- **Procedimiento Nº: EXP202207418 (PS/0680/2022)**

RESOLUCION DEL PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 11/06/22, ***Dª. A.A.A.*** (en adelante, la parte reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos. contra la entidad, HOLALUZ-CLIDOM, S.A., CIF.: A65445033, (en adelante, la parte reclamada o CLIDOM), por la presunta vulneración de la normativa de protección de datos: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/16, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La reclamación se expresa en los siguientes términos:

> *"El día 7 de Abril de 2022, veo un cargo en mi cuenta de ***CANTIDAD.1 de una compañía de luz que desconocía (más del doble de lo que suelo pagar) y devuelvo el recibo ya que pienso que es una estafa. Inmediatamente llamo a la inmobiliaria y les pregunto que, si ellos saben algo sobre esto, y me dicen que sí, que es un cambio masivo que han realizado a todos los inquilinos para que figure la luz a nuestro nombre. Lo que yo les respondo que a mí no se me ha informado de dicho cambio y mucho menos he dado yo mi consentimiento para que me cambien de compañía y hagan un contrato a mi nombre.*
>
> *Intercambio una serie de email con ellos, en los cuales siempre se acogen a que es una práctica legal (que puede ser) pero yo lo que les digo es por qué no me avisaron del cambio y porque no esperaron a mi consentimiento. Yo les comento que yo pago la parte proporcional a lo que he estado pagando hasta el momento y ellos ni contestan a eso.*
>
> *Llame a Holaluz comentándoles el incidente y pidiéndole el contrato de luz que supuestamente yo había firmado y me enviaron el contrato, entonces fue cuando vi que le habían firmado por mí, sin mí consentimiento, una tal **B.B.B.**".*

Al escrito de reclamación, se acompaña la siguiente documentación:

- Copia del contrato de arrendamiento fechado el 24/05/21, donde figura como arrendador: ***D. C.C.C.,*** y como arrendataria: ***Dª A.A.A.***, del domicilio sito en Madrid, ******DIRECCIÓN.1***. En dicho contrato figura como mandatario verbal, ***D.D.D.***, con domicilio en ***DIRECCIÓN.2.

    - De las Cláusulas del contrato, tienen relevancia para el presente caso, la cláusula Nº 5 "GASTOS", la cual indica que: *"Serán de cuenta del Arrendatario los gastos relativos al consumo de luz, agua y teléfono, así*

como cualquier otro servicio de comunicaciones o televisión que contrate el Arrendatario".

- Copia del intercambio de una serie de correos electrónicos que se realizaron el día 11/04/22, entre la arrendataria y la representante de la inmobiliaria ENFO-KA, donde la arrendataria pide explicaciones del porqué la han cambiado de compañía eléctrica sin su consentimiento y su deseo de volver a la antigua compañía eléctrica (Iberdrola).

  - En las Condiciones Particulares del nuevo contrato de suministro eléctrico con CLIDOM se puede leer, entre otras, lo siguiente:

    - Datos del Cliente: ***A.A.A.***; NIF: ******NIF.1***; Teléfono: ******TELÉFONO.1***; Dirección: ******DIRECCIÓN.1***; e-mail: ******EMAIL.1*** .Domiciliación banca-ria: ***(...).***

    - Datos del firmante del contrato: ***B.B.B.*** NIF: ******NIF.2*** Fecha contrato: 24/02/22***.***

SEGUNDO: Con fecha 08/07/22, de conformidad con lo estipulado en el artículo 65.4 de la LOPDGDD, por parte de esta Agencia, se dio traslado de dicha reclamación a la inmobiliaria, ENFOKA SISTEMAS GLOBALES, S.L. (ENFOKA) y a la comercializadora de electricidad, CLIDOM, para que procediesen a su análisis e informasen, en el plazo de un mes, sobre lo que se exponía en el escrito de reclamación.

TERCERO: Con fecha 21/07/22, la inmobiliaria ENFOKA envía a esta Agencia escrito de contestación a la solicitud realizada, en el cual manifiesta, entre otras cuestiones que, en cumplimiento de lo establecido en la LAU y el contrato de arrendamiento, se instó a la arrendataria en numeras ocasiones para que modificase el suministro eléctrico, todas ellas sin éxito. Por ello, en el mes de febrero se la envió un e-mail informando del cambio de compañía y comunicando los datos de la arrendataria a la empresa Runup Business, S.L. (QLIP), perteneciente al canal externo de captación de clientes de CLIDOM.

CUARTO: Con fecha 09/08/22, la entidad CLIDOM envía a esta Agencia escrito de contestación a la solicitud realizada, en el cual manifiesta, como datos a tener en cuenta, los siguientes:

- Que, según la base de datos de CLIDOM, la reclamante consta de alta en la empresa con el CUPS1 ***(...)***, ******DIRECCIÓN.1*** desde el 26/02/22 hasta el 31/03/22. Dicha alta fue llevada a cabo por parte del canal comercial Run Up Business SL con el que CLIDOM mantiene una relación contractual.

  Los comerciales están facultados para subcontratar a cualesquiera otras personas o compañías para prestar los servicios. En el presente caso consta que la empresa subcontratada fue ENFOKA Sistemas Globales, S.L. y que debido a que el colaborador aparentó la veracidad de la contratación no se pudo detectar, hasta que la reclamante no lo manifestó, que dicha contratación había sido realizada sin el consentimiento de la misma.

- Que CLIDOM realiza de forma aleatoria una posterior revisión de la calidad de las llamadas y las altas realizadas por los nuevos colaboradores, mediante un protocolo de revisión de un determinado porcentaje de las altas donde CLIDOM se cerciora de que los clientes efectivamente han mostrado su consentimiento a realizar el cambio de comercializadora o el alta de suministro.

- Que la introducción de los datos personales del Cliente fue realizada por un tercero que incumplió con las obligaciones contractuales establecidas, siendo el mismo el responsable de cualquier perjuicio que se derive del incumplimiento.

Junto al escrito de contestación, la entidad CLIDOM acompaña la siguiente documentación:

- Contrato de Promoción de "Contratos de Suministro de Energía Eléctrica y Gas Natural" entre CLIDOM y QLIP, de fecha 24/08/21.

QUINTO: Con fecha 11/09/22, por parte de la Directora de la Agencia Española de Protección de Datos se dicta acuerdo de admisión de trámite de la reclamación presentada, de conformidad con el artículo 65 de la Ley LPDGDD, al apreciar posibles indicios racionales de una vulneración de las normas en el ámbito de las competencias de la Agencia Española de Protección de Datos.

SEXTO: Con fecha 26/01/23, por parte de la Directoria de la Agencia Española de Protección de Datos, se inicia procedimiento sancionador a la entidad CLIDOM, al apreciar indicios razonables de vulneración de lo establecido en el artículo 25 del RGPD, imponiendo una sanción inicial de 100.000 euros (cien mil euros).

Además, como medidas a implantar, se le indicaba que, en la resolución que se adoptase, esta Agencia podría requerir a la entidad para que, adecuase a la normativa de protección de datos personales las operaciones de tratamiento que realiza y el procedimiento mediante el que los mismos prestan su consentimiento para la recogida y tratamiento de sus datos personales.

SÉPTIMO: Con fecha 15/02/23, la entidad CLIDOM presenta escrito de alegaciones a la incoación del expediente en el cual manifiesta, como datos a tener en cuenta, los siguientes:

- Que, en relación a la posible vulneración del principio de protección de datos, si bien es cierto que CLIDOM responde y se identifica con las definiciones referidas al responsable de tratamiento en los artículos 4 y 24.1 del RGPD, lo es ante la relación contractual que existe con QLIP, a los efectos del contrato de servicios firmado con éste en fecha 24 de agosto de 2021 para la realización de servicios de promoción de contratos de suministro de energía eléctrica y captación de potenciales clientes.

- Que el contrato que se firmó entre las dos partes, CLIDOM, como responsable del tratamiento, incluyó, como obligación contractual a QLIP, en calidad de encargado de tratamiento, la responsabilidad proactiva de recoger el

consentimiento de los interesados de conformidad con las exigencias del RGPD y por ello, recae en el Colaborador hacer las comprobaciones pertinentes en relación con la identidad del consumidor y de su voluntad de contratar.

- Que el subencargado de QLIP, la inmobiliaria ENFOKA, actuó en contra de las instrucciones de CLIDOM en cuanto a la obligación de recabar el consentimiento de los interesados ya que, éste suplantó la identidad de la afectada y, además, firmó un consentimiento no válido sin que pudiera cumplir con los principios de transparencia, libertad y consentimiento expreso, siendo QLIP plenamente responsable de las actuaciones negligentes de su proveedor.

- Que, en relación al cumplimiento de lo dispuesto en el artículo 25.1 RGPD, en lo que respecta a la aplicación de medidas técnicas y organizativas para comprobar la recogida del consentimiento válido de los datos personales de los interesados, CLIDOM dispone de un sistema de calidad y autenticación en relación a la identidad de sus clientes finales mediante un protocolo de revisión de un determinado porcentaje significativo de altas de usuarios finales, especialmente cuando éstos proceden de canales indirectos a CLIDOM. Si bien por razones de volumetría, no se solicitan la totalidad de las autorizaciones.

Junto al escrito de alegaciones, la entidad CLIDOM acompaña los siguientes documentos:

- Contrato de Promoción de “Contratos de Suministro de Energía Eléctrica y Gas Natural” entre CLIDOM y QLIP, de fecha 24/08/21.

- Informe análisis de la necesidad de realizar una evaluación de impacto, de fecha 12/09/22.

- Evaluación de Impacto de privacidad “Gestión de Clientes”.

- Controles derivados de la evaluación de impacto de privacidad de la actividad de «Gestión de Clientes»

OCTAVO: Con fecha 06/04/23, se notifica a la entidad reclamada la propuesta de resolución en la cual, se proponía que, por la Directora de la Agencia Española de Protección de Datos se procediese al ARCHIVO del presente procedimiento sancionador a la entidad, HOLALUZ-CLIDOM, S.A., CIF.: A65445033 con arreglo a lo dispuesto en los artículos 63.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), pues, según se desprende de la relación contractual que existe entre CLIDOM y QLIP, se incluía, como obligación contractual de QLIP, en calidad de encargado de tratamiento, la responsabilidad proactiva de recoger el consentimiento de los interesados de conformidad con las exigencias del citado RGPD, incumpliendo, en este caso, el contrato de encargo firmado con CLIDOM.

NOVENO: Con fecha 10/07/23, por parte de la Directora de la Agencia de la Agencia Española de Protección de Datos se notifica a la parte reclamada la concesión de un plazo de quince días, de acuerdo con el artículo 90.2 de la LPACAP, para que pudiera alegar cuanto considerase en su defensa por la presunta infracción del artículo 25 del RGPD, al considerar, en este caso que, cuando se realizó el cambio de contratación del servicio a nombre de la inquilina, CLIDOM, no realizó las comprobaciones necesarias para corroborar si la reclamante había consentido en realizar el cambio de compañía eléctrica, sobre todo después de que el contrato de cambio de compañía viniese firmado por otra persona ajena a la inquilina, sin justificar representación alguna y dándose el hecho significativo de que esta persona pertenecía a la inmobiliaria ENFOKA, subcontrata de la entidad QLIP.

DÉCIMO: Con fecha 02/08/23, CLIDOM presenta escrito de alegaciones en el cual, entre otras, indica lo siguiente:

> *"Primera.- Defecto de forma.: En fecha 6 de abril de 2023 CLIDOM recibió Propuesta de resolución del procedimiento sancionador con número de procedimiento EXP202207418 (PS/0680/2022) con la siguiente propuesta de resolución por parte del instructor del procedimiento: "Que por la Directora de la Agencia Española de Protección de Datos se proceda al ARCHIVO del presente procedimiento sancionador a la entidad, HOLALUZ- CLIDOM, S.A., CIF.: A65445033 con arreglo a lo dispuesto en los artículos 63.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), por la presunta infracción del artículo 25 del RGPD, 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 hábiles pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 en relación con el art. 82.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas."*
>
> *Dicha propuesta dictaminó el archivo del procedimiento sancionador por la presunta infracción del artículo 25 del RGPD, otorgando un plazo de 10 días para que CLIDOM pudiera alegar las oportunas alegaciones para su defensa así como los pertinentes documentos. Siendo CLIDOM receptora y notificada de la misma sin proceder a aportar alegaciones al estar conforme con la propuesta de resolución de archivo, dado que se probó que no existía ningún tipo de incumplimiento por parte de CLIDOM.*
>
> *Que el artículo 63.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) determina lo siguiente: "No se podrán iniciar nuevos procedimientos de carácter sancionador por hechos o conductas tipificadas como infracciones en cuya comisión el infractor persista de forma continuada, en tanto no haya recaído una primera resolución sancionadora, con carácter ejecutivo", parte de un defecto de forma ante la justificación de la reapertura del procedimiento sancionador notificado en fecha 4 de julio de 2023 puesto que como el propio artículo dice, no será posible iniciar un nuevo procedimiento sancionador cuando todavía no se ha finalizado el procedimiento que se halle en tramitación. En el caso concreto, existió notificación fehaciente del archivo del*

proceso por no existir evidencias de la vulneración de la Ley de Protección de Datos tras aportar todas las pruebas y aclaraciones pertinentes, concurriéndose pues, al correspondiente archivo y comunicación de la propuesta de resolución.

Atendiendo a la presente alegación, y de conformidad con el artículo 76 de la LPACAP, CLIDOM presenta el presente escrito de alegaciones por motivos de defecto de forma atendiendo a la reapertura del procedimiento sancionador sin que el fundamento jurídico alegado por la presente Administración esté debidamente justificado y fundamentado, teniendo en cuenta que la base jurídica que alega la misma se basa en el artículo 90.2 de la LPACAP. Dicho artículo viene a referirse que "[...] el órgano competente para resolver un procedimiento considere que la infracción o la sanción revisten de mayor gravedad que de la determinada en la propuesta de resolución, se notificará al inculpado para que aporte cuantas alegaciones estime convincente en el plazo de 15 días".

El procedimiento de reapertura vuelve a realizar las mismas alegaciones y aporta los mismos fundamentos jurídicos que se reflejaban en el procedimiento sancionador archivado en fecha 6 de abril de 2023, produciéndose así una inseguridad jurídica en el archivo de las actuaciones dado que ya han sido archivadas por no existir incumplimiento por parte de CLIDOM reflejándose el mismo análisis de gravedad en ambos procedimientos. En otras palabras, en ambos procedimientos se reiteran los mismos fundamentos por parte de la Administración y, en consecuencia, se mantiene el mismo nivel de gravedad que previamente se reflejó en el procedimiento de propuesta de resolución, careciendo de validez el artículo 90.2 LPACAP, al no analizarse y concluirse una gravedad mayor en el procedimiento de reapertura.

Dicho todo lo anterior, CLIDOM considera y defiende que existe un defecto de forma de la interpretación del artículo 90.2 aplicado en el procedimiento sancionador de reapertura.

Asimismo, de forma análoga para el presente supuesto, esta parte entiende que debe aplicar el mismo razonamiento que para el principio de non bis in ídem, que se incardina del art. 25 de la Constitución Española. El principio de non bis in ídem, en su aplicación a la potestad sancionadora de la Administración, establece que no pueden sancionarse los hechos que hayan sido sancionados penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento. Así, impone evitar la duplicidad de sanciones por los mismos hechos (STC 2/1981, 30 de Enero de 1981).

En su vertiente procesal, este principio proscribe la dualidad de procedimientos o procesos, en caso de concurrir la triple identidad ya expuesta, lo que supone que, anulada una sanción por razón de fondo o por lesión de derecho fundamental, no cabe incoar un nuevo procedimiento sancionador, aunque se halle abierto el plazo de prescripción (STS 7-3-16, EDJ 16512).

En esta línea, los hechos que el instructor del expediente pretende reabrir se encontraban incluidos en el escrito de alegaciones presentado por CLIDOM del

cual se derivó el archivo del expediente. La presente resolución vulneraría el principio de non bis in ídem porque dota del contenido archivado a un nuevo expediente, que recibe en su seno los mismos hechos que eran objeto del proceso anterior y que ya se descartó que pudieran ser constitutivos de infracción. Sin embargo, pese a considerar que existe un defecto de forma, de forma subsidiaria, a continuación CLIDOM procede a reiterar los siguientes argumentos de defensa vertidos en el anterior escrito de alegaciones:

Segunda.- El Acuerdo de Inicio establece, como supuesta infracción, la posible vulneración del artículo 25 del RGPD en base a que CLIDOM realizara un tratamiento de los datos personales de la reclamante sin corroborar previamente la acreditación de la representación de quien le proporcionó los datos, o comprobar, por cualquier medio, que la reclamante consintiera efectivamente, realizar el cambio de compañía eléctrica o que consintiera que se pudiera realizar un tratamiento de sus datos personales para ese fin.

El artículo aludido regula la protección de datos desde el diseño y por defecto, es decir que el responsable debe aplicar, tanto en el momento de establecer los medios de tratamiento como en el momento del tratamiento mismo, todas aquellas medidas técnicas y organizativas adecuadas y concebidas para aplicar, de manera efectiva, los principios de protección de datos e integrar, en el tratamiento, las garantías necesarias para cumplir los requerimientos que nos señala el RGPD; además, el responsable debe aplicar las citadas medidas para garantizar que, por defecto, sólo se tratan los datos personales necesarios para cada finalidad específica del tratamiento.

Que, en relación a la posible vulneración del principio de protección de datos desde el diseño, si bien es cierto que CLIDOM responde y se identifica con las definiciones referidas al responsable de tratamiento en los artículos 4 y 24.1 del RGPD, lo es ante la relación contractual que existe con Runup Business SL (en adelante, "QLIP") a los efectos del contrato de servicios firmado con éste en fecha 24 de agosto de 2021 para la realización de servicios de promoción de contratos de suministro de energía eléctrica y captación de potenciales clientes, que se adjunta para que conste a los efectos oportunos como Documento número 1. Para el cumplimiento del contrato, se requiere el tratamiento de datos de personas físicas, pues QLIP debe captar potenciales clientes para que éstos se den de alta a los servicios de suministros energéticos de CLIDOM.

No obstante lo anterior, es importante incidir que, en el contrato que se firmó entre las dos partes, CLIDOM, como responsable del tratamiento, incluyó, como obligación contractual a QLIP, en calidad de encargado de tratamiento, la responsabilidad proactiva de recoger el consentimiento de los interesados de conformidad con las exigencias del RGPD. En concreto, en la cláusula séptima del contrato, titulado "obligaciones del colaborador" se detalla lo siguiente: "(…) En el ejercicio de su actividad, el Colaborador debe actuar lealmente y de buena fe, velando por los intereses de Holaluz. Así, el Colaborador desarrollará su actividad con arreglo a las prácticas habituales de la industria y usos de comercio, procurando en todo momento que la información y el asesoramiento que suministre a los Clientes Potenciales sea veraz y acorde con las prácticas

empresariales de la más alta categoría. Asimismo, Holaluz requiere que el Colaborador, al ser un principal aliado en el desarrollo del negocio, adopte sus conductas conforme con los principios generales del Código Ético. Por ello, mediante la firma del presente Contrato, el Colaborador se adhiere al Código Ético de Holaluz y se compromete a adecuar las pautas de conducta establecidas en el mismo. El incumplimiento del Código Ético se considera muy grave en Holaluz y comportará las consecuencias previstas en el presente Contrato." [.....] "En especial, deberá asumir las siguientes obligaciones para la prestación del Servicio: (i) Ocuparse con la diligencia de un ordenado empresario en la prestación del Servicio entre los Clientes Potenciales, cumpliendo lo previsto en el presente Contrato y en la normativa aplicable, especialmente la normativa del sector eléctrico y de defensa de los consumidores y usuarios.

En primer lugar, el Colaborador se compromete a proporcionar información veraz, clara y transparente sobre Holaluz y su actividad en aras de que el consumidor sea consciente de la empresa con la que contrata y el servicio que le van a ofrecer. En segundo lugar, el Colaborador se abstendrá en todo caso de formalizar altas con Holaluz si el Cliente no ha prestado de forma clara e inequívoca su consentimiento para la contratación del suministro con Holaluz. En el caso de que el cliente sea consumidor no profesional, el Colaborador garantizará que la contratación cumple también la normativa de protección de los Consumidores y Usuarios.

Por ello, recae en el Colaborador hacer las comprobaciones pertinentes en relación con la identidad del consumidor y de su voluntad de contratar, para asegurarse de la misma. Paralelamente, Holaluz realizará llamadas de control de forma aleatoria y contactará directamente con el cliente sin necesidad de aviso al Colaborador para verificar que se cumplían dichos requisitos."

Atendiendo a la cláusula anterior, se puede comprobar que CLIDOM obliga a QLIP a cumplir con un seguido de instrucciones y buenas prácticas para que éstos procedan al tratamiento de los datos personales de los potenciales clientes de conformidad con el RGPD. Asimismo, dentro del propio contrato se recogen las obligaciones de QLIP como encargado del tratamiento. Por ello, y para asegurar la diligencia y el buen cumplimiento de las instrucciones impuestas a QLIP, CLIDOM ha establecido medidas de responsabilidad proactiva para la comprobación de la recogida de los consentimientos válidos de los interesados.

Tercera.- Que en el artículo 28.4 del RGPD se recoge lo siguiente ante las obligaciones del Encargado del Tratamiento: "Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las

disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado."

Esta última parte del artículo 28.4 RGPD, hace referencia a que el encargado del tratamiento será responsable ante los tratamientos que realicen sus encargados, de conformidad con el cumplimiento de las obligaciones del artículo 28 del RGPD. Esto se traduce que, en caso de incumplimiento por parte de los proveedores seleccionados por el encargado del tratamiento, es decir, como en el caso presente por QLIP, éste deberá responsabilizarse directamente de las acciones y/u omisiones de sus proveedores, y no, por el contrario CLIDOM.

Cuarta.- En relación a la atribución de las responsabilidades del presente procedimiento sancionador, es importante señalar que en el artículo 82 del RGPD, titulado "Derecho a indemnización y responsabilidad" señala en su segundo apartado que: "Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable."

Éste último apartado, refleja el caso actual puesto que el subencargado de QLIP, la inmobiliaria ENFOKA, actuó en contra de las instrucciones de CLIDOM en cuanto a la obligación de recabar el consentimiento de los interesados ya que, éste suplantó la identidad de la afectada y, además, firmó un consentimiento no válido sin que pudiera cumplir con los principios de transparencia, libertad y consentimiento expreso. Por ende, siendo QLIP plenamente responsable de las actuaciones negligentes de su proveedor, por el incumplimiento de los artículos 28.4 y 82.2 del RGPD.

Quinta.- Que, en relación al cumplimiento de lo dispuesto en el artículo 25.1 RGPD, en lo que respecta a la aplicación de medidas técnicas y organizativas para comprobar la recogida del consentimiento válido de los datos personales de los interesados, CLIDOM dispone de un sistema de calidad y autenticación en relación a la identidad de sus clientes finales mediante un protocolo de revisión de un determinado porcentaje significativo de altas de usuarios finales, especialmente cuando éstos proceden de canales indirectos a CLIDOM, como es el caso en concreto. En aplicación de este protocolo, los agentes de atención al cliente internos de CLIDOM llaman por teléfono a dicha muestra de nuevos clientes cuya alta ha sido gestionada por medio del canal indirecto. Mediante estas llamadas CLIDOM tiene como objetivo cerciorarse de la validez del consentimiento según las características definidas por el propio RGPD y, paralelamente, comprobar y evidenciar que las correspondientes actuaciones de sus encargados son de conformidad a la ley y, a las instrucciones y obligaciones reflejadas en los respectivos contratos con éstos.

Mediante dicho protocolo de calidad, CLIDOM ha implementado medidas de comprobación y aseguramiento de las acciones encomendadas a QLIP, cumpliendo pues con el principio de responsabilidad proactiva.

Asimismo, con el fin de cumplir con el principio de responsabilidad proactiva, también se le solicita a QLIP documentación que acredite que el interesado ha consentido el tratamiento de sus datos para la gestión de la contratación de su suministro de energía. En esta línea, se aporta a modo ejemplificativo dos correos electrónicos remitidos por QLIP donde se aporta la documentación solicitada, tal y como acreditan los Documentos número 2 y 3.

Si bien por razones de volumetría, no se solicitan la totalidad de las autorizaciones, en términos generales CLIDOM realiza una auditoría inicial donde se comprueba que el cumplimiento de las instrucciones dadas por éste son cumplidas por parte de sus Colaboradores, solicitando una muestra de las autorizaciones que recogen el consentimiento del interesado, algo fundamental para la continuación de la relación comercial y, además, se realizan solicitudes puntuales cada cierto tiempo o siempre que se detecta alguna incidencia, para corroborar que, efectivamente, el Colaborador, en este caso QLIP, sigue cumpliendo las directrices de CLIDOM. De hecho, el propio contrato de colaboración incluye en su Anexo III un modelo de referencia de autorización de representación por terceros que pueden usar de base los Colaboradores de CLIDOM, todo ello porque es práctica común en el sector que los titulares de los suministros encarguen la gestión de su contratación a sus asesores energéticos (vid. Documento Número 1 – Anexo

III. MODELO AUTORIZACIÓN DE REPRESENTACIÓN A TERCEROS).

Finalmente, y nuevamente para dar cumplimiento al principio de responsabilidad proactiva, CLIDOM establece en su Anexo IV distintas medidas para controlar la calidad de los servicios prestados por los Colaboradores, entre las que se encuentran la verificación de las políticas de privacidad, seguridad y confidencialidad aplicadas por parte de los Colaboradores, verificación de los controles de seguridad aplicados por los Colaboradores a sus subcontratas, etc.

<u>Sexta</u>.- Que, CLIDOM ha solicitado a QLIP la documentación relativa a la relación comercial que mantiene con ENFOKA, así como el contrato de encargo de tratamiento o de cesión de datos que rige entre las partes, con el fin de conocer, si en calidad de encargado de tratamiento, éste se ha obligado con ellos en los mismos términos en los que QLIP se encuentra obligado con CLIDOM, dado que dicha obligación también se recoge en el contrato de colaboración entre las partes, no obstante, tal y como acreditan los emails adjuntos como Documento número 4, QLIP ha mostrado pasividad ante nuestras peticiones.

<u>Séptima</u>.- A continuación, también se debe manifestar que CLIDOM lleva a cabo análisis de riesgos de forma periódica para determinar aquellos riesgos que se puedan derivar del tratamiento de datos y así, a partir del resultado obtenido, diseñar y establecer todas aquellas medidas de seguridad que se

estimen oportunas para garantizar los derechos y libertades de las personas interesadas.

Por lo que respecta al análisis de riesgos ha resultado que ninguno de los riesgos analizados alcanza niveles altos, siendo los niveles de riesgos moderados. Se adjunta como Documento número 5 el análisis de riesgos relativo al activo de "Proveedores" realizado el pasado 19 de mayo de 2022.

Adicionalmente, CLIDOM el pasado 12 de septiembre de 2022 realizó un informe sobre el análisis de la necesidad de realizar una evaluación de impacto, como mecanismo para garantizar esa responsabilidad en la privacidad desde el diseño en el tratamiento de datos personales. El análisis se compone de dos partes: (i) El primero destinado a analizar si alguno de los tratamientos objeto del análisis se encuentra dentro de los supuestos obligatorios o excluidos recogidos en el listado publicado por la autoridad de control y, en su defecto, si pueden considerarse tratamientos de alto riesgo y (ii) En segundo lugar, se determinará si el tratamiento deberá ser objeto de una EIPD o, por el contrario, dicha evaluación no es necesaria a la vista del análisis.

Del análisis de primer y segundo nivel, se concluye que los tratamientos de datos realizados por CLIDOM para la prestación de sus servicios determinan que no se requiere una Evaluación de Impacto de Protección de Datos según los criterios del RGPD, de la Agencia Española de Protección de Datos y del Comité Europeo de Protección de Datos. Concretamente, de los análisis analizados, el único indicador que sale positivo es el relativo al tratamiento a gran escala.

En base a lo anterior, el tratamiento de datos realizado por CLIDOM NO NECESITA SER OBJETO DE UNA EVALUACIÓN DE IMPACTO. No obstante, al haber un tratamiento de datos a gran escala y, atendiendo a la naturaleza de la actividad de CLIDOM, se decide realizar una evaluación de impacto.

En la evaluación de impacto realizada en fecha 15 de septiembre de 2022 y referida a la gestión de clientes, se concluye que los tratamientos derivados de los procesos de negocio de gestión de clientes de CLIDOM, no suponen un riesgo que requiera la autorización previa de la Autoridad de Control para continuar el tratamiento. Sin embargo, deben llevarse a cabo las medidas de seguridad propuestas en la cláusula 3.5 del documento para reducir los riesgos.

Y, finalmente, tras la realización de la Evaluación de Impacto de la actividad del tratamiento de "Gestión de Clientes" de CLIDOM, surgieron un seguido de controles a implementar de carácter técnicos y organizativos derivados de las amenazas detectadas. Por ello, se realizó en fecha 22 de septiembre un plan de mitigación de las amenazas, con los controles a aplicar para conseguir la minimización de los riesgos.

Se adjuntan los tres Documentos como número 6, 7 y 8 respectivamente. Por ende, de los hechos acaecidos no se desprende, en caso alguno, que CLIDOM

no haya aplicado en todo momento las medidas técnicas y organizativas apropiadas. Adicionalmente, también se han adoptado las siguientes medidas mitigadoras adoptadas con posterioridad a la recepción de la reclamación:

- Se ha redactado un contrato de encargado de tratamiento que regula de forma más detallada la relación entre el Colaborador y CLIDOM respecto al tratamiento de los datos personales, pese a que ya se determinaba de forma expresa en el Contrato de Colaboración (se aporta como Documento número 9).

- Se han incrementado las llamadas telefónicas de control para aquellas contrataciones que provengan de canales comerciales.

- Se está valorando la posibilidad de automatizar la lectura masiva de documentos mediante Inteligencia Artificial con la finalidad de verificar que las autorizaciones remitidas por los canales comerciales han sido debidamente completadas.

- Mejora y aumento de la periodicidad de las auditorías de control a los canales comerciales.

Además, como otras medidas llevadas a cabo para evitar situaciones que pudieran vulnerar la normativa actual de protección de datos, destaca, entre otras, las formaciones sobre Protección de Datos que se han llevado a cabo para todos los trabajadores de la empresa.

No sólo se imparten formaciones de protección de datos a toda la empresa, sino que además se incluye una sesión de protección de datos y seguridad de la información como parte de las sesiones de Onboarding para las nuevas incorporaciones de personal, y mantiene actualizado al personal, mediante el envío de Newsletter a todos los trabajadores relativa a la protección de datos.

Igualmente, la compañía estableció un correo electrónico específico (lopd@clidom.es) para ejercer los derechos de rectificación, cancelación, supresión, limitación del tratamiento, portabilidad y cualquier derecho reconocido respecto al tratamiento de datos. Asimismo, para cualquier cuestión relacionada con las funciones del Delegado de Protección de Datos, se estableció el correo electrónico dpd@holaluz.com.

Finalmente, CLIDOM se somete a una auditoría anual en materia de Protección de Datos con una entidad externa y actualmente, está en proceso de obtener la ISO 27001 certificación de los Sist. de Gestión de Seguridad de la Información.

Octava.- Según el FD Tercero del Acuerdo de Inicio, la AEPD analiza una serie de elementos y criterios para valorar la cuantía de la multa a imponer.

Sin perjuicio de que nuestras alegaciones demuestran el cumplimiento estricto por parte de CLIDOM de la normativa de protección de datos −y, por tanto, que no procede la imposición de las multas indicadas en el Acuerdo de Inicio−,

consideramos también relevante, a efectos de hacer valer nuestro derecho de defensa, formular alegaciones a los criterios valorados por parte de la AEPD.

(i) El alcance o propósito de la operación de tratamiento de datos, así como los interesados afectados. En este sentido debemos poner de manifiesto que CLIDOM tiene actualmente alrededor de 300.000 clientes y que la presente reclamación incumbe a una interesada afectada. Consideramos que, al tratarse de un único caso, ello debería tenerse en cuenta con el fin de rebajar la cuantía de la sanción. Adicionalmente, atendiendo a las circunstancias recogidas en el art. 83.2 RGPD, se debe tener en especial consideración que no existen infracciones anteriores cometidas por parte de CLIDOM y que los datos tratados no se enmarcan en ningún caso como sensibles.

(ii) La intencionalidad o negligencia de la infracción. A este respecto, cabe indicar que, tal y como se ha expuesto en el presente escrito, CLIDOM ha cumplido en todo momento y de forma estricta con sus obligaciones en materia de protección de datos. En esta línea, CLIDOM adopta todas aquellas medidas técnicas y organizativas adecuadas para el tratamiento de los datos personales.

En conclusión, consideramos que en atención a lo anteriormente indicado se proceda automáticamente al archivo del procedimiento o, alternativamente, al reajuste de los criterios y cuantías valoradas.

Novena.- Que, en virtud de todo de lo expuesto y considerando imprescindible argumentar suficientemente en defensa de los legítimos intereses de CLIDOM, al amparo de lo establecido en 28.4 y 82 del Reglamento Europeo de Protección de Datos, esta parte SOLICITA.- Que, teniendo por presentado este escrito, se sirva admitirlo, y, en su virtud, tenga por presentadas en tiempo y forma las alegaciones contra el Acuerdo de Inicio y, a la vista de las manifestaciones que anteceden, dicte resolución por la que, estimando estas alegaciones, el procedimiento sancionador Nº PS/0680/2022 quede archivado".

De las actuaciones practicadas en el presente procedimiento y de la información y documentación presentada han quedado acreditados los siguientes:

HECHOS PROBADOS.

Primero: Consta acreditado la existencia de un contrato de arrendamiento entre la reclamante y la Inmobiliaria ENFOKA de fecha 24/05/21. En dicho contrato y dentro de las obligaciones contractuales de la arrendataria (la reclamante), se encuentra el pago del consumo de luz.

La reclamante tiene contratado este servicio con la comercializadora Iberdrola.

Segundo: En su escrito de reclamación manifiesta que el día 07/04/22 comprobó que en su cuenta corriente había un cargo de ***CANTIDAD.1 euros de otra comercializadora de luz, HOLALUZ, con la que ella no tenía ninguna relación contractual, por lo que se puso en contacto con ella para conocer lo que había ocurrido,

De las conversaciones mantenidas con los operadores de HOLALUZ, pudo saber que el contrato de luz había sido cambiado de compañía con fecha 24/02/22 y que dicho contrato había sido firmado por una tercera persona ajena, dándose el hecho de que era trabajadora de la inmobiliaria ENFOKA: ***B.B.B.*** NIF: ******NIF.2***.

Notar que la inmobiliaria ENFOKA es una subcontrata de la entidad QLIP, que a su vez tiene un contrato de servicio con la compañía de luz HOLALUZ, y cuya misión es captar nuevos clientes para la compañía eléctrica.

Tercero: Según manifiesta la Inmobiliaria ENFOKA ante esta Agencia, se instó a la arrendataria en numeras ocasiones para que modificase la titularidad del suministro eléctrico, pues se estaba realizando un cambio masivo de compañía, de los contratos de luz de todas las viviendas gestionadas por ellos. Al no tener contestación de la inquilina (la reclamante), en el mes de febrero/22 la envió un e-mail informándola de que se procedería a cambiar de compañía eléctrica el suministro de la vivienda que tenía alquilada, comunicando sus datos personales a la empresa Runup Business, S.L. (QLIP), empresa del canal comercial de HOLALUZ-CLIDOM.

Cuarto: Según manifiesta CLIDOM ante esta Agencia, el subencargado de QLIP, la inmobiliaria ENFOKA, actuó en contra de las instrucciones de CLIDOM, en cuanto a la obligación de recabar el consentimiento de los interesados ya que ésta suplantó la identidad de la afectada y, además, firmó un consentimiento no válido sin que pudiera cumplir con los principios de transparencia, libertad y consentimiento expreso y por ende, QLIP es plenamente responsable de las actuaciones negligentes de su proveedor.

Quinto: Respecto de las medidas técnicas y organizativas implantadas en la entidad CLIDOM, para comprobar la recogida del consentimiento válido de los datos personales de los interesados, manifiesta que el sistema que dispone se basa en la revisión de un determinado porcentaje significativo de altas de usuarios finales, especialmente cuando éstos proceden de canales indirectos a CLIDOM, como es el caso. Si bien por razones de volumetría, no se realiza el control a la totalidad de las solicitudes de alta recibidas. No obstante, no se presenta ningún informe o certificado donde se detalle el porcentaje de llamadas realizadas para las comprobaciones indicadas.

FUNDAMENTOS DE DERECHO

I.-
Competencia:

De acuerdo con los poderes que el artículo 58.2 del RGPD, otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, es competente para 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.-
Síntesis de los hechos:

Según expone la reclamante en su escrito de reclamación de fecha 11/06/22, es inquilina de una vivienda desde el 24/05/21, cuya gestión la realiza la inmobiliaria ENFOKA SISTEMAS GLOBALES, S.L.

Según explica en la reclamación, el suministro de luz lo tenía contratado con Iberdrola pero el día 07/04/22 le cargaron en su cuenta la cantidad de ***CANTIDAD.1 euros de una compañía de luz por el suministro energético de la vivienda, de la que no tenía ningún conocimiento ni con la que no había contratado nada (HOLALUZ- CLIDOM).

Puesta en contacto con la inmobiliaria ENFOKA, a la que alquiló la vivienda, para preguntarles el motivo de dicho recibo de luz, la contestaron que había sido un cambio masivo a todos los inquilinos del inmueble para que figurase la luz a su nombre, a lo que la reclamante les contestó que nadie la había informado de dicho cambio y mucho menos que se le hubiera pedido el consentimiento para el cambio de compañía, cuyo suministro, recordemos, debía abonar ella.

También denuncia que, una vez obtenido el nuevo contrato de suministro de luz con la nueva compañía (HOLALUZ-CLIDOM), se dio cuenta de que figuraba en el apartado de "Cliente" sus datos personales, pero en el apartado de la firma del contrato figura una tal "***B.B.B.***" que no conocía de nada.

Según afirma la compañía CLIDOM, dicha alta fue llevada a cabo por parte del canal comercial Run Up Business SL. (QLIP) con el que mantiene una relación contractual para el alta de nuevos clientes y que, la inmobiliaria ENFOKA, actuó en contra de sus instrucciones en cuanto a la obligación de recabar el consentimiento de los interesados ya que, ésta suplantó la identidad de la afectada, y por ende, QLIP es también plenamente responsable de las actuaciones negligentes de su proveedor ENFOKA.

Aunque CLIDOM manifiesta que ENFOKA en un subencargado de QLIP, no aporta ningún tipo de contrato que pueda corroborarlo.

CLIDOM manifiesta también que, respecto de las medidas técnicas y organizativas implantadas para comprobar la recogida del consentimiento válido de los datos personales de los interesados, el sistema que dispone se basa en la revisión de un determinado porcentaje significativo de altas de usuarios finales, especialmente cuando éstos proceden de canales indirectos a CLIDOM, como es el caso en concreto. Si bien por razones de volumetría, no se realiza el control a la totalidad de las solicitudes de alta recibidas. No obstante, no presenta ningún tipo de informe o certificado donde se manifiesta el porcentaje de llamadas realizadas para las comprobaciones indicadas.

III.
Respuesta a las alegaciones presentadas:

Con relación a las alegaciones aducidas en el presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por la entidad:

a).- Contestación a las alegaciones presentadas en el punto “Primero” de su escrito de alegaciones:

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas -LPACAP-, señala en el art. 21.1 que, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación.

Ahora bien, no puede confundirse, en modo alguno, la propuesta de resolución con el acto administrativo de resolución del procedimiento, pues el artículo 89.2 LPACAP señala que, en el caso de procedimientos de carácter sancionador, una vez concluida la instrucción del procedimiento, el órgano instructor formulará una propuesta de resolución dirigida al órgano competente para resolver que también deberá ser notificada a los interesados, indicando en la misma la puesta de manifiesto del procedimiento y el plazo para formular alegaciones y presentar los documentos e informaciones que se estimen pertinentes, disponiendo en el apartado tercero del citado artículo 89 LPACAP que, en la misma se fijarán de forma motivada los hechos que se consideren probados y su exacta calificación jurídica, se determinará la infracción que, en su caso exista, la persona o personas responsables y la sanción que el órgano instructor proponga, la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión, así como las medidas provisionales que, en su caso, se hubieran adoptado.

No obstante, también se establece que, si el órgano competente para resolver considera que la infracción o la sanción propuesta por el órgano instructor reviste mayor gravedad que la propuesta, lo notificará al inculpado para que aporte cuantas alegaciones estime convenientes en el plazo de quince días, antes de notificar su decisión en la resolución.

Por tanto, la propuesta de resolución es solamente un acto de trámite que no determina la finalización del procedimiento pues es solamente una propuesta que se realiza al órgano que realmente tiene las competencias para la resolución del procedimiento sancionador, siendo esta resolución el verdadero acto administrativo expreso donde se resuelve el procedimiento y se impone la sanción, en su caso.

Por tanto, no puede confundirse, en modo alguno, la propuesta de resolución con el acto administrativo de resolución del procedimiento, tal y como defiende la parte reclamada en sus alegaciones, y por tanto, no existe, en este caso, “*un procedimiento de reapertura del procedimiento sancionador*” pues aún es necesario un acto administrativo expreso resolviendo el procedimiento e imponiendo la sanción correspondiente o archivando el procedimiento y eso no ocurre con la propuesta de resolución emitida.

b).- Contestación a las alegaciones presentadas en el punto “Segundo” de su escrito de alegaciones:

Respecto de las alegaciones presentadas en este punto, debemos recordar que, el artículo 4 del RGPD, bajo la rúbrica “Definiciones”, dispone lo siguiente:

> *“2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.*
>
> *7) «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 específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”*

Y que, el artículo 24.1 del RGPD dispone, respecto de la responsabilidad del responsable del tratamiento, que:

> “*Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.”*

Pues bien, en el presente supuesto, consta que la entidad CLIDOM es el responsable de los tratamientos de datos, toda vez que, conforme a la definición del artículo 4.7 del RGPD, es quien determina la finalidad y medios de los tratamientos realizados con las finalidades señaladas en la documentación aportada relativa a la contratación de sus servicios, y así lo reconoce en su escrito de alegaciones, por lo que, en su condición de responsable del tratamiento está obligada a cumplir con lo dispuesto en el transcrito artículo 24 del RGPD, en especial en cuanto al control efectivo y continuado de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos realizados de los clientes es conforme con el RGPD.

Por su parte, el artículo 25.1 del RGPD establece que:

> *“Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de*

protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."

Y si a todo ello, tenemos en cuenta lo señalado en los considerandos del RGPD:

74. "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"

75. "Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

76. "La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto."

Además de todo ello, debemos atender a lo estipulado en el artículo 28 LOPDGDD, pues indica que los responsables tendrán en cuenta los arts. 24 y 25 para la aplicación de las medidas de responsabilidad proactiva y los mayores riesgos que podrían producirse, entre los que se incluyen los supuestos de fraude y suplantación:

“Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación".

Es evidente, por tanto, que el responsable del tratamiento, CLIDOM, estará obligado a realizar un análisis de los riesgos para los derechos y libertades de las personas físicas, implantando las medidas técnicas y organizativas apropiadas para aplicar los principios de protección de datos e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del RGPD, debiendo poder demostrar que el tratamiento realizado es conforme con lo previsto en la citada norma.

Los principios de protección de datos se encuentran recogidos en el artículo 5 del RGPD, debiendo destacarse aquí, el primero de ellos, relativo a la licitud del tratamiento, según el cual:

"Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»).

Mientras que en el apartado "segundo" del citado artículo 5 dispone que:

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

Pues bien, de la documentación aportada en el presente procedimiento y de las alegaciones presentadas por las diferentes partes, se constata que, la inmobiliaria ENFOKA, empresa que gestiona la vivienda donde la reclamante vive de alquiler, envió a QLIP un correo electrónico comunicando los datos de la arrendataria para cambiar de compañía eléctrica el suministro de la vivienda sin que ENFOKA informara de ello a la inquilina, y por supuesto, sin su consentimiento. Después, QLIP trasladó a CLIDOM los datos de la inquilina (la reclamante) y los datos de la persona que firmaba el contrato en nombre de la inquilina procediendo ésta a dar de alta el servicio.

Todo este proceso se gestionó sin que la inquilina (la reclamante) fuera informada de ello y por supuesto, fue realizado sin su consentimiento.

CLIDOM ha venido manifestando a lo largo de todo este procedimiento que la responsabilidad del tratamiento de los datos personales de la reclamante es exclusivamente de QLIP en base al contrato de servicio firmado entre ellos y de la subcontrata de ésta (ENFOKA) pues es la que realizó en un primer momento el tratamiento de datos inconsentido de la reclamante pero no aporta ningún tipo de contrato entre las empresa que pueda corroborar sus alegaciones por lo que se debe considerar como meras manifestaciones sin ningún soporte documental.

Además, se ha observado que, cuando la contratación del servicio se lleva a cabo a través de un presunto representante del nuevo cliente, CLIDOM no requiere que acredite la representación que dice ostentar, evidenciándose con ello que CLIDOM no tiene implantado un sistema eficiente que permita corroborar que los clientes dados de alta a través de un supuesto representante han dado su consentimiento para ello.

CLIDOM se defiende alegando que, tiene implantado un protocolo de revisión de un determinado porcentaje de altas de usuarios finales, cuando dichas altas vienen a través de colaboradores externos, como es el caso. Si bien, según confirma la propia entidad, por razones de volumetría, no se realiza en la totalidad de las solicitudes sino en un determinado porcentaje, que tampoco determina, pues no presenta ningún informe o certificado que pueda corroborar el porcentaje de llamadas realizadas.

Es evidente que realizando una muestra aleatoria de control de altas, se pueden generar riesgos en el tratamiento de los datos personales de los clientes, como puede ser el tratamiento de datos sin legitimación, o el riesgo de suplantación de identidad para la comisión de un fraude, con los perjuicios económicos y sociales que conlleva.

Se alega por CLIDOM que, recae en su colaborador QLIP, hacer las comprobaciones pertinentes en relación con la identidad del consumidor y de su voluntad de contratar, para asegurarse de la misma e indica que, no obstante, CLIDOM realizará llamadas de control de forma aleatoria y contacta directamente con el cliente para verificar el consentimiento.

Pues bien, debe recordase que, las estipulaciones de los artículos 24 y 25 del RGPD hacen referencia a las obligaciones establecidas para el responsable del tratamiento. Así tenemos como, en el artículo 24 se establece la obligación de que el responsable debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD, y el artículo 25, reitera la obligación del responsable de aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas a fin de cumplir los requisitos del RGPD y proteger los derechos de todos y cada uno de los interesados y no solamente de un determinado porcentaje elegido al azar, como realiza CLIDOM.

Por tanto, es el responsable último del tratamiento de los datos personales, en este caso CLIDOM, en cumplimiento de sus obligaciones de responsabilidad proactiva, quien debe implantar las medidas técnicas y organizativas necesarias para el correcto tratamiento de los datos personales, tal y como lo expresan los artículos 24 y 25 del RGPD, o como se señala en los términos del considerando 73: "*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"* y por tanto, es al responsable último del tratamiento de los datos personales, a quien corresponde velar para que tales medidas se cumplan.

CLIDOM debió valorar los riesgos y en particular los riesgos del art. 28 en su análisis de riesgos y evaluación de impacto, pero de la documentación aportada no consta que se haya hecho. Indica que realiza un tratamiento masivo de datos, también realiza evaluaciones de solvencia como se desprende del Contrato entre CLIDOM y QLIP, en el que consta que el encargado recogerá "Información de solvencia, acorde a los procedimientos de evaluación de solvencia establecidos por Holaluz en cada momento". Sin embargo, estos riesgos no se han valorado ni adoptado medidas para mitigarlos. Por lo que aquí interesa el reclamado no ha hecho ninguna valoración sobre el riesgo de usurpación de identidad o fraude, por lo que difícilmente ha podido adoptar medidas adecuadas, no se puede valorar si la medida consistente en realizar

llamadas aleatorias para comprobar la veracidad de la contratación es adecuada cuando ni siquiera se ha valorado el riesgo.

c).- Contestación a las alegaciones presentadas en el punto “Tercero” y “Cuarto” de su escrito de alegaciones:

En estos puntos, solamente dejar claro que el presente procedimiento sancionador no trata sobre la posible responsabilidad del encargado del tratamiento (QLIP) por el posible incumplimiento en el tratamiento de los datos personales de la reclamante por parte de la inmobiliaria ENFOKA, según lo establecido en el artículo 28 del RGPD, sino la responsabilidad del responsable último del tratamiento de los datos (CLIDOM), en base a lo estipulado en el artículo 25 del RGPD, por cuanto se ha constatado que, cuando se realizó el cambio de contratación del servicio a nombre de la inquilina (reclamante), CLIDOM, no realizó ninguna comprobación respecto del consentimiento de la reclamante al cambio de compañía eléctrica, más aún cuando el contrato del cambio de suministro venía firmado por persona ajena a la reclamante y que en dicho contrato no existía señal alguna que pudiera avalar la representación de esta persona en nombre de la reclamante.

En este sentido, la doctrina de la Audiencia Nacional señala que cuando el titular de los datos niega el consentimiento en el tratamiento de sus datos corresponde la carga de la prueba a quien afirma su existencia, debiendo el responsable del tratamiento recabar y conservar la documentación necesaria para acreditar que el consentimiento se ha dado y que ha sido dado por el titular de los datos (Sentencia de la Audiencia Nacional de 31 de mayo de 2006.- Rec. 539/2004): *“Por otra parte es el responsable del tratamiento (por todas, sentencia de esta Sala de 25 de octubre de 2002 Rec. 185/2001) a quien corresponde asegurarse de que aquel a quien se solicita consentimiento, efectivamente lo da, y que esa persona que está dando el consentimiento es efectivamente el titular de esos datos personales, debiendo conservar la prueba del cumplimiento de la obligación a disposición de la Administración”.*

d).- Contestación a las alegaciones presentadas en el punto “Quinto” de su escrito de alegaciones:

Pues bien, tal y como hemos venido indicando a lo largo de todo el procedimiento, el artículo 25 del RGPD establece la obligatoriedad para el responsable del tratamiento de aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, que garanticen el cumplimiento de los requisitos del RGPD y con ello, la protección de los derechos y libertades de los interesados.

Este artículo tiene como antecedente el 24 del RGPD que indica por su parte que, *“Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento”.*

En consonancia con estas previsiones, el considerando 78 del RGPD indica que:

> *"La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."*

Por tanto, el principio de protección de datos desde el diseño es la clave a seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que está obligado a adoptar las políticas internas y aplicar las medidas necesarias que garanticen el cumplimiento de los principios de protección de datos desde el diseño y por defecto.

Así, y respecto de los riesgos que pueden estar presentes en el tratamiento, el responsable deberá llevar a cabo un ejercicio de análisis y detección de los riesgos durante todo el ciclo de tratamiento de los datos, con la finalidad última de proteger los derechos y libertades de todos los interesados, y no sólo cuando efectivamente se produce el tratamiento. Así se expresa en las Directrices 4/2019 del Comité Europeo de Protección de Datos (CEPD) relativas al artículo 25 Protección de datos desde el diseño y por defecto, adoptadas el 20 de octubre de 2020, indicando al respecto:

> *"35. El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del software y hardware y los servicios de tratamiento de datos.*

36. Tomar en consideración la PDDD (protección de datos desde el diseño y por defecto) desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas".

Para ello debe recurrir, al diseñar el tratamiento, a los principios recogidos en el artículo 5 del RGPD, que servirán para aquilatar el efectivo cumplimiento del RGPD. Así, las citadas Directrices 4/2019 del CEPD disponen que "*61. Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD. (…)".*

La Guía de Privacidad desde el Diseño de la AEPD afirma que "*La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada".*

La Guía dispone también que, "*La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña (…) La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida completo de los datos".*

Por ello, la privacidad desde el diseño, obligación del responsable del tratamiento que nace antes de que el sistema esté en funcionamiento, no es un parche que se utiliza para resolver una incidencia detectada en el sistema.

El enfoque de riesgos hace referencia directa e inmediata a un sistema preventivo tendente a visualizar, respecto de un tratamiento de datos personales, los riesgos en los derechos y libertades de las personas físicas. Han de identificarse los riesgos, evaluar su impacto y valorar la probabilidad de que aquellos se materialicen. Se protegen pues, no los datos, sino a las personas que están detrás de ellos.

Los riesgos para los derechos y libertades de las personas físicas, derivados del tratamiento de datos personales, pueden ser de gravedad y probabilidad variables y provocar daños y perjuicios físicos, materiales o inmateriales, consecuencias tangibles o intangibles, en los derechos y las libertades de las personas físicas. El considerando 75 del RGPD y el art. 28.2 de la LOPDGDD recopilan ejemplificativamente algunos, mas no son los únicos. Dependerá del tratamiento y el contexto en el que este se

realiza, de los datos personales tratados, de las personas involucradas o de los medios utilizados:

> *"(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, (…)".*

Del contenido de la documentación que figura en el expediente, se desprende que el origen de la incidencia se encuentra en un mal diseño del sistema implantado por la entidad CLIDOM para la comprobación del consentimiento prestado por el titular del contrato de alta, cuando dicho contrato viene firmado por un presunto representante del mismo, pues según confirma la propia entidad, solamente se realiza un muestreo de las nuevas altas para comprobar la veracidad del consentimiento, pues según la propia entidad, "*por razones de volumetría, no se realiza el control a la totalidad de las solicitudes de alta recibidas*".

El artículo 25 del RGPD no se constriñe a la garantía de una seguridad adecuada al riesgo, implementado medidas de comprobación y aseguramiento aleatorios, como afirma la entidad CLIDOM, sino a la adopción de las medidas que garanticen la aplicación de forma efectiva de los principios de protección de datos y el cumplimiento de los requisitos del RGPD para proteger los derechos de todos y cada uno de los interesados. Y ello no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Cabe recordar que la Protección de Datos desde el Diseño y por Defecto (PDDD) es una obligación legal, cuya vulneración constituye una infracción según lo dispuesto en el artículo 83 del RGPD. La protección de datos desde el diseño forma parte del sistema de gestión del cumplimiento normativo, que implica concebir y planificar el tratamiento, verificar su cumplimiento y poder demostrarlo, todo ello enmarcado en un proceso de revisión y mejora continua.

En el presente caso, se pone de manifiesto la falta de diseño del tratamiento por parte de la entidad CLIDOM, toda vez que, como ella misma reconoce, solamente hace un muestreo en las altas recibidas desde los colaboradores externos para comprobar si realmente ha existido un verdadero consentimiento por parte de los nuevos clientes.

> e).- Contestación a las alegaciones presentadas en el punto "Séptimo" de su escrito de alegaciones:

Señalaba la parte reclamada en su escrito de alegaciones, respecto de la realización de la evaluación de impacto de datos personales (EIPD), que "*el pasado 12 de septiembre de 2022 realizó un informe sobre el análisis de la necesidad de realizar una evaluación de impacto, como mecanismo para garantizar esa responsabilidad en la privacidad desde el diseño en el tratamiento de datos personales y que del análisis se concluye que los tratamientos de datos realizados por CLIDOM para la prestación de sus servicios determinan que no se requiere una Evaluación de Impacto de Protección de Datos según los criterios del RGPD, de la AEPD y del Comité Europeo de Protección de Datos, pero que, al haber un tratamiento de datos a gran escala y,*

atendiendo a la naturaleza de la actividad de CLIDOM, se decide realizar una evaluación de impacto En la evaluación de impacto realizada en fecha 15 de septiembre de 2022, se concluye que los tratamientos derivados de los procesos de negocio de gestión de clientes de CLIDOM, no suponen un riesgo que requiera la autorización previa de la Autoridad de Control para continuar el tratamiento. Sin embargo, deben llevarse a cabo las medidas de seguridad propuestas en la cláusula 3.5 del documento para reducir los riesgos, como, por ejemplo, el incremento de llamadas telefónicas de control para aquellas contrataciones que provengan de canales comerciales o la posibilidad de automatizar la lectura masiva de documentos mediante Inteligencia Artificial con la finalidad de verificar que las autorizaciones remitidas por los canales comerciales han sido completadas.

En primer lugar, se hace necesario poner de manifiesto que, en el momento de la presentación de la reclamación que ha dado lugar al presente procedimiento sancionador, es decir, en el 12 de junio de 2022, según confirma la parte reclamada, ni siquiera se había realizado el estudio sobre la necesidad de una evaluación de impacto, pues éste se realizó el 12 de septiembre de 2022.

En segundo lugar, aunque no ha sido objeto del presente procedimiento sancionador valorar la posible vulneración de los estipulado en el artículo 35 del RGPD, respecto de la obligación de realizar una Evaluación de Impacto de Datos Personales (EIDP), se hace necesario, manifestar respecto de las alegaciones presentadas por la entidad CLIDOM, en este punto que, con carácter general, existe la obligación de llevar a cabo la realización de una EIPD siempre que el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas.

El RGPD dedica la Sección 3 de su capítulo IV “Responsable del tratamiento y encargado del tratamiento” a la Evaluación de Impacto relativa a la protección de datos (EIPD). En concreto, el apartado 1 del artículo 35 establece, con carácter general, la obligación que tienen los responsables de los tratamientos de datos de realizar una EIPD con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que éstos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, alto riesgo que, según el propio Reglamento, se verá incrementado cuando los tratamientos se realicen utilizando “nuevas tecnologías”.

Para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que requieren una EIPD, el RGPD dispone que las autoridades de control deberán publicar una lista con los tratamientos que requieran de una EIPD. Dicha lista deberá ser comunicada al Comité Europeo de Protección de Datos (CEPD).

La parte reclamada ha manifestado que, en un primer momento, no se efectuó la EIPD porque no se encuentra en ninguno de los supuestos que lo exige, según el artículo 35 del RGPD. Sin embargo, no estamos ante una lista exhaustiva, sino que ha de valorarse la complejidad del proceso de gestión de riesgo, teniendo en cuenta no el tamaño de la entidad, la disponibilidad de recursos, la especialidad o sector de esta, sino el posible impacto de la actividad de tratamiento sobre los interesados.

Pues bien, la citada lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 “*Directrices sobre la evaluación de impacto relativa a*

la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD", y debe entenderse, como una lista no exhaustiva, destacando, para el caso que nos ocupa, los tratamientos de datos que,
"(7.) impliquen el uso de datos a gran escala".

En este caso, se debe realizar un análisis de riesgos RGPD que permita identificar los riesgos que pueden derivarse del tratamiento de datos y valorar la probabilidad y el impacto de materialización, para determinar el nivel de los riesgos y si estos son tolerables, se pueden minimizar o eliminar o son inaceptables.

Pero es que además y sin perjuicio de los tratamientos recogidos en la lista, no exhaustiva de la AEPD, los responsables tienen que valorar si procede realizar una evaluación de impacto respecto de los tratamientos que realizan teniendo en cuenta, entre otros, los riesgos recogidos en el art. 28 LOPDGDD.

Cabe señalar que los riegos pueden ser dos tipos: - riesgos que afectan a las personas cuyos datos son tratados y que se pueden concretar en la vulneración de sus derechos y libertades, pérdida de información necesaria o daños causados por la utilización ilícita o fraudulenta de los datos, y riesgos que pueden afectar a la empresa u organización por no haber implementado una política de protección de datos adecuada y suficiente.

Una vez analizado los riesgos se deben establecer medidas para afrontarlos. Es decir, se deben establecer garantías en función de los mismos mediante las cuales se garantice la protección de los datos personales, así como también que todos los procedimientos cumplen escrupulosamente con la normativa (RGPD), siempre sin perder de vista los derechos e intereses legítimos de todos y cada uno de los interesados y de otras personas afectadas.

Estas medidas deben tener como fin eliminar, mitigar o transferir los riesgos detectados. Generalmente, las evaluaciones de impacto también incluyen la aceptación de los riesgos detectados, pero en protección de datos y respecto a cómo pueden verse impactados los derechos y libertades de las personas, la aceptación podría suponer un incumplimiento de la normativa, por lo que las medidas a implementar siempre deben encaminarse a evitar o eliminar esos riesgos. Otra cosa diferente es que, después de haber implementado un sistema que persiga la eliminación total del riesgo, éste se produzca, en cuyo caso se deberá realizar una revisión del método para adaptarle con el objetivo último de erradicar el riesgo.

Por tanto, las medidas propuestas, como el incremento del número de llamadas telefónicas de control para aquellas contrataciones que provengan de canales comerciales no demuestran que se persiga la reducción del riesgo a cero, pues ni se ha valorado el riesgo de suplantación y fraude ni tampoco se detalla el porcentaje de llamadas que se van a realizar sobre el total de solicitudes de alta recibidas de los canales externos.

f).- Contestación a las alegaciones presentadas en el punto "Octavo" de su escrito de alegaciones:

En este apartado, la entidad reclamada manifiesta que tiene alrededor de 300.000 clientes y que la presente reclamación incumbe a una sola interesada afectada. Que no existen infracciones anteriores cometidas por parte de CLIDOM y que los datos tratados no se enmarcan en ningún caso como sensibles y por otra parte, manifiesta que, ha cumplido en todo momento y de forma estricta con sus obligaciones en materia de protección de datos, adoptando aquellas medidas técnicas y organizativas adecuadas para el tratamiento de los datos personales.

El presente procedimiento sancionador se inició por el hecho de que la parte reclamada realizara un tratamiento de los datos personales de la reclamante sin corroborar previamente la acreditación de la representación de quien le proporcionó los datos, o que comprobase, por cualquier medio, que la reclamante consintiera efectivamente, realizar el cambio de compañía eléctrica, según estipula el artículo 25 del RGPD.

Dicha infracción 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.a) del RGPD.

Para graduar la sanción se debe tener en cuenta lo establecido en los artículos 83.1 y 2 del RGPD, y 76 de la LOPDGDD y se estimó aplicar como agravantes para calcular la sanción a imponer, los potencialmente clientes afectados, de acuerdo con las Directrices 4/2022 del CEPD sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión de 12 de mayo de 2022, sometida, en aquel entonces, a consulta pública, estando la sanción inicial impuesta muy por debajo del máximo establecido en el RGPD,

Además se tuvo en cuenta que la actividad empresarial de la reclamada trata necesariamente datos personales. Esta característica de su actividad empresarial repercute, reforzándola, en la diligencia que debe desplegar en el cumplimiento de los principios que presiden el tratamiento de datos de carácter personal y en la calidad y eficacia de las medidas técnicas y organizativas que debe tener implementadas para garantizar el respeto del derecho fundamental.

Y por tanto se debe tener presente lo establecido por la Audiencia Nacional en este caso, (SAN de 17 de octubre de 2007 (rec. 63/2006):

> *“…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. Y 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, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto". Por tanto, si nos atenemos a la jurisprudencia del TS, podríamos considerar incluso este apartado como agravante cualificado, al constatarse la falta de diligencia debía en este caso, con respecto a la gestión de los datos personales.*

Por tanto, en consideración a todo lo expuesto, no puede ser atendida en este caso, la solicitud de la entidad reclamada en el sentido de reducir la sanción impuesta de 100.000 euros.

IV.-
Infracción administrativa

En el presente supuesto, se evidencia que la entidad HOLALUZ-CLIDOM, S.A., es la responsable de los tratamientos de datos, referidos en los antecedentes, toda vez que, conforme a la definición del artículo 4.7 del RGPD, es quien determina la finalidad y medios de los tratamientos realizados relativos a la contratación de sus servicios, esto es, dar de alta a un nuevo cliente y gestionar el suministro de luz a su hogar o negocio, con independencia del canal a través del cual haya obtenido los datos, en este caso, según manifiesta, fueron obtenidos a través del canal comercial Run Up Business SL, con el que HOLALUZ-CLIDOM mantiene una relación contractual para este fin.

En definitiva, el responsable del tratamiento es la persona física o jurídica o autoridad pública, que decide sobre el tratamiento de los datos personales, determinando los fines y los medios de dicho tratamiento. En virtud del principio de responsabilidad proactiva el responsable del tratamiento tiene que aplicar medidas técnicas y organizativas para, en atención al riesgo que implica el tratamiento de los datos personales, cumplir y ser capaz de demostrar el cumplimiento.

Por tanto, los citados hechos expuestos, suponen la vulneración del principio de protección de datos desde el diseño regulado en el artículo 25 del RGPD, que da lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

El hecho de que la parte reclamada realizara un tratamiento de los datos personales de la reclamante sin corroborar previamente la acreditación de la representación de quien le proporcionó los datos, o que comprobase, por cualquier medio, que la reclamante consintió efectivamente, realizar el cambio de compañía eléctrica o que consintió que se pudiera realizar un tratamiento de sus datos personales para ese fin, es constitutivo de una infracción al artículo 25.1) del RGPD.

Esta infracción 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.a) del RGPD.

Por su parte, el artículo 73.d) de la LOPDGDD, considera “graves”, a efectos de prescripción, *“La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679”.*

V.-
Graduación de la sanción

La determinación de la sanción que procede imponer en el presente caso exige observar las previsiones de los artículos 83 del RGPD, y 76 de la LOPDGDD y de acuerdo con dichos preceptos, a efectos de fijar el importe de la sanción de multa a imponer a la entidad reclamada. Se estiman concurrentes en el presente caso los siguientes factores:

En calidad de agravantes:

- El alcance o propósito de la operación de tratamiento de datos, así como los interesados afectados en relación con el número de los potenciales interesados afectados (apartado a del artículo 83.1 RGPD).

- La intencionalidad o negligencia de la infracción, por parte de la entidad, (apartado b del artículo 83.1 del RGPD).

Se considera además que, procede graduar la sanción a imponer de acuerdo con los siguientes criterios agravantes, que establece el artículo 76.2 de la LOPDGDD:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales, (apartado b), considerando que en la actividad que se desarrolla s se ven implicados los datos personales de los clientes de ésta.

Considerando los factores expuestos, la valoración que alcanza la multa final, por la Infracción del artículo 25 del RGPD, es de **100.000 euros (cien mil euros).**

VI.-
Medidas

El artículo 58.2 del RGPD establece los poderes correctivos de los que dispone una autoridad de control y el apartado d) del precepto citado establece que puede consistir en "*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*".

Por tanto, procede imponer la medida correctiva descrita en el artículo 58.2.d) del RGPD y ordenar a la entidad HOLALUZ-CLIDOM, SA. que, en el plazo de seis meses, establezca las medidas técnicas y organizativas adecuadas para que se verifique el consentimiento presuntamente dado por los nuevos clientes de la compañía y/o la veracidad de los presuntos representantes de los mismos.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos

RESUELVE:

PRIMERO: IMPONER a la entidad, HOLALUZ-CLIDOM, S.A., CIF.: A65445033, por la infracción del artículo 25 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de **100.000 euros (cien mil euros).**

SEGUNDO: ORDENAR a la entidad HOLALUZ-CLIDOM, S.A., CIF.: A65445033 que implante, en el plazo de seis meses, las medidas técnicas y organizativas adecuadas para que se verifique el consentimiento presuntamente dado por los nuevos clientes de la compañía y/o la veracidad de los presuntos representantes de los mismos.

TERCERO: NOTIFICAR la presente resolución a HOLALUZ-CLIDOM, S.A.,

CUARTO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida Nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior. De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.6 de la LOPDGDD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [*https://sedeagpd.gob.es/sede-electronicaweb/*], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre.

También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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