriental, S.L.U.

SÉPTIMO: En consecuencia, no habiendo solicitado práctica de pruebas, se tiene por incorporada a efectos probatorios la documentación facilitada por el reclamante, así como las alegaciones al acuerdo de inicio, documentación toda ella de la que ya dispone el reclamado.

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

HECHOS PROBADOS

PRIMERO: Consta que la parte reclamante fue titular de un contrato de suministro de electricidad con la compañía Energía XXI asociado al punto de suministro sito en ******DIRECCION.1***.

SEGUNDO: Se constata que la operadora llevó a cabo un cambio de titularidad y de compañía comercializadora, en un punto de suministro del que no era titular la persona en cuyo nombre se dio de alta el contrato, aportando un SMS certificado no válido, como aceptación de la contratación.

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, 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

En respuesta a las alegaciones presentadas por la entidad reclamada se debe señalar lo siguiente:

En el presente caso, en fecha 21 de octubre de 2021, el canal de venta de Endesa Energía “Agentes Comerciales” contactó telefónicamente con ***C.C.C.***, con la finalidad de ofrecerle una bonificación en la contratación de la tarifa eléctrica. De esta forma, se solicitó a través del canal telefónico, el alta en el suministro eléctrico para la vivienda de la parte reclamante, que fue tramitada bajo la modalidad “C2- Cambio de comercializador con modificaciones en el contrato de acceso”*,* de conformidad con lo contenido en la Resolución de la CNMV, de 17 de diciembre de 2019.

Respecto a las obligaciones que la parte reclamada aduce para el cumplimiento de la normativa específica del sector eléctrico, esta instrucción nada tiene que decir más allá de que las mismas no pueden suponer en ningún caso una vulneración del resto de la normativa aplicable.

El protocolo para la gestión de cambio de comercializadora con cambio de titular atribuye a la comercializadora entrante la condición de único interlocutor del cliente y la responsabilidad de ejecutar todas las actuaciones que fueran necesarias para la gestión del cambio.

En este sentido, no se puede aceptar que, aun con el fin de cumplir con lo allí establecido, se proceda a obviar el necesario cumplimiento de la normativa en materia de protección de datos personales.

A estos efectos, la Ley 24/2013, de 26 de diciembre, del Sector eléctrico (en adelante, “Ley del Sector Eléctrico”), establece el derecho del consumidor a cambiar de empresa comercializadora conforme a lo establecido en las directivas europeas del mercado interior de electricidad.

Para ello, la normativa establece el proceso general que debe llevarse a cabo entre la nueva comercializadora o comercializadora entrante, la distribuidora y comercializadora existente o comercializadora saliente. Dicho cambio implica el alta de un nuevo contrato de suministro energético con la comercializadora entrante y la baja del contrato existente con la comercializadora saliente, mediante un agente que ejecuta el cambio, que es la distribuidora.

El artículo 46 de la Ley del Sector Eléctrico establece entre las obligaciones de los comercializadores, en su apartado 1 letra g) la *de “Formalizar los contratos de suministro con los consumidores de acuerdo con la normativa reglamentaria que resulte de aplicación”*. La mención por la Ley de la obligación de formalizar el contrato entre las obligaciones de los comercializadores pone de manifiesto que corresponde a la comercializadora y, en un caso de cambio de comercializadora, a la comercializadora entrante, comprobar la identidad y la voluntaria, correcta e informada prestación del consentimiento por parte del consumidor, que es su contraparte en el contrato de suministro.

En este sentido, la nueva comercializadora (la parte reclamada) tendrá que gestionar la baja del contrato del reclamante con su comercializadora saliente, que se efectúa tratando sus datos personales.

Trasladando estas consideraciones al caso presente, y habiendo quedado acreditado que la reclamada trató los datos personales del reclamante, tal y como consta en el expediente, la parte reclamada no cumplió sus obligaciones con la diligencia debida,

por cuanto, antes de activar el procedimiento de cambio de comercializadora, debería haber recabado un SMS certificado de confirmación válido.

Y es que, tal y como consta en el expediente, la conducta de la parte reclamada conllevó la vulneración del artículo 32 del RGPD, al llevar a cabo un cambio de titularidad y de compañía comercializadora, en un punto de suministro del que no era titular la persona en cuyo nombre se dio de alta el contrato aportando un SMS certificado no válido, como aceptación de la contratación. Con ello, no se comprobó adecuadamente la identidad de la persona que solicitó la modificación del contrato.

El propio reclamado en escrito de fecha 4 de marzo de 2022 ha manifestado que:

"(…) *EAO ha trasladado a Endesa Energía que ha detectado un comportamiento anómalo por parte de su empleada ya que, según ha podido averiguarse, la operadora no aportó el SMS correcto con la confirmación de contratación de la Sra. C.C.C., puesto que no se correspondía con el número de teléfono confirmado en la llamada por la Sra. C.C.C., (…)"*

Por tanto, pese a las medidas de seguridad existentes, los datos personales de la parte reclamante fueron tratados por la entidad reclamada al emitir y enviar a su domicilio la factura de un contrato, a nombre de una tercera persona. Es decir, se ha producido una falta de medidas de seguridad en la comprobación de los datos de la persona que solicitó la modificación del contrato, por lo que la teleoperadora en ese momento en el que se estaban verificando los datos para proceder a la contratación del suministro eléctrico con el contratante, debió ser diligente adoptando las cautelas necesarias y pertinentes.

Erra la reclamada al afirmar que, simple y llanamente, una operadora se apartó del procedimiento establecido, aportando un SMS certificado correspondiente a un número de teléfono de otra venta ya que las medidas de seguridad deben adoptarse en atención a todos y cada uno de los riesgos presentes en un tratamiento de datos de carácter personal, incluyendo entre los mismos, el factor humano.

El Tribunal Supremo (Sentencias de 16 y 22/04/1991) considera que del elemento culpabilista se desprende *"... que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."*

Por su parte, la Audiencia Nacional, en Sentencia de 29/06/2001, en materia de protección de datos de carácter personal, ha declarado que *"... basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."*.

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido y la profesionalidad exigible al infractor. En este sentido la Sentencia de 05/06/1998 exige a los profesionales del sector *"...un deber de conocer especialmente las normas aplicables".* En similares términos se pronuncian las Sentencias de 17/12/1997, 11/03/1998, 02/03 y 17/09/1999.

Aplicando la anterior doctrina, la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14/02/ y 20/09/2002 y 13/04/2005, exige a las entidades que operan en

el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de los mismos, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren estos, por lo que sus depositarios deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

A este respecto, la parte reclamada incumplió el mandato legal establecido en el artículo 32 del RGPD ya que las medidas de seguridad no fueron las adecuadas para garantizar la protección de los datos de carácter personal de sus clientes y deben ser mejoradas tras haber quedado constatado que no han sido suficientes para evitar los hechos denunciados.

También invoca el reclamado la minoración de la cuantía de la sanción reduciendo la misma.

A este respecto hay que reseñar que teniendo en cuenta que se trata de una infracción calificada como grave y que de conformidad con el artículo 83.4 del RGPD puede ser sancionada *"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,"* ya se aplica una importante minoración de esta.

La STS, Sala 3ª, de 16 de diciembre de 2003 (Rec. 4996/98) ya señalaba que el principio de proporcionalidad de las sanciones exige que *"la discrecionalidad que se otorga a la Administración para la aplicación de la sanción se desarrolle ponderando en todo caso las circunstancias concurrentes, al objeto de alcanzar la debida proporcionalidad entre los hechos imputados y la responsabilidad exigida".*

Principio de proporcionalidad que no se entiende vulnerado, considerándose proporcionada la sanción propuesta a la entidad, por los hechos probados y ponderadas las circunstancias concurrentes, que se detallan más adelante.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

III
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que ENDESA ENERGÍA, S.A.U. es una empresa del sector del comercio de energía eléctrica que, para el desarrollo de su actividad de producción y servicios eléctricos, realiza tratamientos de datos personales.

Realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD:

«responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios es-*

pecíficos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales*" (en adelante brecha de seguridad) como "*todas aquellas violaciones de la seguridad que ocasionen 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.*"

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, toda vez que la entidad reclamada ha permitido el acceso a los datos personales de un cliente sin su consentimiento al llevar a cabo un cambio de titularidad y de compañía comercializadora, en un punto de suministro del que no era titular la persona en cuyo nombre se dio de alta el contrato, aportando además un SMS certificado no válido, como aceptación de la contratación.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en el artículo 32 del RGPD, que reglamenta la seguridad del tratamiento.

IV
Artículo 32 del RGPD

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, 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 Considerando 74 del RGPD establece:

"*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas."*

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán 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, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse 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 tendrán 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.

En este mismo sentido 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".

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

En el caso concreto que se examina, fallaron las medidas de seguridad al tramitar la modificación del contrato sin comprobar adecuadamente la personalidad de quien solicitaba el cambio, logrando llevar a cabo un cambio de titularidad y de compañía comercializadora, en un punto de suministro del que no era titular la persona en cuyo nombre se dio de alta el contrato, aportando además un SMS certificado no válido, como aceptación de la contratación.

Los hechos conocidos son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD, ya que las medidas de seguridad de la entidad reclamada no son adecuadas para garantizar la protección de los datos de carácter personal de sus clientes y deben ser mejoradas tras haber quedado constatado que no han sido suficientes para evitar los hechos denunciados.

Por tanto, los hechos acreditados son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

V

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone 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."

VI
Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III, relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28, bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad constituye el elemento de la culpabilidad.

VII
Sanción

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

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. 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 nú-

mero 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,
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."

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo con 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."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 32, procede graduar la multa teniendo en cuenta:

Como agravantes:

Artículo 76.2 b) LOPDGDD:" La vinculación de la actividad del infractor con la realización de tratamientos de datos personales".

La actividad empresarial de la entidad reclamada exige un continuo tratamiento de datos de carácter personal, tanto de clientes como de terceros. Asimismo, la entidad reclamada realiza para el desarrollo de su actividad, un elevado volumen de tratamiento de datos personales ya que se trata de una de las mayores empresas del país en su sector de negocio o actividad.

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa es de 50.000 € por infracción del artículo 32 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales.

VIII
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.

Se advierte que no atender a los requerimientos de este organismo puede 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.

A la vista de lo expuesto se procede a emitir la siguiente

PROPUESTA DE RESOLUCIÓN

Que por la Directora de la Agencia Española de Protección de Datos se sancione a ENDESA ENERGÍA, S.A.U., con NIF A81948077, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, con una multa de 50.000,00 euros y ordene la implantación de las medidas correctoras que impidan que en el futuro se repitan hechos similares.

Asimismo, de conformidad con lo establecido en el artículo 85.2 de la LPACAP, se le informa que podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá una reducción de un 20% del importe de esta. Con la aplicación de esta reducción, la sanción quedaría establecida en 40.000,00 euros y su pago implicará la terminación del procedimiento. La efectividad de esta reducción 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 la cantidad especificada anteriormente, de acuerdo con lo previsto en el artículo 85.2 citado, deberá hacerla efectiva mediante su ingreso en la cuenta restringida nº ***IBAN: 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, por pago voluntario, de reducción del importe de la sanción. Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para proceder a cerrar el expediente.

En su virtud se le notifica cuanto antecede, y se le pone de manifiesto el procedimiento a fin de que en el plazo de DIEZ DÍAS pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP.

926-181022

R.R.R.
INSTRUCTOR/A

>>

SEGUNDO**:** En fecha 23 de noviembre de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **40000 euros** haciendo uso de la reducción prevista en la propuesta de resolución transcrita anteriormente.

TERCERO: El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere la propuesta de resolución.

CUARTO: En la propuesta de resolución transcrita anteriormente se constataron los hechos constitutivos de infracción, y se propuso que, por la Directora, se impusiera al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa, 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…".*

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

SEGUNDO: REQUERIR a ***ENDESA ENERGÍA, S.A.U.*** para que en el plazo de un mes notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho de la propuesta de resolución transcrita en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a ***ENDESA ENERGÍA, S.A.U.***.

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.

1331-281122

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