- **Expediente N.º: EXP202204846**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes Antecedentes, Hechos Probados y Fundamentos de Derecho, la Directora de la Agencia Española de Protección de Datos resuelve adoptar la presente resolución de procedimiento sancionador.

TABLA DE CONTENIDO

ANTECEDENTES

PRIMERO: Con fecha 10 de febrero de 2022, se notificó a la Agencia Española de Protección de Datos (AEPD) una violación de seguridad de los datos personales, remitida por ENDESA ENERGÍA, S.A.U. con NIF A81948077 (en adelante, ENDESA), consistente en un posible acceso no autorizado a ciertos sistemas comerciales de Endesa Energía que podría haber afectado a unos mil clientes.

En esta notificación se informa a la AEPD de lo siguiente:

En agosto de 2021, se detectan ciertos anuncios de Facebook que anuncian la venta de credenciales para acceder a la plataforma ******PLATAFORMA.1*** de ENDESA (que contiene datos básicos y relativos al punto de suministro). Se valoró ese incidente y se adoptaron las medidas pertinentes. El 17/01/2022 se detecta un anuncio de Facebook con características similares a los anteriores que informa de la venta de bases de datos de clientes de energía y gas. Se hace una valoración del anuncio y no se encuentran coincidencias con datos de clientes de ENDESA incluidos en el sistema CRM. El 8/02/2022 se detectan datos de, entre otros, algunos clientes de ENDESA incluidos en el sistema CRM.

Número aproximado de personas físicas sobre las que recoge, almacena o trata datos personales de otra forma; referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales: 6.500.000.

El incidente ha sido: Intencionado, para hacer daño al responsable / encargado o a las personas afectadas.

El origen del incidente ha sido: Externo: Otros, ajenos al responsable y encargado del tratamiento

¿Qué puede haber ocurrido?: Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales

Como consecuencia del incidente, se ha visto afectada la: Confidencialidad

Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?: No

¿Qué puede haber ocurrido?: Usurpación de identidad, Pérdida de control sobre sus datos personales

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?:

Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

A fecha de esta notificación, ¿tiene constancia de que se hayan materializado alguno de los daños identificados, con el grado indicado en la cuestión anterior?: Si

Tipos de datos afectados: Datos básicos (Ej nombre, apellidos, fecha de nacimiento), DNI, NIE, Pasaporte y / o cualquier otro documento identificativo, Datos de medios de pago (Tarjeta bancaria, etc.), Datos de contacto

En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales?: 1000

Indique la fecha de detección de la brecha: 08/02/2022

¿Conoce la fecha en la que se inició la brecha? Aproximadamente el 24/08/2021

Indique la fecha en la que se dio por resuelta la brecha: 10/02/2022

¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas?: No serán informados

Las personas afectadas no serán informadas porque: No existe un riesgo alto para sus derechos y libertades

Junto a la notificación se aporta como Anexo I las medidas tomadas para solucionar la brecha y minimizar el impacto:

"Tras la detección inicial, en agosto de 2021, de venta no autorizada de credenciales de acceso a la plataforma ******PLATAFORMA.1****, se adoptaron las siguientes medidas al objeto de mitigar posibles efectos negativos:*

• Reseteo de las contraseñas de los usuarios afectados para acceder a la plataforma ******PLATAFORMA.1****. Esta medida se lleva a cabo de manera continua.*
• Seguimiento de nuevas publicaciones en Facebook. Esta medida se lleva a cabo de manera continua.
• Deshabilitar las sesiones simultaneas en ******PLATAFORMA.1****, de tal manera que no puedan acceder dos o más personas a la vez con un único usuario. Esta medida se implantó en el mes de noviembre de 2021.*
• Ampliar la trazabilidad (logs) de los accesos a ******PLATAFORMA.1*** *para obtener información detallada del uso realizado por parte de los usuarios. Esta medida se implantó a finales del mes de diciembre de 2021.*
• Solicitar la baja de los anuncios de Facebook donde se ofrecía la venta de dichos usuarios. Esta medida se lleva a cabo de manera continua.
Posteriormente, con motivo de los nuevos acontecimientos detectados (venta en Facebook de ciertas bases de datos que contienen, entre otros, datos de clientes de Endesa Energía incluidos en el sistema CRM que alberga datos básicos, de contacto, CUPS, datos relativos al contrato de electricidad o gas y el número de cuenta), se van a implantar, entre otras, las siguientes medidas adicionales:

(...)

SEGUNDO: Con el registro de salida ******REGISTRO.1***, la AEPD notifica a ENDESA el 8 de marzo de 2022 una orden de comunicar el incidente en cuestión a los afectados en el plazo máximo de 30 días conforme al artículo 34 del RGPD. Esta orden informa que la comunicación a los interesados se realizará siguiendo lo previsto en el artículo 34 del RGPD, en particular en su apartado segundo, debiendo describir en lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y las posibles medidas que pudieran ser tomadas por los interesados en función de los riesgos que, en cada caso, pudieran ser identificados por los afectados.

TERCERO: Con fecha 6 de abril de 2022 se recibe en esta Agencia un escrito de ENDESA con número de entrada ******REGISTRO.2***, en el que informa que ha procedido, con fecha 1 de abril de 2022, a remitir una comunicación por correo postal a los potencialmente afectados informando sobre los hechos ocurridos.

Junto con el escrito se aporta:

- Como Documento número 2: el modelo de carta remitida, en español y catalán. El contenido de este modelo en español es el siguiente:

  "31 de Marzo de 2022
  Estimado cliente,
  Nos ponemos en contacto contigo para informarte que hemos detectado un posible acceso indebido a determinados sistemas comerciales de Endesa Energía y que desde el mismo momento que hemos sido conocedores de este hecho, hemos adoptado las oportunas medidas de seguridad, técnicas y organizativas, para evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades de nuestros clientes, con lo que la confidencialidad y la integridad de tus datos personales no se ha visto comprometida.

  *Puedes consultar nuestra política de privacidad en www.endesa.com/es/proteccion-datos-endesa, donde encontrarás la información relativa al tratamiento de tus datos personales. Si lo prefieres, puedes contactar directamente con nuestro Delegado de Protección de Datos enviando una comunicación a ***EMAIL.1 para conocer el detalle de las medidas adoptadas u obtener más información.*

  Aprovechamos para agradecerte la confianza depositada en Endesa.

  Un cordial saludo,
  Endesa Energía."

- Como Documento número 3: la declaración responsable del proveedor ******EMPRESA.2*** en la que reconoce que ha impreso y puesto a disposición de la empresa encargada del servicio postal 760 envíos el día 1 de abril de 2022, y el correspondiente albarán de entrega a Correos, del mismo día.

CUARTO: Con fecha 20 de abril de 2022, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración el citado escrito de notificación de violación de

la seguridad de los datos personales remitido por ENDESA, recibido en esta Agencia el 10 de febrero de 2022, y se ordena a la Subdirección General de Inspección de Datos (SGID) que realice las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

QUINTO: La SGID procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), teniendo conocimiento de los siguientes extremos:

Al objeto de investigar la ocurrencia de los hechos descritos, en fecha 27 de junio de 2022, mediante registro de salida ***REGISTRO.3,** se solicitó información a ENDESA y, en fechas 16 de septiembre de 2022 y 3 de noviembre de 2022 mediante registros de salida ***REGISTRO.4** y ***REGISTRO.5**, respectivamente, se le solicitó ampliación de documentación. Las respuestas a dichos requerimientos tuvieron entrada en la sede electrónica de la Agencia Española de Protección de Datos en fechas 26 de julio de 2022, 7 de octubre de 2022 y 11 de noviembre de 2022 con números de registro ***REGISTRO.6**, ***REGISTRO.7** y ***REGISTRO.8**, respectivamente.

En fecha 27 de septiembre de 2022, mediante registro de salida ***REGISTRO.9** se solicitó información al Delegado de Protección de Datos de ENDESA (***A.A.A.***) y en fecha 19 de octubre de 2022, con número de registro ***REGISTRO.10**, se recibió su respuesta en esta Agencia.

Asimismo, en fecha 20 de octubre de 2022 mediante registro de salida ***REGISTRO.11** se solicitó información a ***EMPRESA.1**, proveedor externo de ENDESA, y en fecha 25 de noviembre de 2022 con número de registro ***REGISTRO.12** tuvo entrada en la sede electrónica de la AEPD su escrito de respuesta.

En su respuesta al requerimiento, con entrada en esta Agencia el 26 de julio de 2022, ENDESA ha manifestado que:

1. ***HERRAMIENTA.1** es una herramienta especialmente diseñada para facilitar el asesoramiento, la atención y venta en los diferentes canales comerciales de Endesa Energía.

Esta herramienta incorpora la información comercial de los productos y servicios que ofrece en cada momento ENDESA (tales como precios, complementos, validez, ofertas o condiciones), contiene información técnica de todos los puntos de suministro, así como ciertos datos identificativos básicos.

2. Los usuarios de ***HERRAMIENTA.1** pueden ser de dos tipos: (i) usuario “interno”, habilitado para los empleados de ENDESA y (ii) usuario “externo”, habilitado para los proveedores externos. No existen otros usuarios externos, como puedan ser clientes.

Tanto los usuarios internos como los usuarios externos tienen acceso a todas las funcionalidades principales de la herramienta.

A su vez, desde el punto de vista funcional la plataforma cuenta con el rol de usuario "básico", y el rol con "perfil de administrador". Es decir, un usuario con "perfil de administrador" también puede ser, a su vez, "interno" o "externo". Únicamente los usuarios que tienen el "perfil de administrador" pueden acceder al menú de administración y realizar cargas de información en el sistema (tales como nuevas ofertas, tarifas o argumentarios). También pueden editar ciertos campos de la herramienta y obtener extracciones e informes.

3. El alta de los usuarios externos e internos la realizan los responsables de cada Cs o de atención en la herramienta de soporte técnico corporativa a la que se accede a través de la Intranet habilitada para todos los empleados internos del Grupo Endesa. Los accesos se solicitan desde Intranet. Se adjunta proceso explicativo como Documento número 2.

Los usuarios externos e internos acceden a la plataforma insertando el usuario y la contraseña asociada.

4. La plataforma permite la opción de introducir el denominado Código Universal de Punto de Suministro (en adelante, "CUPS") o la dirección del punto de suministro, para mostrar la información técnica asociada (se describe en el Documento número 4). En caso de que el cliente ya tenga un contrato en vigor con ENDESA también muestra la siguiente información: nombre y apellidos del titular del punto de suministro, su número de Documento Nacional de Identidad, número de contrato, CUPS, importe de facturación anual, datos técnicos referentes al punto de suministro, datos de consumo y gráfico de utilización. Dentro de la ficha relativa al punto de suministro aparecen una serie de apartados que permiten recomendar al cliente otras tarifas.

5. La brecha se detecta el 8 de febrero de 2022 cuando se constata que en el incidente se han visto afectados datos personales. Con fecha 9 de febrero de 2022 se hace una valoración del alcance de la brecha en la que se considera la existencia de un riesgo para los derechos y libertades de los afectados y la necesidad de notificar la misma a la AEPD. Se aporta, como Documento número 5 la valoración realizada, firmada digitalmente.

Sin embargo, la fecha en la que se advierten ciertas posibles anomalías es el 24 de agosto de 2021, cuando la persona responsable del ***DEPARTAMENTO.1 de ENDESA envió un correo electrónico al responsable de Seguridad de la Información del Grupo Endesa, en el que se informa de un anuncio sospechoso en Facebook. Con este aviso se activa el proceso de análisis e investigación, cuyo primer paso es confirmar la veracidad del anuncio. Se aporta como Documento número 6, el correo electrónico mencionado.

A pesar del seguimiento de esa situación, entre ambas fechas desde ENDESA no se advierten situaciones anómalas de las que pudiera concluirse la existencia de una brecha de seguridad. Es por ello por lo que, sólo es el día 8 de febrero de 2022, cuando tras las investigaciones oportunas, se tuvo conocimiento de la existencia de

ciertas coincidencias entre la base de datos de clientes de ENDESA y las bases de datos en venta en Facebook, y por ello se llevó a cabo una nueva valoración de la que resultó la necesidad de proceder a la notificación a la Agencia Española de Protección de Datos, hecho que se produjo el día 10 de febrero de 2022.

Dichas investigaciones se produjeron con motivo del proceso continuo y sistemático de monitorización de “eventos críticos” y, concretamente, con la realización de actividades de detección temprana de cualquier evento de riesgo que se realiza en la compañía. Estas tareas las realiza ***DEPARTAMENTO.2, de acuerdo con lo establecido en ***DOCUMENTO.1, que se aporta como Documento número 7.

6. Únicamente en los anuncios publicados el día 17 de enero de 2022, por parte del usuario ***B.B.B.***, se detectó afectación a bases de datos de clientes de energía. Se aporta, como Documento número 8, capturas de los anuncios publicados.

7. Para determinar el número de personas potencialmente afectadas por el incidente, se llevó a cabo el siguiente análisis:
(i) Se comprobó la supuesta práctica irregular llevada a cabo por una empresa subcontratista de uno de los proveedores de ENDESA que presta servicios de venta telefónica, y que se verificó no se había extendido a otros proveedores.
(ii) Se acotó el perímetro de análisis a todas aquellas contrataciones efectuadas entre el 1 de julio de 2021, fecha en la que el volumen de ventas de ENDESA sufrió un aumento inusual y no justificado (+500%), y el 15 de octubre de 2021, fecha en la que se rescindió el contrato con el proveedor y, por tanto, dejó de prestar sus servicios.
(iii) Posteriormente, se llevó a cabo un control de calidad y auditoría de las contrataciones objeto de valoración, y se descartaron aquellos casos en los que los propios clientes ya se habían puesto en contacto con ENDESA para realizar acciones propias de sus contratos (por ejemplo, consultas comerciales).

El número de potenciales afectados por el incidente resultante fue: 760 clientes. En cualquier caso, una vez que ENDESA llevó a cabo la comunicación de la brecha a los afectados, tan sólo se ha recibido un correo electrónico por parte de uno de los destinatarios de dicha comunicación, el día 6 de abril de 2022. Se solicitó la documentación acreditativa de su identidad, y no consta respuesta por su parte. Dicho extremo se acredita con el Documento número 9.

8. A pesar de no ser posible determinar el posible objetivo buscado por las personas que facilitaban la venta de credenciales para acceso a la plataforma ******HERRAMIENTA.1***, así como, en su caso, la venta de bases de datos de clientes de ENDESA, se considera que las consecuencias de la brecha se limitan a que las personas afectadas podrían encontrar ciertos inconvenientes, muy limitados y, en todo caso, reversibles.

Debido al objetivo, aparentemente fraudulento, de sustracción de datos, las consecuencias para los clientes afectados serían fundamentalmente la venta de sus datos para la realización de llamadas comerciales, así como para el envío de correos y SMS, ofreciendo la posibilidad de cambiar de compañía comercializadora de energía, lo que, en los peores escenarios y de llegar a materializarse, podría resultar en el cambio de empresa comercializadora sin su consentimiento.

9. Durante el análisis del incidente se realizaron tres evaluaciones, a medida que paulatinamente, se fue obteniendo información sobre el mismo, dentro del proceso de constante seguimiento que se estaba llevando a cabo desde que se advirtieron las posibles anomalías. Las valoraciones que se llevaron a cabo fueron las siguientes:

El 13 de septiembre de 2021, se realiza la primera valoración donde se recoge la información obtenida hasta ese momento. En base a dicha información se consideró que el riesgo derivado era bajo, debido principalmente a que no se tenía constancia alguna de que se hubiera materializado el acceso fraudulento a la plataforma ******HERRAMIENTA.1***. Se aporta, como Documento número 10, la valoración realizada con fecha 13 de septiembre de 2021, firmada digitalmente.

El 28 de septiembre de 2021, se realiza una segunda valoración donde se completa la información de la primera y se considera que el riesgo derivado continúa siendo bajo. Se aporta, como Documento número 11, la valoración realizada con fecha 28 de septiembre de 2021, firmada digitalmente.

El 9 de febrero de 2022, se realiza la última valoración. En ella se refleja la detección de ciertos anuncios en Facebook de características similares a los anteriores, en los que aparecen bases de datos de clientes de ENDESA. Tras varios análisis de las bases de datos publicadas, se detectan coincidencias entre los datos que aparecen en dichas bases de datos y los que puedan estar incluidos en el sistema comercial de ENDESA ******HERRAMIENTA.2***). Por esta razón se considera oportuno comunicar el incidente a la Agencia Española de Protección de Datos. Se hace referencia a la valoración realizada con fecha 9 de febrero de 2022, firmada digitalmente, aportada anteriormente como Documento número 5.

En consecuencia, y tal y como se ha expuesto anteriormente, a raíz de los nuevos hechos detectados el día 8 de febrero de 2022, se llevó a cabo una valoración del incidente en la que se tuvo en cuenta la variación con respecto a la situación anterior y, de manera proactiva, se comunicó el incidente a la Agencia Española de Protección de Datos el día 10 de febrero de 2022.

10. La brecha ha sido provocada por la aparente venta fraudulenta de credenciales de la plataforma ******HERRAMIENTA.1***. Estas credenciales estaban asignadas a proveedores de Endesa Energía, como usuarios externos de la plataforma, para facilitar las tareas captación, asesoramiento y atención al cliente.

En este sentido, se hace referencia al Documento número 8, aportado anteriormente, en el que se incluyen imágenes de los anuncios de ventas de credenciales.

11. ENDESA tuvo conocimiento del posible uso ilícito de las credenciales a través del correo de uno de los proveedores donde se indican irregularidades por varios de sus trabajadores, en ese mismo correo se indican cinco usuarios que han sido empleados de forma aparentemente irregular.

Por otra parte, se identifican otros cuatro usuarios que pudieran estar comprometidos, detectados en los videos de demostración y en las capturas de los anuncios publicados. A continuación, se detallan todos los usuarios comprometidos:

- ******USUARIO.1***

- ***USUARIO.2**
- ***USUARIO.3**
- ***USUARIO.4**
- ***USUARIO.5**
- ***USUARIO.6**
- ***USUARIO.7**
- ***USUARIO.8**
- ***USUARIO.9**

12. Tal y como se ha expuesto anteriormente, ENDESA no ha recibido ninguna reclamación por parte de los clientes potencialmente afectados por este incidente.

13. Se aporta, como Documento número 12, el análisis de riesgos realizado sobre el acceso y uso de ***HERRAMIENTA.1** y, como Documento número 13, el análisis de riesgos del acceso y uso de ***HERRAMIENTA.2**.

14. ENDESA, como parte del Grupo Endesa cuenta con una serie de normas y estándares de seguridad para garantizar la protección de los datos personales, basados, principalmente, en los siguientes elementos: (i) un marco de ciberseguridad, (ii) normativa interna sobre ciberseguridad.

[…]

- Concretamente las medidas implementadas en las aplicaciones objeto de la presente brecha de seguridad consisten, ***(…)***.

15. Entre las distintas actividades y medidas de seguridad distintas medidas de seguridad que existían en ***HERRAMIENTA.2** antes del incidente destacan las siguientes:

(…).

Se aporta, como Documento número 17, la acreditación de que la aplicación ***HERRAMIENTA.2** se encontraba integrada (...) en la fecha del incidente.

16. Entre las distintas actividades y medidas de seguridad que se tenían implementadas en la plataforma ***HERRAMIENTA.1** antes del incidente destacan las siguientes:

(…)

17. Con el objetivo de reducir el impacto de la incidencia detectada, y prevenir nuevas brechas de este tipo, se han adoptado las medidas adicionales que se detallan a continuación.

A medida que se fue desarrollando el incidente y advirtiéndose sus posibles efectos, se

implantaron las siguientes medidas para reforzar la seguridad de las aplicaciones ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***:

(i) Para el caso de ******HERRAMIENTA.2***, se ha activado el factor múltiple de autenticación en la aplicación, por lo que cada usuario, además de la introducción de sus credenciales en el área de acceso de la aplicación, deberá facilitar un código de seguridad recibido a través de un teléfono móvil previamente registrado. Se adjunta documento número 24.

Adicionalmente, también se ha desactivado la opción de multisesión. Por tanto, cada usuario únicamente podrá tener una sesión activa (se adjunta Documento número 25).

(ii) Para el caso de ******HERRAMIENTA.1***, tras el incidente, se han adoptado las siguientes medidas de
seguridad:

- Se ha activado el factor múltiple de autenticación en la aplicación (se adjunta Documento número 26).
- Se ha desactivado la opción de multisesión. Por tanto, cada usuario únicamente podrá tener una sesión activa (se adjunta Documento número 27).
- Adicionalmente, se han mejorado los logs (trazabilidad) que se recogen por parte de la aplicación en el entorno de producción. Esto permite tener mayores evidencias de las operaciones de los usuarios para el análisis y diagnóstico futuros. Se adjunta Documento número 28.

Por último, el último anuncio identificado relacionado con el uso ilícito de credenciales de la plataforma ******HERRAMIENTA.1*** fue el 13 de diciembre de 2021, así como de la última publicación identificada de la venta de bases de datos de clientes de electricidad y gas se produjo en el mes de enero de 2022 (se adjunta Documento número 29). En consecuencia, no se han detectado nuevas publicaciones relacionadas con este incidente con fecha posterior a la notificación realizada el día 10 de febrero de 2022.

18. Se aporta, como Documento número 30, la copia del registro de incidentes donde aparecen las valoraciones realizadas durante los años 2021 y 2022 relacionadas con el presente caso.

19. En fecha 15 de septiembre de 2022 desde la SGID se comprueba que siguen publicados en Facebook anuncios identificados por ENDESA donde se ofrece la venta de credenciales de acceso a *****HERRAMIENTA.1** y bases de datos (ver en el expediente el documento de Diligencia del 16 de diciembre de 2022).

En su respuesta al requerimiento, con entrada en esta Agencia el 7 de octubre de 2022, ENDESA ha manifestado que:

20. ENDESA identificó en los propios anuncios y videos demostrativos publicados en la red social Facebook cuatro usuarios de la herramienta ******HERRAMIENTA.1*** (en adelante "******HERRAMIENTA.1***") que, por tanto, estaban comprometidos.

Se aporta como Documento número 2, capturas de los anuncios publicados en Facebook en los que se observa, en el margen superior derecho, la identificación de los usuarios utilizados para acceder a ******HERRAMIENTA.1***.

Asimismo, los otros cinco usuarios de ******HERRAMIENTA.1*** comprometidos fueron identificados por la empresa subcontratista de un proveedor de ENDESA, que alertó sobre el uso irregular que, algunos de sus asesores, habían realizado con ciertas credenciales de acceso a ******HERRAMIENTA.1*** que habían adquirido de manera ilícita (se adjunta Documento número 3).

21. Por otra parte, los usuarios comprometidos identificados habían sido asignados a alguna de las siguientes empresas proveedoras de Endesa Energía:

- ******EMPRESA.3***
- ******EMPRESA.4***
- ******EMPRESA.5***
- ******EMPRESA.6***
- ******EMPRESA.7***
- ******EMPRESA.8***

22.- El proveedor de ENDESA que prestaba servicios de venta telefónica cuya empresa subcontratista llevó a cabo la supuesta práctica irregular fue ******EMPRESA.1*** y la empresa subcontratista a la que encargó la prestación de parte de los servicios encomendados fue ******EMPRESA.9***.

Se aporta como Documento número 4 copia del contrato suscrito entre ENDESA y ******EMPRESA.1***.

En relación con la subcontratación de ******EMPRESA.9***, se aporta, como Documento número 5, extracto de las condiciones generales de contratación aplicables al contrato suscrito entre ENDESA y ******EMPRESA.1*** relativo al régimen de subcontratación y, como Documento número 6, autorización emitida por ENDESA para llevar a cabo la mencionada subcontratación de ******EMPRESA.9***.

23. Desde la detección de los anuncios de venta ilegal de credenciales de acceso a la herramienta ******HERRAMIENTA.1*** en la red social Facebook, como primera medida, se solicitó en repetidas ocasiones la baja de los anuncios a través del formulario-tipo habilitado para dicho fin por Facebook (tal y como se acredita a modo de ejemplo con el Documento número 7). Como resultado de ello, Facebook inhabilitó el acceso o eliminó el contenido de los anuncios, pero no de todos ellos. Se aporta como Documento número 8, algunas de las respuestas facilitadas por Facebook en este sentido.

En segundo lugar, con el objetivo de agilizar la eliminación de todos los anuncios detectados, con fecha 4 de febrero de 2022, se envió mediante burofax una comunicación escrita a FACEBOOK SPAIN S.L. (en adelante “FB SPAIN”), la cual se aporta como Documento número 9, poniendo en su conocimiento la publicación por parte de usuarios de la plataforma de determinada información que podría ser constitutiva de un delito y solicitando su colaboración para su eliminación. Con fecha 8 de febrero de 2022, dicha comunicación fue respondida mediante correo electrónico en el que se indicaba que FB SPAIN no era la entidad competente para resolver la

cuestión, sino FACEBOOK IRELAND LIMITED, y solicitando que se dirigiera la comunicación a dicha entidad (se aporta Documento número 10). Finalmente, con fecha 28 de febrero de 2022, ENDESA envió un nuevo comunicado (se aporta Documento número 11), reiterando nuevamente su escrito inicial a FB SPAIN.

24. En el análisis que se llevó a cabo para la correcta identificación de los clientes cuyos datos aparentemente habían sido sustraídos sin autorización de la herramienta ******HERRAMIENTA.3*** y, por tanto, podían eventualmente haber sido tratados sin su consentimiento, se realizaron las siguientes actuaciones:

> i. En primer lugar, una vez el proveedor ******EMPRESA.1*** puso en conocimiento de ENDESA la práctica irregular cometida por personal de ******EMPRESA.9*** y se realizaron las comprobaciones oportunas, se verificó que dicha práctica no se extendía a otros proveedores.
> ii. En segundo lugar, una vez identificado el posible origen de las contrataciones supuestamente irregulares, se procedió a acotar el alcance temporal de sus actuaciones, verificándose que a partir de 1 de julio de 2021 el volumen de ventas de ENDESA experimentó un aumento inusual no justificado (concretamente, las ventas se incrementaron en más del 500%) lo cual podía ser representativo de las actuaciones irregulares del personal contratado por ******EMPRESA.9***. Con fecha 15 de octubre de 2021 se cesó la actividad de dicho subcontratista – como consecuencia de la rescisión del contrato con ******EMPRESA.9*** –, limitando, por tanto, el perímetro temporal de análisis de las contrataciones al período comprendido entre el 1 de julio y 15 de octubre de 2015.
> iii. Finalmente, se llevó a cabo un control de calidad y auditoría de las contrataciones llevadas a cabo por ******EMPRESA.9*** en el perímetro temporal fijado. En dicho análisis, se descartaron aquellos casos en los que los propios clientes en cuyo nombre se había efectuado una contratación en la que intervino ******EMPRESA.9*** – en el período de tiempo delimitado –, se habían puesto en contacto con ENDESA para realizar acciones propias de sus contratos (por ejemplo, consultas comerciales), lo cual era indicativo de que los propios clientes eran conocedores de sus contratos y no manifestaron objeción alguna.

25. Si bien es el 8 de febrero de 2022 cuando, tras las investigaciones oportunas, se tuvo conocimiento del alcance de la brecha de seguridad al constatar la existencia de coincidencias entre la base de datos de clientes de ENDESA y las bases de datos en venta en Facebook, ENDESA, con fecha 31 de enero de 2022, ante el incumplimiento de los procedimientos establecidos, tomó la decisión de rescindir el contrato a ******EMPRESA.1*** por vulneración de los compromisos asumidos ante Endesa Energía por dicha contratista.

Asimismo, los empleados de ******EMPRESA.9*** que presuntamente habían hecho un uso irregular de credenciales de acceso a ******HERRAMIENTA.1*** fueron despedidos según fue comunicado por la propia empresa en el correo de fecha 20 de octubre de 2021 y denunciados ante las autoridades locales (se aporta Documento número 12).

En su respuesta al requerimiento, con entrada en esta Agencia el 19 de octubre de 2022, el DPD de ENDESA ha manifestado que:

26. La función de Delegado de Protección de Datos se regula de acuerdo con lo establecido en ***DOCUMENTO.2 (actualmente en trámite de su cuarta revisión). De acuerdo con dicha norma interna y otras del Grupo, corresponde al Delegado de Protección de Datos el asesoramiento en materia de Protección de Datos Personales cooperando con otras áreas de la organización en aquellas materias que puedan referirse -entre otras- a incidentes de seguridad.

Se trata de una tarea desarrollada con carácter continuo, toda vez que la coordinación con las áreas afectadas de la organización es permanente y opera a través de diversos mecanismos como pueden ser reuniones periódicas, emisiones de informes o participación en comités.

27. Como parte de dicho asesoramiento continuo, tal y como consta en la información incluida en los informes correspondientes a las valoraciones del incidente realizadas con fechas 13 y 28 de septiembre de 2021, y 9 de febrero de 2022, en su condición de Delegado de Protección de Datos y junto con el área de Seguridad, el área de Sistemas, el equipo de Ventas de ENDESA y ***DEPARTAMENTO.3 tuvo participación en las diferentes evaluaciones llevadas a cabo en relación con la Brecha.

Cabe señalar que en los informes correspondientes a las valoraciones realizadas los días 13 y 28 de septiembre de 2021, se puso de manifiesto que "…desde ***DEPARTAMENTO.4 se señala la necesidad de continuar con la investigación al objeto de poder realizar una nueva valoración del incidente, por considerar que la información aportada no es completa y el presente análisis tiene carácter preliminar".

Finalmente, en el informe correspondiente a la valoración del día 9 de febrero de 2022, se expuso que "…tras realizar una valoración, en tiempo y forma, del alcance del incidente de seguridad y de las posibles repercusiones para los derechos y libertades de los interesados afectados, se adopta la decisión preliminar de comunicar el incidente de seguridad a la autoridad de control". Por tanto, como consecuencia del asesoramiento efectuado por el Delegado de Protección de Datos, se procedió a comunicar la Brecha ante la Agencia Española de Protección de Datos el día 10 de febrero de 2022.

28. El Delegado de Protección de Datos envió un correo electrónico el día 9 de febrero de 2022, en el que insistía en la necesidad de llevar a cabo la notificación de la Brecha (se aporta como Documento número 1). Como consecuencia de tal solicitud, la comunicación se realizó al día siguiente tras recopilar en su totalidad la información solicitada en el formulario de notificación de la Agencia Española de Protección de Datos.

29. Como parte del asesoramiento constante, como Delegado de Protección de Datos, personalmente y por medio del equipo de la oficina de protección de Datos que dirige, se hizo un seguimiento constante de la Brecha, particularmente al objeto de determinar la procedencia o no de comunicación a la vista de las novedades que pudieran producirse o los criterios que pudieran emanar de esa Agencia.

30. Como Delegado de Protección de Datos, junto a otras personas, participó en las reuniones mantenidas con motivo de la notificación remitida a ENDESA por la Agencia

Española de Protección de Datos el día 8 de marzo de 2022 (se aporta Documento número 2), en la que ordenaba al responsable del tratamiento a llevar a cabo la comunicación de la brecha de seguridad a los interesados en el plazo máximo de 30 días. Concretamente, con fecha 9 de marzo de 2022 se mantuvo una primera reunión para tratar este asunto, y el día 28 de marzo de 2022 se celebró una segunda reunión en la que se acordó cómo realizar el envío de la comunicación.

31. Durante el plazo otorgado para llevar a cabo la comunicación, desde el equipo del Delegado de Protección de Datos bajo su responsabilidad se asesoró acerca de cómo debería llevarse a cabo la comunicación. A modo de ejemplo, se aporta, como Documento número 3, un correo electrónico de fecha 16 de marzo de 2022 remitido por uno de los miembros del equipo del Delegado de Protección de Datos bajo su responsabilidad, en el que se ponía de manifiesto la necesidad de incluir ciertos aspectos en la comunicación que se envió a los interesados el día 1 de abril de 2022.

Igualmente, se aporta como Documento número 4, un correo electrónico remitido en su calidad de Delegado de Protección de Datos en el que insistía en la necesidad de priorizar el envío de la comunicación a los afectados sobre la Brecha con respecto a otras comunicaciones que se preveían llevar a cabo ese mismo mes (éstas últimas sobre cuestiones que no estaban relacionadas con la Brecha).

En su respuesta al requerimiento, con entrada en esta Agencia el 11 de noviembre de 2022, ENDESA ha manifestado que:

32. Durante la investigación iniciada a finales del mes de agosto del año 2021, se identificaron un total de 440 anuncios en la red social Facebook en los que se ofrecía el alquiler y/o venta de credenciales de acceso a la herramienta de ENDESA ******HERRAMIENTA.1***.

Los dos usuarios identificados desde cuyos perfiles de Facebook se publicaron dichos anuncios fueron los correspondientes a "***B.B.B.***" (quien, presumiblemente, también realizó publicaciones bajo el perfil de ***C.C.C.***) y "***D.D.D.***". En el trascurso de la investigación, el área de Seguridad de la Información de ENDESA realizó un contacto con el usuario ***B.B.B.*** quien ofreció la venta de credenciales para acceder a ******HERRAMIENTA.1*** a cambio de un pago mensual. Asimismo, indicaba que disponía de diferentes usuarios para su venta.

Gracias al proceso continuo y sistemático de seguimiento de "eventos críticos" de ENDESA se identificaron durante el mes de enero del año 2022 nuevos anuncios publicados por el usuario ***B.B.B.***, donde se ofrecía la venta de bases de datos de clientes de energía de diversas empresas suministradoras del sector. Tras las investigaciones oportunas, en el mes de febrero del año 2022, se verificó la existencia de ciertas coincidencias entre esa base de datos y la base de datos de clientes de ENDESA albergada en la aplicación ******HERRAMIENTA.2*** – motivo por el que se llevó a cabo una valoración que resultó en la necesidad de proceder a la notificación a la Agencia Española de Protección de Datos, hecho que se produjo el día 10 de febrero de 2022.

Se aporta como Documento número 2, capturas de varios de los anuncios de Facebook en los que, ***B.B.B.*** o ***D.D.D.***, ofrecían el alquiler o venta de las credenciales para acceder a la plataforma ******HERRAMIENTA.1***.

Como consecuencia de las conversaciones mantenidas entre los responsables de ENDESA y sus proveedores y, a su vez, de éstos con sus subcontratistas, se ha tenido conocimiento de que tras el usuario "***B.B.B.***" / "***C.C.C.***" se encuentra ***C.C.C.***, quien, tal y como ha sido trasladado a esta Oficina, fue empleado hasta el año 2016 de ******EMPRESA.10***. Esta sucursal nunca ha prestado servicios para ENDESA y consecuentemente ***C.C.C.*** nunca tuvo asignado a su nombre un usuario de acceso a las aplicaciones de ENDESA (se aporta Documento número 3).

Por su parte, el usuario "***D.D.D.***" se corresponde con la trabajadora de ******EMPRESA.11***, empresa subcontratista en ***PAÍS.1 del proveedor ******EMPRESA.12*** quien presta servicios para ENDESA, ***D.D.D.***, quien, sin embargo, se dio de baja al inicio del año 2020 (se aporta Documento número 4.

Según la información que ha sido trasladada a esta Oficina por ENDESA, no figura en los sistemas internos de la compañía ningún registro de alta de un usuario a nombre de ***D.D.D.*** (se aporta Documento número 5).

Consecuentemente, los dos anunciantes que vendían en Facebook credenciales de usuarios de ENDESA no eran extrabajadores de proveedores (o subcontratistas de éstos) de ENDESA en el momento de la publicación de anuncios (uno nunca lo fue y otra, dejó de trabajar para una subcontrata de un proveedor de ENDESA mucho antes de la publicación de los anuncios de los que trae causa la Brecha).

33. A continuación, se reflejan los usuarios comprometidos puestos a la venta junto con el proveedor al que fueron asignados:

******USUARIO.1***	******EMPRESA.13*** **(en adelante, ****EMPRESA.13*)**
******USUARIO.9***	******EMPRESA.14*** **(en adelante, ****EMPRESA.14*)**
******USUARIO.2***	******EMPRESA.8.*** **(en adelante, ****EMPRESA.8*)**
******USUARIO.10***	******EMPRESA.15***

En relación con los proveedores ******EMPRESA.13, ***EMPRESA.14 y ***EMPRESA.8***, los tres prestaban servicios de venta a ENDESA por vía telefónica mediante llamadas salientes de la compañía. Tal y como se acredita mediante la declaración realizada por cada uno de los responsables territoriales de ENDESA que gestionaban la relación con dichos proveedores, las cuales se aportan como Documento número 6, la comunicación relativa a la Brecha y al uso indebido de los usuarios de acceso a las aplicaciones de ENDESA que les habían sido asignados, se llevó a cabo por medio de conversaciones y reuniones telefónicas.

En relación con el proveedor ******EMPRESA.15***, éste prestaba servicios de atención y venta telefónica a ENDESA, atendiendo las llamadas que, sin previa intervención comercial de ENDESA, realizan los interesados. Tal y como se acredita con el Documento número 7, el responsable de operaciones, de forma inmediata tras conocer los hechos, se puso en contacto con el proveedor para solicitarle

explicaciones sobre lo ocurrido y la toma inmediata de medidas con el usuario implicado.

34. A continuación, se muestra para cada uno de los usuarios los datos relativos al alta y a la baja en la herramienta ******HERRAMIENTA.1***, así como el rol asignado a cada usuario y las funciones y permisos de acceso otorgados.

Usuario	Proveedor al que se le asignó el usuario	Fecha de petición de alta	Fecha de reseteo o deshabilitación	Fecha de retirada y eliminación en sistemas	Rol	Funciones y permisos otorgados
******USUARIO.13***	******EMPRESA.13***	11/03/2021	15/02/2022	24/08/2022	Usuario	Consulta
******USUARIO.94***	******EMPRESA.14***	09/12/2021	15/02/2022	24/08/2022	Usuario	Consulta
******USUARIO.11***	******EMPRESA.8***	26/11/2019	19/11/2021	19/11/2021	Usuario	Consulta
******USUARIO.10***	******EMPRESA.15***	21/12/2020	10/09/2021	24/08/2022	Usuario	Consulta
******USUARIO.10***	******EMPRESA.16***	20/10/2020	03/09/2021	24/08/2022	Usuario	Consulta
******USUARIO.10***	******EMPRESA.15***	15/08/2021	29/11/2021	04/03/2022	Usuario	Consulta
******USUARIO.10***	******EMPRESA.16***	20/10/2020	21/09/2021	24/08/2022	Usuario	Consulta
******USUARIO.10***	******EMPRESA.17***	28/10/2020	24/08/2022	24/08/2022	Usuario	Consulta

Se aporta como Documento número 8, capturas de pantalla de los sistemas en acreditación de las fechas de alta, así como de la retirada y eliminación en sistemas. Asimismo, se aporta como Documento número 9, diversas comunicaciones en las que se acredita la fecha en las que los responsables de asignación de dichos usuarios solicitaron o informaron sobre la inhabilitación o el reseteo de las credenciales comprometidas.

35. En relación con la herramienta ******HERRAMIENTA.2***, a continuación, se muestran los usuarios comprometidos que tenían permisos de acceso a dicha herramienta, junto con los datos relativos al alta y a la baja, así como el rol asignado a cada usuario y las funciones y permisos de acceso otorgados.

Usuario	Proveedor al que se le asignó el usuario	Fecha de petición de alta	Fecha último acceso	Fecha de eliminación en sistemas	Rol	Funciones y permisos otorgados
******USUARIO.10***	******EMPRESA.15***	12/04/2021	09/09/2021	10/09/2021	***ROL.1	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
******USUARIO.10***	******EMPRESA.16***	19/02/2020	26/11/2021	12/01/2022	***ROL.3	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
******USUARIO.10***	******EMPRESA.15***	06/03/20	18/02/2022	16/03/2022	***ROL.1	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
******USUARIO.10***	******EMPRESA.16***	23/10/2020	25/11/2021	12/01/2022	***ROL.3	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
******USUARIO.10***	******EMPRESA.17***	20/07/2020	3/12/2021	17/02/2022	***ROL.2	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).

Se aporta como Documento número 10, capturas de los sistemas, así como comunicaciones en acreditación de las fechas de alta o solicitud de alta, así como del último acceso y de la baja y de eliminación de los usuarios en la herramienta ******HERRAMIENTA.2***.

36. Los usuarios identificados tenían un rol de “usuario” en la herramienta ******HERRAMIENTA.1***, con permiso asignado de consulta, por lo que únicamente podían visualizar (i) en relación con todos consumidores, clientes o no de ENDESA, datos técnicos – como potencia, tensión, consumos estimados – asociados al punto de suministro al introducir la dirección o el denominado Código Universal de Puntos de Suministro (en adelante “CUPS”); y (ii) en caso de que se tratara de clientes de ENDESA con un contrato en vigor, podían acceder a la siguiente información: nombre y apellidos del titular del punto de suministro, número de Documento Nacional de

Identidad, número de contrato, CUPS, importe de facturación anual, indicador de deuda, información sobre precios, datos técnicos referentes al punto de suministro, datos de consumo y gráfica de utilización.

El volumen aproximado de puntos de suministro que potencialmente se puede consultar – uno a uno, de manera individual – desde la herramienta ******HERRAMIENTA.1***, siempre y cuando se introduzca previamente un CUPS o una dirección, es de 30, 6 millones de puntos de suministro de electricidad y de 8,6 millones de puntos de suministro de gas. En el caso de clientes con un contrato en vigor, el volumen aproximado que un usuario puede consultar, bajo las mismas premisas indicadas anteriormente, es de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas.

En relación con la herramienta ******HERRAMIENTA.2***, los usuarios identificados comprometidos podían acceder a los datos relativos a clientes con un contrato en vigor con ENDESA, siendo el volumen aproximado durante el periodo comprendido entre el 1 de julio de 2021 y el 15 de octubre de 2021, de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas. En cuanto a la tipología de datos que podía visualizar, principalmente son: nombre y apellidos del titular del punto de suministro, dirección postal, número de Documento Nacional de Identidad, CUPS, teléfono, correo electrónico, productos contratados, facturas, número de cuenta bancaria, calidad del crédito, deudas con la compañía.

Finalmente, tal y como ha sido trasladado a esta Oficina, en relación con los usuarios comprometidos y con el periodo en que la Brecha se desarrolló no se mantiene un registro (logs) del uso de las herramientas ******HERRAMIENTA.1*** o ******HERRAMIENTA.2***. Es necesario indicar que, con motivo de la Brecha se adoptaron una serie de medidas entre las que se encuentra la ampliación de la trazabilidad (logs) de los accesos a ******HERRAMIENTA.1*** para obtener información detallada del uso realizado por parte de los usuarios – medida que se implantó a finales del mes de diciembre de 2021.

37. Se aporta como Documento número 11, copia del burofax remitido a ******EMPRESA.1*** comunicando la rescisión del contrato que ha sido trasladado a esta Oficina por la unidad correspondiente responsable de las actuaciones realizadas al respecto.

En su respuesta al requerimiento, con entrada en esta Agencia el 25 de noviembre de 2022, ******EMPRESA.1*** ha manifestado que:

38. En relación con la práctica irregular llevada a cabo por personal de la empresa subcontratada ******EMPRESA.9 (***EMPRESA.9)***, descripción detallada y cronológica de los hechos:

> - 19/10/2021. ******EMPRESA.1*** detecta que un usuario del agente ******EMPRESA.9*** ha intentado realizar un alta fraudulenta ya que, entre otras cuestiones, se puede apreciar que el número de teléfono utilizado para enviar al cliente el SMS de confirmación de venta (el cliente debe responder a este SMS para confirmar la venta) es coincidente con otro número de teléfono utilizado con la misma finalidad para otro cliente.

Esto quiere decir que es posible que el cliente no hubiera aceptado el contrato, habiéndose aceptado el mismo mediante confirmación de SMS por una persona diferente al titular de la contratación.

- 19/10/2021. Ante la sospecha de que esto pudiera haberse realizado por parte de otros agentes de ******EMPRESA.9***, ******EMPRESA.1*** inicia un proceso de auditoría interna y comunica a la persona Responsable de su cuenta en ENDESA lo sucedido telefónicamente, enviando también un email (se adjunta el e-mail como imagen 1 en el Documento 2) con las primeras averiguaciones realizadas y las primeras medidas tomadas al respecto. Este mismo día se lleva a cabo el cierre total de todos los usuarios de ******EMPRESA.9*** y el acceso a cualquier herramienta de la campaña de ENDESA y se inicia una auditoría interna para valorar el volumen de clientes afectados por contrataciones fraudulentas.

- 19/10/2021. ******EMPRESA.1*** envía una comunicación a todos sus Subagentes (******EMPRESA.9*** y resto de colaboradores) participantes en la campaña de ENDESA informando de lo sucedido, de la auditoría interna abierta y de las consecuencias de realizar este tipo de prácticas delictivas (se adjunta el e-mail como imagen 2 en el Documento 2).

- 20/10/2021. ******EMPRESA.1***, tras la auditoría realizada, envía una comunicación a ENDESA indicando las operaciones afectadas por la práctica fraudulenta de ******EMPRESA.9***, identificándose 137 contrataciones realizadas y otras 7 operaciones pendientes de validación por parte de ENDESA que no han llegado a darse de alta. También se identifican y se bloquean, para que no se tramite su contratación, otras 172 órdenes que están pendientes de validar por el back office de ******EMPRESA.9***. Además, en esta comunicación se indican las medidas que se pretenden seguir llevando a cabo en los próximos días para detectar cualquier otra irregularidad adicional.

Entre estas medidas, se propone a ENDESA realizar llamadas a los clientes que hayan podido verse afectados para confirmar tanto la legalidad de la contratación como la comprobación del número de cuenta facilitado. No obstante, ENDESA prohíbe a ******EMPRESA.1*** realizar estas llamadas comerciales indicando que procederán ellos mismos a verificar las contrataciones (se adjunta la comunicación enviada a Endesa como imagen 3 en el Documento 2).

Por otra parte, en esta comunicación realizada a ENDESA se remite adjunto un e-mail del gerente de ******EMPRESA.9*** comunicando a ******EMPRESA.1*** las denuncias presentadas, ante la Policía de ***PAÍS.1, contra sus comerciales implicados en esta práctica fraudulenta, así como los números de teléfono utilizados de forma fraudulenta para la confirmación de las ventas mediante el envío de SMS.

- 25/10/2021. Para evitar que se refugiasen en otras subcontratas los trabajadores de ******EMPRESA.9***, el día 25 de octubre, ******EMPRESA.1***,

procedió a cerrar los sistemas y a comunicar de forma fehaciente al resto de agentes de la zona el cierre de la campaña.

- 27/10/2021. ******EMPRESA.1*** recibe un email del gerente de ******EMPRESA.9*** detallando las averiguaciones realizadas sobre la práctica fraudulenta llevaba a cabo por algunos de sus agentes y su modus operandi ya que algunos de los comerciales han decidido colaborar tras ver la denuncia presentada contra ellos ante la Policía. En este e-mail se detallan las tres formas de operar, según la gerencia de ******EMPRESA.9***, de los comerciales.

Se detalla a continuación las formas de operar detalladas en el e-mail:

1. Contactaban con el cliente y explicaban el producto, de estar de acuerdo y ser consciente con la contratación procedían con el cierre. Sin embargo, el cliente ponía la objeción indicando que no podían responder el sms por diferentes motivos (bloqueado para sms, no tenía móvil, no tenía batería, próximo a viajar, etc). Lo que hacía el comercial era conseguir un número de otro cliente que era de endesa y pedían a este último que respondiera el sms.

2. Por medio de internet los comerciales contrataban el programa ******PLATAFORMA.1*** de ENDESA. Como se puede apreciar en las imágenes 4.1, 4.2, 4.3 y 4.4 adjuntas en el Documento 2, diferentes personas "comercializaban" accesos al programa ******PLATAFORMA.1*** de ENDESA. Lo que hacían los comerciales es utilizar esta herramienta para poder extraer datos de clientes de ENDESA, por lo que las grabaciones las hacían con otras personas.

3. Otro caso fueron clientes que por algún momento no quisieron pasar textos por ser muy largos, se cansaron de recibir varias llamadas. Lo que hicieron en este caso es una simulación de ventas con otras personas y el mensaje también fue respondido por otros (se adjunta el e-mail enviado por ******EMPRESA.9*** y recibido por ******EMPRESA.1*** como imagen 4 del Documento 2).

39. Se adjunta como Documento 1 el informe de evaluación de la brecha presentado en el Comité interno de riesgos. Cabe tener en cuenta que la brecha se gestiona en calidad de Encargado de Tratamiento habiéndose colaborador con el responsable en la medida en que este así lo solicitó y permitió dicha colaboración.

40. Se adjunta como Documento 3 la copia del Registro de las actividades de tratamiento de datos personales de los clientes de ENDESA efectuadas por parte de ******EMPRESA.1*** en calidad de encargado del tratamiento, en cuanto a tratamientos referentes a venta telefónica.

41. Listado de los usuarios comprometidos en la práctica irregular:

- Usuarios de ******EMPRESA.1*** con acceso a: ******EMPRESA.1*** disponía de un único usuario de acceso (******USUARIO.11***) a la herramienta de ******HERRAMIENTA.4***.

- Usuarios de ******EMPRESA.1*** para realizar la carga masiva de solicitudes a través de la herramienta ******HERRAMIENTA.4***: ******EMPRESA.1*** disponía de un único usuario de acceso (******USUARIO.12***).

- Usuarios de ******EMPRESA.9*** autorizados para cargar solicitudes de venta en crm de ******EMPRESA.1***. Se aporta listado de todos los 46 usuarios relacionados son a través de los cuales se han cargado las ventas fraudulentas.

42. Con el fin de entender la relación entre las partes intervinientes en la contratación de productos y servicios de ENDESA es conveniente aclarar que:

- Cada usuario de ******EMPRESA.9*** disponía de un usuario independiente en el CRM de ******EMPRESA.1*** para realizar la carga de las solicitudes de contrataciones que hubieran formalizado a través de las llamadas de captación comercial realizadas. A través de su usuario, cada agente cargaba en el CRM de ******EMPRESA.1*** la siguiente información:
  - Los datos necesarios para realizar la contratación por parte del cliente.
  - La grabación de la llamada de principio a fin comprensiva de oferta comercial + textos legales+ consentimiento del cliente a la oferta comercial y contratación de los Productos y Servicios Ofertados y los archivos necesarios para la aportación de la llamada completa.

  Una vez cargada esta información por parte de cada agente se generaba, en los sistemas de ******EMPRESA.1***, un Excel con los datos necesarios para que el Back Office de ENDESA pudiera gestionar los datos en los sistemas comerciales de ENDESA. Los datos con los que se generaba el Excel se obtenían de la carga que el agente había hecho previamente el Crm de ******EMPRESA.1***.

  Además, se generaba un certificado por un tercero de confianza con el SMS enviado para la confirmación de la venta donde se certificada, además, el SI o el NO del cliente a la Oferta Comercial.

- Una vez realizado el procedimiento anterior, ******EMPRESA.1*** procedía, diariamente, a cargar masivamente vía ftp en la herramienta de ******HERRAMIENTA.4***, propiedad de ENDESA, toda la información descrita anteriormente, es decir, la grabación de la llamada, el certificado por tercero de confianza del SMS de aceptación de la venta por parte del cliente y el Excel con la información del cliente para la gestión por parte del Back Office de ENDESA. Para esta carga masiva, ******EMPRESA.1*** disponía sólo del usuario de acceso a ******HERRAMIENTA.4*** y al acceso vía ftp.

En relación con lo expuesto anteriormente cabe destacar que los subagentes (usuarios de ******EMPRESA.9***) solo podían acceder al CRM de ******EMPRESA.1***, sin que en ningún caso tuvieran acceso directo al CRM de Endesa.

43. En relación con los usuarios de ******EMPRESA.9*** con acceso al CRM de ******EMPRESA.1*** cabe destacar que en el CRM de ******EMPRESA.1*** existen diferentes perfiles de usuarios (se adjunta Doc. 4, imagen 1 para acreditar la relación de perfiles de usuarios), siendo el responsable de la aplicación, en cualquier caso, ******EMPRESA.1***.

44. Por su parte, ******EMPRESA.1*** solo tenía un usuario de acceso a las siguientes herramientas de ENDESA:

- ******HERRAMIENTA.4*** y al acceso vía FTP autorizado por ENDESA para realizar la carga masiva de las solicitudes de contratación. (Se adjunta Doc. 4, imagen 4 y 5 para acreditar el proceso de alta a la aplicación). Con el perfil de usuario autorizado por parte de ENDESA, solo era posible cargar las ventas desde el CRM de ******EMPRESA.1*** a ******HERRAMIENTA.4*** y visualizar los feedback de ENDESA sobre el estado de las ventas cargadas. (…)
- ******PLATAFORMA.1***: Es la plataforma para la descarga de ficheros "no molestar" de ENDESA. ******EMPRESA.1***, a través de esta plataforma, descargaba los ficheros que ENDESA ponía a su disposición semanalmente y que contenían los números de teléfonos de clientes que habían ejercido su derecho de oposición a recibir llamadas comerciales por parte de ENDESA. Una vez obtenido este fichero, se cruzaba con las bases de datos utilizadas para la realización de llamadas comerciales. Existía un único usuario con acceso a esta aplicación y se accedía a través de la web. ******EMPRESA.1*** solo tenía permisos en esta aplicación para realizar la descarga del fichero.

No existe ninguna otra aplicación a la que tuvieran acceso ******EMPRESA.1*** y/o sus colaboradores en el marco de la relación contractual con ENDESA para la captación telefónica de clientes.

45. Cada usuario de ******EMPRESA.9*** podía cargar en el CRM de ******EMPRESA.1*** exclusivamente las operaciones que ellos mismos habían realizado, pudiendo visualizar únicamente los estados de dichas operaciones hasta el cierre completo de la venta por parte de ENDESA. Solo tenían acceso a los datos personales que ellos mismos introducían en el CRM de ******EMPRESA.1*** y que eran, en todo caso, datos identificativos y de contacto (nombre, apellidos, nº de DNI, nº de teléfono, e-mail, dirección de punto de suministro, voz, nº CUPS, dirección de facturación), datos económicos (nº de cuenta bancaria) y de características personales (la fecha de nacimiento). Se aporta una tabla en la que se diferencia entre clientes con quien se finalizó el proceso completo de contratación y clientes con los que por diferentes cuestiones no se llegó a formalizar la contratación. En cualquier caso, no todos los clientes a quienes tenían acceso estos usuarios se vieron afectados por la práctica fraudulenta de ******EMPRESA.9***, ya que solo 137 operaciones fueron las afectadas cuya contratación fraudulenta se culminó.

Por su parte, ******EMPRESA.1*** podía acceder con su usuario a ******HERRAMIENTA.4*** para visualizar el estado de cualquier contratación de cualquiera de sus Subagentes, pudiendo acceder a la misma tipología- de datos personales que los descritos en el punto anterior.

46. En el CRM de ******EMPRESA.1*** se registraban:

- los logs de acceso de usuarios al CRM de ******EMPRESA.1*** (fecha, hora, dirección ip y el resultado)
- los logs de registro de accesos a las URL del servidor (fecha, hora, dirección ip y el resultado)
- Trazabilidad en base de datos (fecha, hora y usuario) de creación de una operación por parte de un usuario y de una modificación del estado de la

operación (por ejemplo, si hay alguna incidencia en la contratación, falta documentación o la contratación ha sido denegada por ENDESA).

Además, se permitía realizar una limitación de acceso al CRM por IP para que los usuarios solo pudieran acceder desde una IP conocida por un perfil de usuario de rango superior. Cabe destacar que las prácticas fraudulentas llevadas a cabo por los usuarios de ******EMPRESA.9*** se debieron a acciones intencionadas realizadas por los propios usuarios, es decir, las contrataciones no se realizaron por el acceso no autorizado por parte de terceros al CRM de ******EMPRESA.1***, sino a través de acciones premeditadas por parte de los usuarios autorizados. Por este motivo, en el análisis de logs realizado se observa un funcionamiento "normal" de la actividad de los usuarios sin que sea posible apreciar irregularidades en cuanto a la utilización de los usuarios.

47. Tras la auditoría realizada internamente por parte de ******EMPRESA.1*** cuando se tuvo conocimiento de la práctica fraudulenta llevada a cabo por ******EMPRESA.9***, se determinó que había un total de 137 contrataciones que, posiblemente, estuvieran afectadas. Esto se dedujo porque, en estas operaciones, el número de teléfono utilizado para el envío del SMS de solicitud de consentimiento del cliente para cerrar la venta coincidía con el de al menos otra operación.

48. Se adjunta como Documento 5 la copia del contrato suscrito con ******EMPRESA.9*** que se encontraba vigente en el período en que tuvo lugar la brecha de seguridad, así como la rescisión de éste con fecha efectiva 19 de octubre de 2021, día en que se tuvo conocimiento de la práctica fraudulenta llevaba a cabo por ******EMPRESA.9***. En el documento de rescisión del contrato se puede apreciar una errata en la fecha del contrato objeto de la rescisión, ya que se hace referencia a la fecha en que se formalizo el primer contrato con ******EMPRESA.9*** para la distribución de servicios de ENDESA y que ya no se encontraba vigente en la fecha en que tuvo lugar la brecha de seguridad. En cualquier caso, dado que es la única campaña comercial que ******EMPRESA.9*** gestionaba por cuenta de ******EMPRESA.1*** en favor de ENDESA, con la citada comunicación de rescisión se entendió resuelta la relación comercial entre las partes y se procedió, entre otras cosas, a retirarles el acceso a sus usuarios para la carga de ventas en el Crm de ******EMPRESA.1***.

Según consta en la diligencia realizada el día 13 de octubre de 2022, ENDESA es una sociedad anónima de nacionalidad española. Según los datos obrantes en AXESOR la empresa tiene tamaño "Grande" con XXX empleados y en el año 2021 (último ejercicio presentado) tuvo un volumen de ventas de ***CANTIDAD.1 euros y un resultado de ejercicio de ***CANTIDAD.3 euros.

SEXTO: Con fecha 27 de enero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ENDESA con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, en el que se le indicaba que tenía un plazo de diez días para presentar alegaciones, a fin de imponerle:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 2.500.000,00 euros.

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 1.500.000,00 euros.

- Por la supuesta infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 800.000,00 euros.

- Por la supuesta infracción del artículo 34 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 800.000,00 euros.

- Por la supuesta infracción del artículo 44 del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 2.000.000,00 euros.

Este acuerdo de inicio, que se notificó a ENDESA conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en fecha 30 de enero de 2023.

SÉPTIMO: Con fecha 30 y 31 de enero y 1, 2 y 3 de febrero de 2023, ENDESA presentó un escrito a través del cual solicitaba la ampliación del plazo para aducir alegaciones y que se le facilitara copia del expediente.

Con fecha 3 de febrero de 2023, el órgano instructor del procedimiento acordó la ampliación de plazo instada hasta un máximo de cinco días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP y que se le remitiera a ENDESA copia del expediente.

El citado acuerdo se notifica a ENDESA, en fecha 6 de febrero de 2023, como consta en el acuse de recibo que obra en el expediente.

OCTAVO: Con fecha 20 de febrero de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de ENDESA en el que aduce alegaciones al acuerdo de inicio.

En estas alegaciones, en síntesis, manifestaba que:

- Alegación previa: Concreción de determinados puntos fácticos esenciales para el análisis jurídico del expediente, toda vez que existen, a su entender, en el Acuerdo de Inicio, algunas cuestiones que, siendo muy relevantes para el enjuiciamiento de la conducta de ENDESA, no han sido interpretadas por la AEPD, a su juicio, de manera correcta.
- ENDESA tenía implementadas medidas de seguridad adecuadas al riesgo:
  - Se aporta Documento número 1 con la explicación detallada de cada uno de los desarrollos en la plataforma ******HERRAMIENTA.1***, así como de su valoración horaria.
  - Se aporta Documento número 2 con la explicación detallada de cada uno de los desarrollos y tareas necesarias para la implementación de la medida de seguridad en ******HERRAMIENTA.2.***
- Existe concurrencia de infracciones del artículo 5.1.f) del RGPD y artículo 32 del RGPD.
- Se ha vulnerado el principio de tipicidad del artículo 5.1.f) del RGPD.
- No procede la sanción por la infracción del artículo 33 del RGPD:
  - Se aporta Documento número 3 en el que ENDESA sigue solicitando a ******EMPRESA.1*** información adicional sobre la Violación de la Seguridad de los Datos para, continuamente, reevaluar su conclusión de que la

Violación no es notificable, sin que ***EMPRESA.1 ni ***EMPRESA.9 aporten información relevante, a su juicio.

- Se aporta Documento número 4 en el que ENDESA vuelve a requerir a ***EMPRESA.1 para que aporte más información sobre la Violación de la Seguridad de los Datos y ***EMPRESA.1, una vez más, facilita información incompleta, a su juicio.
- Se aporta Documento número 5 con el protocolo de gestión de brechas de seguridad elaborado por ENDESA.

- No procede la sanción por la infracción del artículo 34 del RGPD.
- No procede la sanción por la infracción del artículo 44 del RGPD:
  - Se aporta Documento número 6 con las Cláusulas Contractuales Tipo suscritas con sus proveedores ubicados fuera del Espacio Económico Europeo, en cumplimiento de su procedimiento interno para la realización de transferencias internacionales.
  - Se aporta Documento número 7, 8 y 9 con las Cláusulas Contractuales Tipo suscritas con los proveedores ***EMPRESA.15, ***EMPRESA.12, y ***EMPRESA.9, respectivamente.
- Existe falta de proporcionalidad sobre la graduación de la sanción a imponer a ENDESA.

NOVENO: Con fecha 13 de junio de 2023, el órgano instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporados la notificación de la violación de la seguridad de los datos personales a que dio lugar el presente procedimiento y su documentación, los documentos obtenidos y generados durante la fase de actuaciones previas de investigación y el informe correspondiente, que forman parte del procedimiento AI/00178/2022, así como las alegaciones al acuerdo de inicio presentadas por ENDESA y la documentación que a ellas acompaña.

En ese mismo escrito esta Agencia ha requerido a ENDESA para que en el plazo de cinco días hábiles presentara la siguiente información: el informe pericial de un tercero independiente a que hace referencia la citada empresa en la página 7 de su escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, a fin de demostrar que "*a pesar de que algunos anuncios de Facebook se hubieran mantenido activos (…), las credenciales que se ofertaban a través de ese medio ya no permitían, de modo alguno, acceder a los sistemas* ***HERRAMIENTA.1 *y* ***HERRAMIENTA.2 *porque estaba deshabilitadas*" y que "*como consecuencia de las nuevas medidas de seguridad implementadas por Endesa, ningún usuario adicional no autorizado conseguiría la finalidad de vender/alquilar credenciales de acceso a los sistemas de Endesa, puesto que dichas medidas se lo impedirían*".

Con fecha 14, 16 y 19 de junio de 2023, ENDESA presentó un escrito a través del cual solicitaba la ampliación del plazo para presentar el citado informe.

Con fecha 19 de junio de 2023, el órgano instructor del procedimiento acordó la ampliación de plazo instada hasta un máximo de dos días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP.

El citado acuerdo se notifica a ENDESA en fecha 20 de junio de 2023, como consta en el acuse de recibo que obra en el expediente.

Con fecha 23 de junio de 2023, ENDESA presentó escrito de respuesta ante esta Agencia, en el que aporta como Documento número 1 el informe solicitado.

DÉCIMO: Con fecha 23 de junio de 2023, el órgano instructor del procedimiento envió un requerimiento a ENDESA para que en el plazo de cinco días hábiles presentara la siguiente información:

> -Indicación de si ha firmado nuevas cláusulas contractuales tipo para las trasferencias internacionales de datos realizadas a ******EMPRESA.9***, adaptadas a la decisión de ejecución 2021/914 de la Comisión, 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE), y, en su caso, aporte copia firmada de las mismas.
>
> - Acreditación de la evaluación sobre el derecho y las prácticas de ***PAÍS.1 y ***PAÍS.2 aplicables al tratamiento de los datos personales realizados por las entidades ******EMPRESA.15***, ******EMPRESA.12*** y ******EMPRESA.9,*** a la que se refiere la letra b) de la cláusula 14 de la citada Decisión de Ejecución, de 4 de junio de 2021.

El citado requerimiento se notifica a ENDESA en fecha 26 de junio de 2023, como consta en el acuse de recibo que obra en el expediente.

Con fecha 3 de julio de 2023, ENDESA presentó escrito de respuesta ante esta Agencia, en el que aporta:

- Documento número 1: copia del burofax remitido por ******EMPRESA.1*** a ******EMPRESA.9*** comunicándole el cierre definitivo de la campaña de venta que ******EMPRESA.9*** realizaba para Endesa.
- Documento número 2: justificante de Correos que acredita el envío del citado burofax a ******EMPRESA.9***.
- Documento número 3: aviso del sistema interno de proveedores de Endesa acreditando que, con fecha 2 de noviembre de 2021 se desasoció al subcontratista ******EMPRESA.9***.
- Documento número 4 y número 5: evaluaciones de impacto de las trasferencias internacionales respecto de los datos transferidos a ***PAÍS.1 y ***PAÍS.2, casos en los que ******EMPRESA.15*** y ******EMPRESA.12*** actuaban como importadores de los datos, todo ello por cuanto la relación contractual ente Endesa y ******EMPRESA.15*** sigue estando vigente en la actualidad y, en el caso de ******EMPRESA.12***, se mantuvo hasta el mes de noviembre del año 2022.
- Documento número 6: evaluación de impacto sobre el derecho y las prácticas de ***PAÍS.2 aplicables al tratamiento de los datos personales realizados por el propio proveedor ******EMPRESA.15***.
- Documento número 7: acuerdo de resolución del contrato suscrito entre Endesa y ******EMPRESA.16***, el cual implica la finalización de la subcontratación con ******EMPRESA.12.***

DÉCIMO PRIMERO: Con fecha 23 de agosto de 2023**,** el órgano instructor del procedimiento dictó propuesta de resolución en la que propone imponer a ENDESA:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 2.500.000,00 euros.

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 1.500.000,00 euros.

- Por la supuesta infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 800.000,00 euros.

- Por la supuesta infracción del artículo 34 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 800.000,00 euros.

- Por la supuesta infracción del artículo 44 del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 2.000.000,00 euros.

Esta propuesta de resolución, que se notificó a ENDESA conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 24 de agosto de 2023, como consta en el acuse de recibo que obra en el expediente.

DÉCIMO SEGUNDO: Con fecha 24 de agosto de 2023, ENDESA presenta un escrito a través del cual solicita la ampliación del plazo para aducir alegaciones y que se le facilite copia del expediente.

DÉCIMO TERCERO: Con fecha 28 de agosto de 2023, el órgano instructor del procedimiento acuerda la ampliación de plazo instada hasta un máximo de cinco días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP y que se le remita a ENDESA copia del expediente.

El citado acuerdo se notifica a ENDESA en fecha 30 de agosto de 2023, como consta en el acuse de recibo que obra en el expediente.

DÉCIMO CUARTO: Con fecha 14 de septiembre de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de ENDESA en el que aduce alegaciones a la propuesta de resolución. En estas alegaciones, en síntesis, manifestaba que:

- Alegación previa: Concreción de determinados puntos fácticos esenciales para el análisis jurídico del expediente, toda vez que existen, a su entender, en el Acuerdo de Inicio, algunas cuestiones que, siendo muy relevantes para el enjuiciamiento de la conducta de ENDESA, no han sido interpretadas por la AEPD, a su juicio, de manera correcta.
- No procede la sanción por la infracción del artículo 32 del RGPD:
    - Se aporta Documento número 1 el correo electrónico de 29 de noviembre de 2021 por el cual ENDESA solicita el reseteo de los usuarios comunicados por ******EMPRESA.1*** como fraudulentos y la confirmación de que ese mismo día se habían reseteado con éxito.
- Existe concurrencia de infracciones del artículo 5.1.f) del RGPD y artículo 32 del RGPD.
- Se ha vulnerado el principio de tipicidad del artículo 5.1.f) del RGPD.

- No procede la sanción por la infracción del artículo 33 del RGPD.
- No procede la sanción por la infracción del artículo 34 del RGPD:
  - Se aporta Documento número 2 con una declaración de ***DEPARTAMENTO.7 en la que se detallan las actuaciones llevadas a cabo por Endesa para atender de manera personalizada a los interesados que se hubieran podido ver afectados por el incidente, así como unos ejemplos de dichas tareas.
- No procede la sanción por la infracción del artículo 44 del RGPD.
- Existe falta de proporcionalidad sobre la graduación de la sanción a imponer a ENDESA.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes:

HECHOS PROBADOS

PRIMERO: Con fecha 1 de diciembre de 2015, según consta en el Documento número 7 que acompaña el escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, la Directora de la Agencia Española de Protección de Datos dictó resolución en la que se autoriza la transferencia internacional de datos personales solicitada por ENDESA a ***EMPRESA.15**, ubicada en ***PAÍS.2.

SEGUNDO: El 1 de junio de 2020 ENDESA y ***EMPRESA.1** suscribieron un contrato para comercializar los productos y servicios de ENDESA a través de diferentes acciones comerciales, según se indica en el Documento 1 del escrito de ***EMPRESA.1** de 25 de noviembre de 2022.

TERCERO: El 22 de julio de 2020, según consta en el Documento 9 que acompaña al escrito de alegaciones de ENDESA al acuerdo de inicio del presente procedimiento sancionador, ENDESA como exportador de datos y ***EMPRESA.9** (con domicilio en ***PAÍS.1) en calidad de importador de datos suscribieron un contrato de prestación de servicios, a los efectos de dar cumplimiento al artículo 46.2.c) del Reglamento (UE) 2016/679, de 27 de abril, de Protección de Datos ("RGPD") y, de conformidad con lo dispuesto en la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2020, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países.

CUARTO: El 3 de marzo de 2021, según consta en el Documento 5 que acompaña al escrito de ***EMPRESA.1** de 25 de noviembre de 2022, ***EMPRESA.1** y ***EMPRESA.9** firmaron un contrato para la "*actividad de intermediación en altas de clientes para ENDESA mediante la realización de llamadas telefónicas de captación comercial utilizando bases de datos de Endesa*".

QUINTO: El 14 de marzo de 2021 el usuario "***D.D.D.**" publica un anuncio en Facebook, según consta en el Documento número 2 del escrito de ENDESA de 11 de noviembre de 2022: "*Se alquila sistema para obtener cups de energía y gas solo con la dirección del cliente. Info al inbox*!!"

SEXTO: El 28 de abril de 2021 firmaron un contrato ***(…)*** y ******EMPRESA.1***, de servicios de venta telefónica, según consta en el Documento número 4 que acompaña el escrito de ENDESA de 7 de octubre de 2022.

SÉPTIMO: El 5 de mayo de 2021, según consta en el Documento 8 que acompaña al escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, ENDESA y ******EMPRESA.12*** firmaron un contrato, a los efectos de dar cumplimiento al artículo 46.2.c) del Reglamento (UE) 2016/679, de 27 de abril, de Protección de Datos ("RGPD"), de conformidad con la Decisión de 2010/87 UE de la Comisión, de 5 de febrero de 2020, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países..

OCTAVO: El 28 de julio de 2021 ENDESA autorizó a ******EMPRESA.1*** la subcontratación de ******EMPRESA.9*** para la prestación de los servicios de venta telefónica, según consta en el Documento número 6 que acompaña el escrito de ENDESA de 7 de octubre de 2022, en el que se fija como "*fecha de inicio de los trabajos subcontratados 1 agosto 2021*" y como "*fecha de fin 1 Agosto 2022*".

NOVENO: El 24 de agosto de 2021, la persona responsable del ***DEPARTAMENTO.1 de ENDESA envió un correo electrónico al responsable de Seguridad de la Información del Grupo Endesa, en el que se informa de un anuncio sospechoso en Facebook.

Según consta en el Documento número 6 que acompaña el escrito de ENDESA presentado el 26 de julio de 2022, el contenido del correo electrónico era el siguiente:

"(…)"

Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, con este aviso se activó el proceso de análisis e investigación, cuyo primer paso es confirmar la veracidad del anuncio.

DÉCIMO: El 1 de septiembre de 2021, según consta en el Documento número 4 que acompaña al escrito de ENDESA de 11 de noviembre de 2022, ENDESA recibe un correo electrónico procedente de ******EMPRESA.16***, con el siguiente contenido:

"(…) La persona que si conocemos es ***D.D.D.****, pues hemos reconocido su foto de perfil. (…) Su nombre completo es* ***D.D.D.****. (…)"*

DÉCIMO PRIMERO: El 3 de septiembre de 2021, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó en la plataforma ******HERRAMIENTA.1*** el usuario "******USUARIO.3***" asignado a ******EMPRESA.12.***

DÉCIMO SEGUNDO: El 10 de septiembre de 2021, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, ENDESA envió un correo electrónico con el siguiente contenido:

"(…) Dado que hablamos de un empleado actualmente activo en ******EMPRESA.15****, agradeceré actuéis con la máxima rapidez y procedáis a desvincularlo de nuestras operaciones.*

Entiendo que, entre otras, adoptaréis medidas legales contra dicho empleado. Agradeceré me mantengas puntualmente informado de las medidas que adoptéis contra él.

Asimismo, entiendo que ******EMPRESA.15*** *deberá instaurar las medidas de ciberseguridad y rastreo necesarias que permitan localizar, como lo ha hecho ENDESA, posibles comercializaciones de usuarios asignados a vosotros y, por tanto, de vuestra entera responsabilidad.*

Por nuestra parte, procedemos a dar de baja el usuario con carácter inmediato. (…)"

DÉCIMO TERCERO: El 10 de septiembre de 2021, según consta en los Documentos 8, 9 y 10 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó en la plataforma ******HERRAMIENTA.1*** el usuario ******USUARIO.8***, asignado a ******EMPRESA.15***. Y se procedió a su retirada y eliminación de los sistemas de ******HERRAMIENTA.2***.

DÉCIMO CUARTO: El 13 de septiembre de 2021, según consta en el Documento número 10 que acompaña el escrito de ENDESA de 26 de julio de 2022, se realiza la primera valoración de la violación de la seguridad de los datos personales, donde se recoge la información obtenida hasta ese momento en un documento firmado el 14 de septiembre de 2021.

El contenido del documento es el siguiente:

"*El día 24 de agosto se detectó en Facebook un anuncio donde se vendía usuario de* ******PLATAFORMA.1*** *con acceso a información de clientes para campaña de energía en España, la imagen de abajo contiene el anuncio.*
(…)
Una vez detectado el anuncio se inicia el estudio del incidente, obteniendo el 10 de septiembre la comprobación de la veracidad del mismo y la identificación de las credenciales usados de forma fraudulenta para el acceso a la aplicación de Endesa ******PLATAFORMA.1.****.*

Durante la investigación del incidente se ha detectado el compromiso de las credenciales de un usuario del aplicativo que estaban siendo usados por el anunciante de Facebook para vender accesos. Se ha comprobado la validez de estos, pero no se ha podido confirmar que se haya materializado la venta de las credenciales y en caso de haberse realizado se desconoce el número de registros del aplicativo que han podido ser accedidos. Basándonos en la información recogida hasta ahora, que incluye el tiempo transcurrido desde la publicación del anuncio, el tipo de servicio ofertado y las limitaciones en las consultas ofrecidas por el aplicativo, se estima que el número de registros afectado podría estar en una horquilla de accesos de entre 100 y 1.000 registros afectados.

En el momento de realizar esta valoración no se han detectado reclamaciones de clientes que se puedan asociar a este incidente.

Con fecha 13 de septiembre se convoca Comité de Brechas de Seguridad para analizar el incidente.

Valoración del alcance

(…)

II. TOMA DE DECISIÓN

- **VOLUMEN** (números de registros completos e identificativos)

  - Menos de 100 registros (1)
  - Entre 100 y 1.000 (2) X
  - Entre 1.000 y 100.000 (3)
  - Más de 100.000 (4)
  - Más de 1.000.000 (5)

- **TIPOLOGÍA DE DATOS (Según GDPR y Sector)**

  - Datos no sensibles (x1) X
  - Datos sensibles (x2)

- **IMPACTO (EXPOSICIÓN)**

  - Nulo (2)
  - Interno (dentro de la empresa - controlado) - (4)
  - Externo (Perímetro proveedor, atacante) - (6) X
  - Pública (Accesible en Internet) - (8)
  - Desconocido (10)

-ANÁLISIS DEL INCIDENTE

Volumen	Desconocido, se considera un número muy bajo nunca superior a 1.000	2
Tipología de datos	Datos no sensibles	1
Impacto	Medio	6
Riesgo	3 x (1 x 6)	12

III. CONCLUSIÓN

En reunión mantenida ***(…),*** tras realizar una valoración, en tiempo y forma, del alcance del incidente de seguridad y de las posibles repercusiones para los derechos y libertades de los interesados afectados, se adopta la decisión preliminar de no comunicar el incidente de seguridad a la autoridad de control por no alcanzar el umbral previsto en la guía de la agencia sobre brechas de seguridad. No obstante, desde ***DEPARTAMENTO.4 se señala la necesidad de continuar con la investigación al

objeto de poder realizar una nueva valoración del incidente, por considerar que la información aportada no es completa y el presente análisis tiene carácter preliminar.

Considerando los planteamientos anteriores, se enumera el plan de acción ejecutado y previsto para garantizar las medidas de seguridad a establecer:

- ***(…)***

DÉCIMO QUINTO: El 21 de septiembre de 2021, según consta en el Documento número 3 que acompaña al escrito de ENDESA de 11 de noviembre de 2022, ENDESA recibe un correo electrónico con el siguiente contenido:

*"(…) confirmarte que la persona que nos indicas (**C.C.C.**) fue empleado de *****EMPRESA.15** pero es baja de la compañía desde 2016. Hemos intentado identificar algún tipo de vínculo entre esta persona y el agente del usuario que se utiliza, hasta el momento, no se ha encontrado nada. Hemos rastreado RRSS de ambos y sin ningún vínculo aparente."*

DÉCIMO SEXTO: El 21 de septiembre de 2021, según consta en el Documento 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó el usuario ******USUARIO.5***, de la plataforma ******HERRAMIENTA.1***, asignado a ******EMPRESA.12***.

DÉCIMO SÉPTIMO: El 28 de septiembre de 2021, según consta en el Documento número 11 que acompaña el escrito de ENDESA de 26 de julio de 2022, se realiza una segunda valoración donde se completa la información de la primera, si bien su contenido es prácticamente idéntico, se añade como medida propuesta la "Desvinculación de la empresa y estudio de actuaciones legales contra el empleado cuyas credenciales han sido comprometidos." (sic) Se considera en el informe que el impacto del presente incidente era "Medio" y que no era necesario notificar el incidente a la AEPD.

DÉCIMO OCTAVO: El 18 de octubre de 2021, como consta en el Documento número 8 que acompaña al escrito de ENDESA de 7 de octubre de 2022, se recibe un correo electrónico desde Facebook con el asunto "Formulario de reporte de derechos de autor ***#(…)***", en el que se comunica que Facebook eliminó o inhabilitó el acceso a tres enlaces que habían sido reportados, por infringir su Declaración de derechos y responsabilidades. También se indica que dos enlaces ya fueron eliminados de Facebook. Por último, respecto de otros seis enlaces se dice "*Tenga en cuenta que este canal es solo para denunciar infracciones de propiedad intelectual, como derechos de autor o de marca comercial. A partir de la información que proporcionó, parece que necesita ayuda con otro asunto. Los siguientes enlaces de ayuda pueden resultarle útiles: (…*)".

DÉCIMO NOVENO: El 19 de octubre de 2021, según ha manifestado ******EMPRESA.1*** en su escrito de 25 de noviembre de 2022, detecta que un usuario del agente ******EMPRESA.9*** ha intentado realizar un alta fraudulenta ya que, entre otras cuestiones, se puede apreciar que el número de teléfono utilizado para enviar al cliente el SMS de confirmación de venta (el cliente debe responder a este SMS para confirmar la venta) es coincidente con otro número de teléfono utilizado con la misma finalidad para otro cliente, por lo que es posible que el cliente no hubiera aceptado el

contrato, habiéndose aceptado el mismo mediante confirmación de SMS por una persona diferente al titular de la contratación.

VIGÉSIMO: El 19 de octubre de 2021, según consta en el Documento 2 del escrito de ***EMPRESA.1** de 26 de noviembre de 2022, ***EMPRESA.1** envía un correo electrónico a ENDESA, con el siguiente contenido:

"(…)"

VIGÉSIMO PRIMERO: El 19 de octubre de 2021, según consta en el Documento 2 del escrito de ***EMPRESA.1** de 25 de noviembre de 2022, ***EMPRESA.1** envió una comunicación a todos los Subagentes participantes en la campaña de ENDESA, con el siguiente contenido:

"Hemos detectado una serie de operaciones de distintos titulares en las que el número de contacto (móvil donde se envía el SMS) son coincidentes. Esto quiere decir que no es el cliente el que ha firmado las condiciones particulares del contrato. Este tipo de acciones (suplantación de identidad) derivan a responsabilidad penal y lógicamente al cierre de la campaña.

Para evitar este tipo de situaciones confirmad de forma obligatoria antes de enviar el SMS que el número móvil es el del titular del contrato antes de realizar la grabación de la venta. Se están realizando auditorías al respecto y quien esté realizando este tipo de acciones tendrá cierre de código automático. (…)"

VIGÉSIMO SEGUNDO: El 20 de octubre de 2021, según consta en el Documento 2 del escrito de ***EMPRESA.1** de 25 de noviembre de 2022, ***EMPRESA.1** envió un correo electrónico a ENDESA con el siguiente contenido:

*"(…) Tras análisis interno sobre exportación de archivo de **HERRAMIENTA.4**, tras poner los siguientes filtros:*

*Ventas en trámite o en vigor, correspondientes a los contratos que están en estos estados con último cambio de estado en **HERRAMIENTA.4** correspondientes a los meses de Julio, Agosto, Septiembre y Octubre filtramos 144 clientes que tienen el teléfono de consentimiento de contrato duplicado.*

De estas órdenes hay 7 (detallo los clientes) en trámite o pendiente BO (las marco en rojo). Las restantes 137 (marcadas en negro) son de clientes activos con número de consentimiento de contrato duplicado. (…)"

VIGÉSIMO TERCERO: El 20 de octubre de 2021 se envía un correo electrónico desde ***EMPRESA.9** a ***EMPRESA.1** con el siguiente contenido, el cual fue reenviado a ENDESA, según consta en el Documento número 12 del escrito que presentó ENDESA el 7 de octubre de 2022 y en el Documento 2 del escrito de ***EMPRESA.1** de 26 de noviembre de 2022:

"Hoy procedimos con el despido y la denuncia correspondiente por fraude informático, ley tipificada (...) en contra de los comerciales implicados en la venta fraudulenta. Esta última acción la realizamos con el fin de que independientemente de la

responsabilidad que claramente cómo empresa asumimos, queremos dejar claro que no es una práctica avalada por nosotros, repudiamos totalmente y definitivamente no define nuestra forma de trabajo.

Por ese motivo adicionalmente iniciamos una auditoría interna, donde encontramos otros clientes y comerciales con prácticas similares, con los que procedimos de la misma manera y ponemos a su disposición todos los datos encontrados hasta el momento, e iremos en posteriores correos ampliando información."

Y se aporta el listado de todos los comerciales denunciados y de los móviles duplicados en ventas.

VIGÉSIMO CUARTO: El 20 de octubre de 2021, según consta en el Documento 2 que acompaña al escrito de ******EMPRESA.1*** de 25 de noviembre de 2022, ******EMPRESA.1*** envió un correo electrónico a ENDESA con el siguiente contenido:

"Paso a detallaros los puntos que ya estamos trabajando para poder detectar la cualquier posible incidencia adicional a la ya detectada.

- *Verificar con llamada telefónica (aportado grabaciones de llamadas y listado en Excel) los siguientes puntos:*
- *Confirmación con el cliente que si están interesados en la contratación, los que no estén interesados indicarlo para solicitar la cancelación del cambio de comercializadora a Endesa*
- *Confirmar con todos los clientes que la cuenta de pago es correcta, los que no sea aportada por el cliente indicarlo para cancelar el cambio de compañía o si están activos modificar la cuenta de pago.*

En un primer punto se van a gestionar las ventas que entendemos pueden estar afectadas por esta casuística y posteriormente se va a llamar a todos los clientes tramitados desde Septiembre (fecha en la que hemos detectado tras revisión el comienzo de esta práctica) para en caso de que haya alguno más afectado solucionar la situación del contrato.

*En otro orden estamos cancelando en ***HERRAMIENTA.4 las 172 órdenes que están en pendiente BO de* ******EMPRESA.9*** *para que avancen. (…)"*

VIGÉSIMO QUINTO: El 25 de octubre de 2021, según manifestó ******EMPRESA.1*** en su escrito de 25 de noviembre de 2022, para evitar que se refugiasen en otras subcontratas los trabajadores de ******EMPRESA.9***, ******EMPRESA.1***, procedió a cerrar los sistemas y a comunicar de forma fehaciente al resto de agentes de la zona el cierre de la campaña.

VIGÉSIMO SEXTO: El 27 de octubre de 2021, según consta en el Documento 2 del escrito de ******EMPRESA.1*** de 25 de noviembre de 2022, ******EMPRESA.1*** recibió un correo electrónico de ******EMPRESA.9***, con el siguiente contenido:

"(…) Con el fin de poder identificar todos los clientes afectados, se han tomado medidas que ya se han comentado antes por teléfono; lo cual ha sido denunciados por la acción realizada.

En base a esto varios comerciales han decidido colaborar dando detalle indicándonos a detalle qué es lo que estaban realizando.

1. Se contactaron con el cliente y explicaban el producto, de estar de acuerdo y ser consciente con la contratación procedían con el cierre, sin embargo el cliente ponía la objeción indicando que no podían responder el sms por diferentes motivos (bloqueado para sms, no tenía móvil, no tenía batería, próximo a viajar, etc.) Lo que hacía el comercial era conseguir número de otro cliente que era de Endesa y pedían a este último que respondan el sms.

2. Por medio de internet los asesores han contratado el ******PLATAFORMA.1****. Lo que han hecho los comerciales es utilizar esta herramienta para poder extraer datos, por lo que las grabaciones lo hacían con otras personas. Adjunto los usuarios de* ******PLATAFORMA.1*** *que han usado. Cabe mencionar que nosotros en su momento pedimos esta herramienta por lo que nos negaste indicando que estaba prohibido.*

Adjunto usuarios que han utilizado:

******USUARIO.3***

******USUARIO.10***

******USUARIO.5***

******USUARIO.6***

******USUARIO.7***

3. Otro caso ha sido clientes que por algún momento no han querido pasar textos por ser muy largos, se cansaron de recibir varias llamadas. Lo que han hecho es una simulación de ventas con otras personas y el mensaje también ha sido respondido por otros. (…)"

A este correo electrónico se adjuntan cuatro imágenes:

- Imagen de un anuncio de Facebook, de 17 de octubre, del usuario "***E.E.E.***", con el siguiente contenido:
"Se crean usuarios para campaña energía
Sistema de ******PLATAFORMA.1***
Para campaña energía"

- Imagen de un anuncio de Facebook, de 13 de octubre, del usuario "***F.F.F.***", con el siguiente contenido:
"******PLATAFORMA.1*** alquiler x 30 días"

- Imagen de un anuncio de Facebook, de 13 de octubre, del usuario "***F.F.F.***", con el siguiente contenido:
"Contamos con usuario ******PLATAFORMA.1*** en modo de alquiler al mes"

- Imagen de un anuncio de Facebook, del usuario "***C.C.C.***", con el siguiente contenido:
"[varios emojis de cara de sorpresa]
Si recién empiezas en el mundo de ventas para Energía España
Tenemos un sistema que te ayudará en incrementar tus habilitadas y venta!!!!!
*Se crea usuario de #****PLATAFORMA.1** para campaña de energía España!!!!... Ver más"*

VIGÉSIMO SÉPTIMO: El 27 de octubre de 2021, según ha manifestado ENDESA en su escrito de 7 de octubre de 2022, un proveedor de ENDESA le alertó sobre el uso irregular que, algunos de sus asesores, habían realizado con ciertas credenciales de acceso a ***HERRAMIENTA.1** que habían adquirido de manera irregular. En esta comunicación se identifican cinco usuarios de ***HERRAMIENTA.1** comprometidos que fueron identificados por la empresa subcontratista del proveedor de ENDESA.

En el documento número 3 que acompaña al citado escrito, se observa un correo electrónico recibido por ENDESA el 27 de octubre de 2021 en el que se indica:

*"Por medio de Internet los asesores han contratado el ***PLATAFORMA.1**. Lo que han hecho los comerciales es utilizar esta herramienta para poder extraer datos, por lo que las grabaciones lo hacían con otras personas. (…)*

Adjunto usuarios que han utilizado:

***USUARIO.3**

***USUARIO.10**

***USUARIO.5**

***USUARIO.6**

***USUARIO.7**

VIGÉSIMO OCTAVO: El 27 de octubre de 2021, según consta en el Documento 1 y 2 del escrito presentado por ENDESA el 3 de julio de 2023 en respuesta a requerimiento de esta Agencia, ***EMPRESA.1** envió una carta certificada a ***EMPRESA.9**, con el siguiente contenido:

"(…)
*En fecha 19 de Octubre de los corrientes, el ***PUESTO.1, **G.G.G.**, le remite un correo electrónico en el que le advierte que se estaban detectado en varios clientes, suplantaciones de identidad, puesto que los teléfonos y grabaciones no coincidían con el cliente contratado y que se suspendía cautelarmente, la campaña de venta para iniciar una auditoría y esclarecer los hechos, junto con Endesa Energía.*

En este momento y todavía sin haber podido determinar el número exacto de ventas fraudulentas por lo laborioso que está resultando, le comunico, en la representación que ostento, el cierre definitivo con efectos 19 de Octubre, de la campaña de venta

para de contratos de suministro de Endesa Energía y todo ello, de acuerdo con el clausulado del contrato suscrito entre las partes. (…)"

VIGÉSIMO NOVENO: El 28 de octubre de 2021, según consta en el Documento 5 del escrito de ******EMPRESA.1*** de 25 de noviembre de 2022, ******EMPRESA.1*** envió una comunicación certificada electrónica a ******EMPRESA.9***, con el siguiente contenido:

"(…)
*En fecha 19 de Octubre de los corrientes, el ***PUESTO.1,* ***G.G.G.****, le remite un correo electrónico en el que le advierte que se estaban detectado en varios clientes, suplantaciones de identidad, puesto que los teléfonos y grabaciones no coincidían con el cliente contratado y que se suspendía cautelarmente, la campaña de venta para iniciar una auditoría y esclarecer los hechos, junto con Endesa Energía.*

En este momento y todavía sin haber podido determinar el número exacto de ventas fraudulentas por lo laborioso que está resultando, le comunico, en la representación que ostento, el cierre definitivo con efectos 19 de Octubre, de la campaña de venta para de contratos de suministro de Endesa Energía y todo ello, de acuerdo con el clausulado del contrato suscrito entre las partes. (…)"

TRIGÉSIMO: El 2 de noviembre de 2021 fue desactivado ******EMPRESA.9*** como proveedor en los sistemas de ENDESA, según consta en el Documento 3 del escrito presentado por ENDESA el 3 de julio de 2023.

TRIGÉSIMO PRIMERO: El 4 de noviembre de 2021, según consta en el Documento 1 del escrito de ******EMPRESA.1*** de 25 de noviembre de 2022, ******EMPRESA.1*** ha realizado un informe sobre la violación de la seguridad de los datos personales en cuestión, por ellos detectada el 19 de octubre de 2021. El informe indica:

"(…)
La brecha de seguridad puede ser clasificada como de integridad en tanto en cuanto ha habido una alteración intencionada del número de teléfono móvil del cliente utilizado para enviar el SMS de confirmación de la venta, con la finalidad de que la aceptación de la venta la realizara otra persona y, en algunos casos, también ha habido una alteración intencionada del número de cuenta bancaria del cliente.

De igual forma, la brecha de seguridad puede ser considerada como una brecha de confidencialidad ya que, en algunos casos, la grabación de la llamada se realizaba con un cliente ficticio y, por lo tanto, esta persona tuvo acceso a datos personales del cliente cuya identidad estaba siendo suplantada.

(…)

Volumen de personas afectadas: Hay 137 operaciones de venta afectadas por contratación fraudulenta finalizada, otras 7 operaciones de venta pendientes de validación por parte de Endesa y 172 operaciones de venta que se bloquearon cuando estaban pendientes de validación por el back office de ******EMPRESA.9.*** *Puede haber personas que se hayan visto afectadas por dos o más contrataciones fraudulentas, por lo que el número de personas afectadas será inferior al número de operaciones de venta indicadas. El número final de personas afectadas lo determinará Endesa al terminar de ges-*

tionar la brecha de seguridad ya que no permiten que ******EMPRESA.1*** *continúe colaborando con ellos en la resolución de la brecha.*

No obstante, los afectados son fácilmente identificables.

Perfil de personas afectadas: Personas mayores de edad y hasta 65 años residentes en España clientes o potenciales clientes de Endesa.

El nivel de severidad de las consecuencias para las personas afectadas puede ser considerado como alto ya que podrían enfrentarse a cortes de suministro de energía, estrés y costes adicionales.

(…)

La brecha de seguridad sufrida se debe a la comisión de un delito de suplantación de identidad y contratación fraudulenta por parte de la empresa ******EMPRESA.9*** *que puede tener consecuencias negativas para los interesados afectados.*

Tras el análisis realizado, se llega a la conclusión de que se debe reforzar el procedimiento de verificación de las ventas realizadas, así como procedimiento impuesto por Endesa a sus distribuidores para la contratación telefónica. Con el procedimiento impuesto actualmente existen casos en los que es difícil verificar si la identidad de la persona que dice contratar el servicio se corresponde con la que realmente está contratándolo.

Por ejemplo, en una situación real, un cliente real podría solicitar que se introduzca un número de teléfono a efectos de contratación diferente al número donde se le está realizando la llamada comercial o, incluso, podría solicitar que el envío del SMS de confirmación de la venta se realice a un número diferente a donde se está realizando la llamada comercial (por ejemplo, si la llamada la está recibiendo en un teléfono fijo).

Por otra parte, si la operación fuera objeto de fraude, como ha sido el caso, incluso con una llamada de bienvenida o fidelización existiría una posibilidad de que no se identificara el fraude ya que el comercial involucrado podría haber introducido un número de teléfono diferente al real del titular del contrato.

Por lo tanto, entendemos que se necesitan medidas adicionales por parte de Endesa para identificar a los titulares del contrato, ya que no es posible ampliar las medidas técnicas para limitar brechas de seguridad como la sufrida teniendo en cuenta el procedimiento que como Encargado del Tratamiento ******EMPRESA.1*** *debe seguir a instancia del Responsable."*

Actualmente la brecha de seguridad sigue gestionándose por parte de Endesa."

TRIGÉSIMO SEGUNDO: El 4 de noviembre de 2021, según consta en el Documento 8 que acompaña al escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, ENDESA, *****EMPRESA.16 y ***EMPRESA.11** firmaron un ANEXO AL ACUERDO MARCO FIRMADO (...), por el que se dio cumplimiento al artículo 46.2.c) del Reglamento (UE) 2016/679, de 27 de abril, de Protección de Datos ("RGPD"), a la Decisión de Ejecución (UE) 2021/94 de la Comisión, de 4 de junio de

2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el RGPD, en lo que a las transferencias internacionales de datos entre responsable y encargado se refiere, en el que se indica que ******EMPRESA.16*** presta a ENDESA servicios de marketing telefónico y resulta necesario para ello que se subcontrate a ******EMPRESA.11***, quien actuará como importador de datos.

TRIGÉSIMO TERCERO: El 11 de noviembre de 2021, según consta en el Documento 7 que acompaña al escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador, ENDESA y ******EMPRESA.15*** firmaron un ANEXO AL ACUERDO MARCO FIRMADO, por el que se dio cumplimiento al artículo 46.2.c) del Reglamento (UE) 2016/679, de 27 de abril, de Protección de Datos ("RGPD"), a la Decisión de Ejecución (UE) 2021/94 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el RGPD, en lo que a las transferencias internacionales de datos entre responsable y encargado se refiere.

TRIGÉSIMO CUARTO: El 19 de noviembre de 2021, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó y se procedió a su retirada y eliminación en los sistemas de ******HERRAMIENTA.1***, del usuario ******USUARIO.2,*** asignado a ******EMPRESA.8***.

TRIGÉSIMO QUINTO: El 29 de noviembre de 2021, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó en los sistemas de ******HERRAMIENTA.1***, el usuario ******USUARIO.4***, asignado a ******EMPRESA.15.***

También el 29 de noviembre de 2021, según consta en el Documento número 1 que acompaña al escrito de alegaciones a la propuesta de resolución del presente procedimiento sancionador, se envió un correo electrónico en inglés al "***DEPARTAMENTO.5", en el que se informa que los siguientes usuarios se han visto comprometidos y se solicita sean reseteados lo antes posible:

- ******USUARIO.3***
- ******USUARIO.4***
- ******USUARIO.5***
- ******USUARIO.6***
- ******USUARIO.7***

Ese mismo día, según consta en el Documento número 1 que acompaña al escrito de alegaciones a la propuesta de resolución del presente procedimiento sancionador, se envió un correo electrónico en inglés desde "***DEPARTAMENTO.5", en respuesta al anterior, confirmando que las cuentas comprometidas habían sido reseteadas correctamente y que, para cada usuario, se había enviado un SMS con un enlace para cambiar la contraseña (para los casos en que fuera posible) y se había enviado un correo electrónico al manager de ese usuario con la información sobre que se había visto comprometido el usuario en cuestión, junto con el cambio de contraseña.

TRIGÉSIMO SEXTO: El 13 de diciembre de 2021, según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, se publicó el último anuncio identificado

relacionado con el uso ilícito e de credenciales de la plataforma ***HERRAMIENTA.1***. Y en enero de 2022 se realizó la última publicación identificada de la venta de bases de datos de clientes de electricidad y gas. No se han detectado nuevas publicaciones relacionadas con este incidente con fecha posterior a la notificación realizada el día 10 de febrero de 2022.

TRIGÉSIMO SÉPTIMO: El 14 de diciembre de 2021, como consta en el Documento número 8 que acompaña el citado escrito, se recibió un correo electrónico de Facebook con el asunto "Denuncia de propiedad intelectual n.º ***(...)***", en el que se indica: "*El equipo de Facebook ha recibido su denuncia. (…) Le recordamos que si se ha puesto en contacto con nosotros en relación con una supuesta vulneración de sus derechos legales, no tiene que realizar ninguna otra acción. Investigaremos el asunto lo antes posible. (…)".*

TRIGÉSIMO OCTAVO: El 12 de enero de 2022, según consta en el Documento número 9 y 10 del escrito de ENDESA de 11 de noviembre de 2022, se procedió a la eliminación en los sistemas de ***HERRAMIENTA.2*** el usuario ***USUARIO.3*** y el usuario ***USUARIO.5***, asignados a ***EMPRESA.12***.

El último acceso del usuario ***USUARIO.5*** al sistema ***HERRAMIENTA.2*** había sido el 25 de noviembre de 2021.

El último acceso del usuario ***USUARIO.3*** al sistema ***HERRAMIENTA.2*** había sido el 26 de noviembre de 2021.

TRIGÉSIMO NOVENO: El 17 de enero de 2022 (según consta en el documento número 8 del escrito presentado por ENDESA el 26 de julio de 2022), se publicaron anuncios por parte del usuario ***B.B.B.***, en los que existió afectación a bases de datos de clientes de energía de ENDESA.

CUATRIGÉSIMO: El 31 de enero de 2022 ENDESA redactó un burofax, según consta en el Documento número 11 del escrito de ENDESA de 11 de noviembre de 2022, dirigido a ***EMPRESA.1***, con el siguiente contenido:

"Estimado Proveedor:

*Nos dirigimos a ti en relación con el Contrato Nº **(...)** firmado entre ENDESA ENERGÍA, S.A.U., (en adelante ENDESA ENERGÍA) y **EMPRESA.1,** (en adelante **EMPRESA.1**) y como continuación de anterior comunicación remitida por parte de esta entidad con fecha de 20 de diciembre de 2021 por medio de la que pusimos en conocimiento de **EMPRESA.1** la aplicación de penalizaciones de conformidad con lo dispuesto en la Cláusula 12 del referido Contrato.*

*Como es conocido por parte de **EMPRESA.1** por parte de ENDESA ENERGÍA se han detectado, mediante la correspondiente auditoria de control de calidad conforme a lo dispuesto en la Cláusula 15.4 del Contrato suscrito, numerosas irregularidades en relación con el procedimiento de gestión de contrataciones previsto en el Anexo 2D del Contrato suscrito en el periodo comprendido entre octubre y noviembre de 2021, ambos inclusive. Tanto es así que como también es conocido por parte de*

***EMPRESA.1** se han recibido diversos requerimientos de información por parte de la AEPD en relación con contrataciones gestionadas por parte de *****EMPRESA.1**.*

*En concreto y a modo recordatorio, venimos a enumerar los diversos requerimientos que hasta la fecha se han recibido en ENDESA ENERGÍA por parte de la AEPD y que tienen su origen en gestiones de contratación llevadas a cabo por parte de *****EMPRESA.1** y que ponen de manifiesto el incumplimiento de forma reiterada y continuada del Contrato suscrito y de los procedimientos establecidos en éste:*

(…)

Ante la gravedad de las irregularidades detectadas que constituyen un incumplimiento además reiterado del Contrato suscrito, por medio del presente y sin perjuicio de la aplicación de penalizaciones que ya fue comunicada mediante misiva de 20 de diciembre de 2021 y de otras posibles que procedan de conformidad con el contrato suscrito, le informamos que es voluntad de ENDESA ENERGÍA, al amparo de lo previsto en su Cláusula 13, resolver éste con efectos la citada resolución desde la fecha de recepción de la presente comunicación.(…)"

CUATRIGÉSIMO PRIMERO: El 7 de febrero de 2022, según consta en el Documento número 9 del escrito de ENDESA presentado el 7 de octubre de 2022, ENDESA envió un burofax con una comunicación escrita a FACEBOOK SPAIN S.L., el cual fue entregado el 8 de febrero de 2022, con el siguiente contenido:

"(…) PRIMERO: Se ha detectado desde finales del 2021 hasta la fecha que la red social FACEBOOK se viene utilizando para prácticas fraudulentas que perjudican de forma grave los intereses de ENDESA, todas ellas relacionadas con la venta de credenciales de acceso a plataformas de gestión con datos de carácter personal. En este sentido:

1. Se han efectuado búsquedas en redes sociales y fuentes abiertas, detectando que todos los anuncios de venta de credenciales se publicitan en FACEBOOK.
2. Actualmente, se han identificado al menos un total de 10 publicaciones activas (…)
3. De todas ellas se les ha solicitado la baja sin obtener respuesta alguna y sin que conste ninguna acción al respecto. Para los anuncios con fecha de publicación más antigua esta solicitud de baja se ha efectuado en más de 10 ocasiones sin haber conseguido que se lleve a término.
*4. Estos anuncios han sido publicados por 3 perfiles esencialmente: "**B.B.B.", "C.C.C." y "D.D.D.**", siendo los dos primeros los más activos, e incluyendo sus perfiles público y marketplace (…)*
*5. Paralelamente, se han identificado 2 perfiles marketplace asociados a "**B.B.B.**" y "**C.C.C.**", presumiblemente controladas por la misma persona, a las que se asocian más de 210 y 197 publicaciones, respectivamente (…). Estos anuncios son capturas de pantalla de bases de datos de carácter personal cuya procedencia o titularidad las desconocemos.*

Adicionalmente a lo señalado, se han detectado Grupos que incluyen acciones similares a las señaladas: (…)

Como podrán comprobar, los distintos anuncios de usuarios aparecen anunciando la venta/alquiler de usuarios y contraseñas de acceso a la plataforma ******PLATAFORMA.1****, propiedad de ENDESA. A día de hoy se desconoce si existe un número superior de perfiles así como de ofertas.*

(…)

CUARTO: Han sido reiteradas las advertencias a su compañía de los citados comportamientos sin que, siendo esto más grave aún, se haya reparado el daño pese a la constancia de la situación. En numerosos casos incluso se señala que "no tenemos claro que el contenido que ha denunciado sea ilegal, por lo que no podemos realizar ninguna acción en estos momentos". El presente requerimiento se remite por burofax tras numerosos intentos previos enviados a las direcciones facilitadas para estos.

QUINTO: Ante la gravedad de los hechos mencionados en el apartado anterior, (…) nos vemos en la obligación de informarles de que las prácticas descritas, a priori (…) podría constituir una venta/alquiler de credenciales propiedad de ENDESA susceptible de ser tipificada como un delito contemplado en el artículo197 ter b) del Código Penal español (…)

Por lo expuesto en los apartados anteriores, requerimos a su compañía a que, con carácter inmediato, se comprometa a retirar dichos anuncios y los preserve para que, en caso de ser reclamados, puedan ser tratados como evidencia en un posible proceso judicial. (…)"

CUATRIGÉSIMO SEGUNDO: El 8 de febrero de 2022, Facebook Spain S.L. contestó a ENDESA lo siguiente (según consta en el Documento 10 que acompaña el escrito de ENDESA de 7 de octubre de 2022):

"Facebook Spain S.L. (en adelante <<Facebook Spain>>) acusa recibo de su correspondencia.

Facebook Spain S.L. (en adelante, «Facebook Spain») acusa recibo de su correspondencia. En primer lugar, por favor tenga en cuenta que Facebook Spain no es la entidad competente para resolver su consulta. Nada en esta correspondencia debe ser interpretado como una admisión de lo contrario. Le informamos que, para los usuarios situados en España, Facebook Spain no opera ni tiene control sobre los Productos de Facebook (tal y como están definidos en nuestras Condiciones del servicio, disponibles en https://www.facebook.com/terms.php).

Para los usuarios situados en España, la operación y el control de los Productos de Facebook corresponde a Facebook Ireland Limited, una entidad constituida en Irlanda con domicilio social en Dublín. Facebook Ireland Limited es la entidad con la cual los usuarios situados en España mantienen una relación contractual. Facebook Spain es una entidad autónoma, independiente y jurídicamente distinta de Facebook Ireland Limited. Por lo tanto, Facebook Spain no tiene capacidad alguna para decidir o tomar acción alguna en relación con lo solicitado en su correspondencia.

Le solicitamos que dirija su consulta a la entidad competente, Facebook Ireland Limited, a través de los Servicios de ayuda disponibles en: https://www.facebook.com/help/ , https://help.instagram.com/ , o a través de:
Facebook Ireland Limited
Attn: Legal Department
4 Grand Canal Square
Grand Canal Harbour
Dublin 2, Ireland

Gracias por ponerse en contacto con nosotros. Esperamos que la información anterior sea de utilidad. Nos reservamos todos nuestros derechos.

Atentamente,
Facebook Spain"

CUATRIGÉSIMO TERCERO: El día 8 de febrero de 2022, tras las investigaciones oportunas, ENDESA tuvo conocimiento de la existencia de ciertas coincidencias entre los datos que aparecían en las bases de datos publicadas y los que podían estar incluidos en el sistema comercial de ENDESA, ******HERRAMIENTA.2***.

ENDESA llevó a cabo una nueva valoración del incidente y con fecha 9 de febrero de 2022 comprobó la veracidad de los anuncios y la identidad de los dos anunciantes, ambos extrabajadores de proveedores de ENDESA con acceso a ******PLATAFORMA.1 (***HERRAMIENTA.1)***. Se detectaron un total de nueve usuarios comprometidos entre septiembre de 2021 y enero de 2022, que estaban siendo usados por los anunciantes de Facebook para vender accesos *a* ******PLATAFORMA.1 (***HERRAMIENTA.1***). Además, se comprobó que seis de ellos tenían acceso a ******HERRAMIENTA.2***. Se comprobó también la validez de las credenciales, en todos los casos asignadas a proveedores de ENDESA para realizar trabajos de captación y atención al cliente.

CUATRIGÉSIMO CUARTO: El 9 de febrero de 2022 se realiza un informe de valoración del alcance de la violación de la seguridad de los datos personales, según consta en el Documento número 5 que acompaña el escrito de ENDESA de 26 de julio de 2022, en la que se considera la existencia de un riesgo para los derechos y libertades de los afectados y la necesidad de notificar la misma a la AEPD.

En este informe se indica lo siguiente:

"*El día 24 de agosto se detectó en Facebook varios anuncios donde se vendían usuarios de la aplicación* ******PLATAFORMA.1*** *con acceso a información de clientes para campaña de energía en España. Una vez detectado los anuncios se inicia una investigación, obteniendo la comprobación de la veracidad de estos y la identidad de los dos anunciantes, ambos extrabajadores de proveedores de Endesa con acceso a* ******PLATAFORMA.1****.*

Durante el avance de la investigación se detectan un total de nueve usuarios comprometidos entre septiembre de 2021 y enero de 2022. Dentro de las medidas tomadas para el control del incidente se hace un seguimiento de los anuncios publicados por los dos perfiles relacionados con el incidente, detectándose en enero de 2022 un anuncio de venta de bases de datos de clientes de energía y

comprobándose que en las imágenes de los Excel publicados en los anuncios, hay datos parciales de clientes de Endesa y datos de usuarios de otras compañías, estos últimos no han podido ser obtenidos de las aplicaciones de Endesa por lo que se deduce que son recopilaciones de datos de clientes de distintas compañías.

Los nueve usuarios comprometidos estaban siendo usados por los anunciantes en Facebook para vender accesos a ******PLATAFORMA.1****, además se comprueba que seis de ellos tenían acceso a* ******HERRAMIENTA.2****. Se ha comprobado la validez de las credenciales, en todos los casos asignadas a proveedores de Endesa para realizar trabajos de captación y atención al cliente, estos usuarios podrían haberse usado en paralelo de forma ilegal, esto impide conocer el número de registros de los aplicativos que han podido ser accedidos.*

Basándonos en la información recogida hasta ahora, que incluye el tiempo transcurrido desde la publicación del anuncio, el tipo de servicio ofertado y las limitaciones en las consultas ofrecidas por los aplicativos, se estima que el número de registros afectado podría estar en una horquilla de accesos de entre 1.000 y 100.000.
(…)

III. CONCLUSIÓN
En reunión mantenida ***(…)****, tras realizar una valoración, en tiempo y forma, del alcance del incidente de seguridad y de las posibles repercusiones para los derechos y libertades de los interesados afectados, se adopta la decisión preliminar de comunicar el incidente de seguridad a la autoridad de control.*

Considerando los planteamientos anteriores, se enumera el plan de acción ejecutado:

- *Reseteo de las contraseñas de los usuarios potencialmente afectados (****…)***
- *Baja de los anuncios de Facebook donde se ofrecían los accesos (****…)***
- *Burofax a Facebook para agilizar las bajas (****…)***
- *Deshabilitar las sesiones simultaneas en* ******PLATAFORMA.1.***
- *Ampliar los registros (logs) de* ******PLATAFORMA.1*** *para obtener información detallada del uso realizado por sus usuarios.*

Se propone, a su vez, la adopción de las siguientes medidas al objeto de evitar problemas similares, así como al objeto de mitigar potenciales efectos negativos en perjuicio de los interesados:

(…)

CUATRIGÉSIMO QUINTO: El 9 de febrero de 2022 el Delegado de Protección de Datos envió un correo electrónico, con el siguiente contenido, según Documento número 1 que acompaña el escrito del DPD de 19 de octubre de 2022:

*"(…) Para que no haya ningún género de duda, y como anticipé en la reunión, la conclusión desde ***DEPARTAMENTO.4 y mía como responsable último ante la AEPD es que vamos a notificar esta brecha.*
Para justificar que notificamos ahora es necesario que nos facilitéis en la mañana de hoy una relación detallada de fechas y acciones realizadas que podamos aportar a la AEPD (…)"

CUATRIGÉSIMO SEXTO: Con fecha 10 de febrero de 2022, ENDESA notificó a la Agencia Española de Protección de Datos (AEPD) una violación de la seguridad de los datos personales, consistente en un posible acceso no autorizado a ciertos sistemas comerciales de Endesa Energía que podría haber afectado a unos mil clientes.

En esta notificación se informa a la AEPD de lo siguiente:

"En agosto de 2021, se detectan ciertos anuncios de Facebook que anuncian la venta de credenciales para acceder a la plataforma ******PLATAFORMA.1*** *de ENDESA (que contiene datos básicos y relativos al punto de suministro). Se valoró ese incidente y se adoptaron las medidas pertinentes. El 17/01/2022 se detecta un anuncio de Facebook con características similares a los anteriores que informa de la venta de bases de datos de clientes de energía y gas. Se hace una valoración del anuncio y no se encuentran coincidencias con datos de clientes de ENDESA incluidos en el sistema CRM. El 8/02/2022 se detectan datos de, entre otros, algunos clientes de ENDESA incluidos en el sistema CRM.*

Número aproximado de personas físicas sobre las que recoge, almacena o trata datos personales de otra forma; referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales: 6.500.000.

El incidente ha sido: Intencionado, para hacer daño al responsable / encargado o a las personas afectadas.

El origen del incidente ha sido: Externo: Otros, ajenos al responsable y encargado del tratamiento

¿Qué puede haber ocurrido?: Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales

Como consecuencia del incidente, se ha visto afectada la: Confidencialidad

Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?: No

¿Qué puede haber ocurrido?: Usurpación de identidad, Pérdida de control sobre sus datos personales

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?:
Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

A fecha de esta notificación, ¿tiene constancia de que se hayan materializado alguno de los daños identificados, con el grado indicado en la cuestión anterior?: Si

Tipos de datos afectados: Datos básicos (Ej nombre, apellidos, fecha de nacimiento), DNI, NIE, Pasaporte y / o cualquier otro documento identificativo, Datos de medios de pago (Tarjeta bancaria, etc.), Datos de contacto

En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales?: 1000

Indique la fecha de detección de la brecha: 08/02/2022

¿Conoce la fecha en la que se inició la brecha? Aproximadamente el 24/08/2021

Indique la fecha en la que se dio por resuelta la brecha: 10/02/2022

¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas?: No serán informados

Las personas afectadas no serán informadas porque: No existe un riesgo alto para sus derechos y libertades

Junto a la notificación se aporta como Anexo I las medidas tomadas para solucionar la brecha y minimizar el impacto:

"Tras la detección inicial, en agosto de 2021, de venta no autorizada de credenciales de acceso a la plataforma ******PLATAFORMA.1****, se adoptaron las siguientes medidas al objeto de mitigar posibles efectos negativos:*

• Reseteo de las contraseñas de los usuarios afectados para acceder a la plataforma ******PLATAFORMA.1****. Esta medida se lleva a cabo de manera continua.*
• Seguimiento de nuevas publicaciones en Facebook. Esta medida se lleva a cabo de manera continua.
• Deshabilitar las sesiones simultaneas en ******PLATAFORMA.1****, de tal manera que no puedan acceder dos o más personas a la vez con un único usuario. Esta medida se implantó en el mes de noviembre de 2021.*
• Ampliar la trazabilidad (logs) de los accesos a ******PLATAFORMA.1*** *para obtener información detallada del uso realizado por parte de los usuarios. Esta medida se implantó a finales del mes de diciembre de 2021.*
• Solicitar la baja de los anuncios de Facebook donde se ofrecía la venta de dichos usuarios. Esta medida se lleva a cabo de manera continua.
Posteriormente, con motivo de los nuevos acontecimientos detectados (venta en Facebook de ciertas bases de datos que contienen, entre otros, datos de clientes de Endesa Energía incluidos en el sistema CRM que alberga datos básicos, de contacto, CUPS, datos relativos al contrato de electricidad o gas y el número de cuenta), se van a implantar, entre otras, las siguientes medidas adicionales:

(…)

CUATRIGÉSIMO SÉPTIMO: El 15 de febrero de 2022, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó o deshabilitó de la plataforma ******HERRAMIENTA.1*** al usuario ******USUARIO.1***, asignado a ******EMPRESA.13***. y al usuario ******USUARIO.9***, asignado a ******EMPRESA.14***

CUATRIGÉSIMO OCTAVO: El 17 de febrero de 2022, según consta en el Documento número 9 y 10 del escrito de ENDESA de 11 de noviembre de 2022, se eliminó de los sistemas de ******HERRAMIENTA.2*** el usuario ******USUARIO.6***, asignado a ******EMPRESA.17***.

CUATRIGÉSIMO NOVENO: El 28 de febrero de 2022, según consta en el Documento número 11 del escrito de ENDESA presentado el 7 de octubre de 2022, ENDESA envió un burofax con una comunicación escrita a FACEBOOK SPAIN S.L., con el siguiente contenido:

"(…)
En la mencionada contestación a nuestro burofax ponen de manifiesto que Facebook Spain SL no tiene capacidad alguna para decidir o tomar acción alguna en relación con lo solicitado en nuestra correspondencia. Por parte de nuestra compañía, discrepamos absolutamente de lo manifestado ya que mi representada no es usuaria de la plataforma y, por tanto, reiteramos nuevamente nuestro escrito inicial en calidad de afectados.

Tal y como se les señalaba, se ha detectado que determinados usuarios de su plataforma están haciendo uso de la misma para publicar determinadas informaciones que podrían ser constitutivas de delito, delito que entendemos debería ser enjuiciado en España al no estar mi representada sometida a la jurisdicción de los tribunales irlandeses por no haber aceptado dicha jurisdicción y producirse el delito en España contra una empresa española.

Por tanto nuestra comunicación tiene como principal finalidad recabar la colaboración de Facebook (Meta) con el objetivo de limitar estas presuntas acciones delictivas que están perjudicando seriamente los intereses de nuestra compañía. Les reiteramos igualmente la necesidad de mantener los archives oportunos de cara a un posible proceso judicial. (…)"

QUINCUAGÉSIMO: El 4 de marzo de 2022, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se retiró y eliminó de los sistemas de ******HERRAMIENTA.1*** el usuario ******USUARIO.4***, asignado a ******EMPRESA.15***, si bien expiró por caducidad.

QUINCUAGÉSIMO PRIMERO: El 16 de marzo de 2022, según consta en el Documento 9 y 10 del escrito de ENDESA de 11 de noviembre de 2022, se eliminaron de los sistemas de ******HERRAMIENTA.2*** el usuario ******USUARIO.4***, asignado a ******EMPRESA.15.***

QUINCUAGÉSIMO SEGUNDO: El 23 de marzo de 2022 se completa el despliegue de MFA (autenticación multifactor) en la plataforma ******HERRAMIENTA.2*** y en la plataforma ******PLATAFORMA.1***, según se indica en el informe pericial de fecha 23 de junio de 2023, presentado por ENDESA el 3 de julio de 2023.

QUINCUAGÉSIMO TERCERO: El 1 de abril de 2022, según consta en los Documentos número 2 y 3 del escrito presentado por ENDESA en fecha 6 de abril de 2022, ENDESA, a través de su proveedor ******EMPRESA.2***, ha impreso y puesto a disposición de

la empresa encargada del servicio postal 760 envíos, los cuales fueron entregados a Correos ese mismo día.

El modelo de comunicación remitido en español es el siguiente:

> *"31 de Marzo de 2022*
> *Estimado cliente,*
> *Nos ponemos en contacto contigo para informarte que hemos detectado un posible acceso indebido a determinados sistemas comerciales de Endesa Energía y que desde el mismo momento que hemos sido conocedores de este hecho, hemos adoptado las oportunas medidas de seguridad, técnicas y organizativas, para evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades de nuestros clientes, con lo que la confidencialidad y la integridad de tus datos personales no se ha visto comprometida.*
>
> *Puedes consultar nuestra política de privacidad en www.endesa.com/es/proteccion-datos-endesa, donde encontrarás la información relativa al tratamiento de tus datos personales. Si lo prefieres, puedes contactar directamente con nuestro Delegado de Protección de Datos enviando una comunicación a ***EMAIL.1 para conocer el detalle de las medidas adoptadas u obtener más información.*
>
> *Aprovechamos para agradecerte la confianza depositada en Endesa.*
>
> *Un cordial saludo,*
> *Endesa Energía."*

QUINCUAGÉSIMO CUARTO: El 6 de abril de 2022 ENDESA recibió un correo electrónico por parte de uno de los destinatarios de la comunicación de la violación de la seguridad de los datos personales a los afectados, según consta en el Documento número 9 del escrito de ENDESA de 26 de julio de 2022, con el siguiente contenido:

"Buenos días:

Me dirijo a ustedes por una carta que me envían para hablar de un posible acceso indebido al sistema de Endesa energía.

No se de que me hablan, pues yo no soy cliente de Endesa y aunque a veces me llega un recibo a mi nombre con 0 cargo, el dni no corresponde con el mío, he intentado solucionarlo llamando por teléfono sin resultado ni solución, con lo cual espero respuesta por su parte, si es que quieren arreglar el entuerto, si quieren contactar conmigo por teléfono es el número (…)

Un saludo"

Según manifestó ENDESA en el citado escrito, sólo se ha recibido este único correo electrónico por parte de uno de los destinatarios de dicha comunicación. Se solicitó la documentación acreditativa de su identidad, y no consta respuesta por su parte.

QUINCUAGÉSIMO QUINTO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, ******HERRAMIENTA.1*** es una herramienta especialmente diseñada

para facilitar el asesoramiento, la atención y venta en los diferentes canales comerciales de ENDESA.

Esta herramienta incorpora la información comercial de los productos y servicios que ofrece en cada momento ENDESA (tales como precios, complementos, validez, ofertas o condiciones), contiene información técnica de todos los puntos de suministro, así como ciertos datos identificativos básicos.

QUINCUAGÉSIMO SEXTO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, los usuarios de ******HERRAMIENTA.1*** pueden ser de dos tipos: (i) usuario "interno", habilitado para los empleados de Endesa Energía y (ii) usuario "externo", habilitado para los proveedores externos. No existen otros usuarios externos, como puedan ser clientes.

Tanto los usuarios internos como los usuarios externos tienen acceso a todas las funcionalidades principales de la herramienta.

A su vez, desde el punto de vista funcional la plataforma cuenta con el rol de usuario "básico", y el rol con "perfil de administrador". Es decir, un usuario con "perfil de administrador" también puede ser, a su vez, "interno" o "externo". Únicamente los usuarios que tienen el "perfil de administrador" pueden acceder al menú de administración y realizar cargas de información en el sistema (tales como nuevas ofertas, tarifas o argumentarios). También pueden editar ciertos campos de la herramienta y obtener extracciones e informes.

QUINCUAGÉSIMO SÉPTIMO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, el alta de los usuarios externos e internos la realizan los responsables de cada canal de ventas o de atención en la herramienta de soporte técnico corporativa a la que se accede a través de la Intranet habilitada para todos los empleados internos del Grupo Endesa. Los accesos se solicitan desde Intranet.

Los usuarios externos e internos acceden a la plataforma insertando el usuario y la contraseña asociada.

QUINCUAGÉSIMO OCTAVO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, la plataforma permite la opción de introducir el denominado Código Universal de Punto de Suministro (en adelante, "CUPS") o la dirección del punto de suministro, para mostrar la información técnica asociada (se describe en el Documento número 4). En caso de que el cliente ya tenga un contrato en vigor con Endesa Energía también muestra la siguiente información: nombre y apellidos del titular del punto de suministro, su número de Documento Nacional de Identidad, número de contrato, CUPS, importe de facturación anual, datos técnicos referentes al punto de suministro, datos de consumo y gráfico de utilización. Dentro de la ficha relativa al punto de suministro aparecen una serie de apartados que permiten recomendar al cliente otras tarifas.

QUINCUAGÉSIMO NOVENO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, para determinar el número de personas potencialmente afectadas por el incidente, se llevó a cabo el siguiente análisis:

(i) Se comprobó la supuesta práctica irregular llevada a cabo por una empresa subcontratista de uno de los proveedores de ENDESA que presta servicios de venta telefónica, y se verificó no se había extendido a otros proveedores.
(ii) Se acotó el perímetro de análisis a todas aquellas contrataciones efectuadas entre el 1 de julio de 2021, fecha en la que el volumen de ventas de ENDESA sufrió un aumento inusual y no justificado (+500%), y el 15 de octubre de 2021, fecha en la que se rescindió el contrato con el proveedor y, por tanto, dejó de prestar sus servicios.
(iii) Posteriormente, se llevó a cabo un control de calidad y auditoría de las contrataciones objeto de valoración, y se descartaron aquellos casos en los que los propios clientes ya se habían puesto en contacto con ENDESA para realizar acciones propias de sus contratos (por ejemplo, consultas comerciales).

SEXAGÉSIMO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, el número de potenciales afectados por el incidente resultante fue: 760 clientes.

SEXAGÉSIMO PRIMERO.- Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, a pesar de no ser posible determinar el posible objetivo buscado por las personas que facilitaban la venta de credenciales para acceso a la plataforma ******HERRAMIENTA.1***, así como, en su caso, la venta de bases de datos de clientes de Endesa Energía, ENDESA considera que las consecuencias de la violación de la seguridad de los datos personales se limitan a que las personas afectadas podrían encontrar ciertos inconvenientes, muy limitados y, en todo caso, reversibles.

Debido al objetivo, aparentemente fraudulento, de sustracción de datos, las consecuencias para los clientes afectados serían fundamentalmente la venta de sus datos para la realización de llamadas comerciales, así como para el envío de correos y SMS, ofreciendo la posibilidad de cambiar de compañía comercializadora de energía, lo que, en los peores escenarios y de llegar a materializarse, podría resultar en el cambio de empresa comercializadora sin su consentimiento.

SEXAGÉSIMO SEGUNDO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, la violación de la seguridad de los datos personales ha sido provocada por la aparente venta fraudulenta de credenciales de la plataforma ******HERRAMIENTA.1***. Estas credenciales estaban asignadas a proveedores de ENDESA, como usuarios externos de la plataforma, para facilitar las tareas captación, asesoramiento y atención al cliente.

SEXAGÉSIMO TERCERO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, ENDESA tuvo conocimiento del posible uso ilícito de las credenciales a través del correo de uno de los proveedores donde se indican irregularidades por varios de sus trabajadores, en ese mismo correo se indican cinco usuarios que han sido empleados de forma aparentemente irregular.

SEXAGÉSIMO CUARTO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, se identifican otros cuatro usuarios que pudieran estar comprometidos, detectados en los videos de demostración y en las capturas de los anuncios publicados.

SEXAGÉSIMO QUINTO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, los usuarios comprometidos fueron:

- ******USUARIO.1***
- ******USUARIO.2***
- ******USUARIO.3***
- ******USUARIO.4***
- ******USUARIO.5***
- ******USUARIO.6***
- ******USUARIO.7***
- ******USUARIO.8***
- ******USUARIO.9***

SEXAGÉSIMO SEXTO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, no ha recibido ninguna reclamación por parte de los clientes potencialmente afectados por este incidente.

SEXAGÉSIMO SÉPTIMO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, ENDESA, como parte del Grupo Endesa cuenta con una serie de normas y estándares de seguridad para garantizar la protección de los datos personales, basados, principalmente, en los siguientes elementos: (i) un marco de ciberseguridad, (ii) normativa interna sobre ciberseguridad.

[…]

- Concretamente las medidas implementadas en las aplicaciones objeto de la presente violación de la seguridad de los datos personales de seguridad consisten, ***(…)***.

SEXAGÉSIMO OCTAVO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, entre las distintas actividades y medidas de seguridad distintas medidas de seguridad que existían en ******HERRAMIENTA.2*** antes del incidente destacan las siguientes:

(…)

Y la aplicación ******HERRAMIENTA.2*** se encontraba integrada ***(…)*** en la fecha del incidente.

SEXAGÉSIMO NOVENO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, entre las distintas actividades y medidas de seguridad que se tenían implementadas en la plataforma ******HERRAMIENTA.1*** antes del incidente destacan las siguientes:

- ***(…).***

SEPTUAGÉSIMO: Según manifestó ENDESA en su escrito presentado el 26 de julio de 2022, a medida que se fue desarrollando el incidente y advirtiéndose sus posibles efectos, se implantaron las siguientes medidas para reforzar la seguridad de las aplicaciones ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***:

(…)

SEPTUAGÉSIMO PRIMERO: El 3 de agosto de 2022 el usuario "***D.D.D.***" publicó en Facebook un anuncio con el siguiente contenido, según consta en el Documento número 2 que acompaña al escrito de ENDESA de 11 de noviembre de 2022: "*Se alquila sistema para obtener cups de energía y gas [emoji de la bandera de España] Mediante la dirección del cliente. [Emoji de una bombilla encendida] Precios super accesibles [emoji de un fajo de billetes] Información al wsp."*

SEPTUAGÉSIMO SEGUNDO: El 23 de agosto de 2022 el usuario "***B.B.B.***" publicó en Facebook un anuncio con el siguiente contenido, según consta en el Documento número 2 que acompaña al escrito de ENDESA de 11 de noviembre de 2022:
"Se vende usuario
Contactar al vendedor
[varios emojis de cara de sorpresa]
*Se vende usuario de #****PLATAFORMA.1*** *para campaña de energía España!!!*
- Te brinda total de suministros que tiene el titular bajo su nombre.
- Te da toda la información de su suministro (cups, DNI, código postal, dirección, tarifa, última boleta).
- Te da la información completa si el cliente cuenta con luz y gas
Si te interesa incrementar el número de ventas en tu Call Center, escríbeme por imbox"

Se observan en el anuncio dos capturas de imagen del sistema, con domicilio completo y datos de consumo de luz y gas.

SEPTUAGÉSIMO TERCERO: El 24 de agosto de 2022, según consta en el Documento número 8 del escrito de ENDESA de 11 de noviembre de 2022, se reseteó en la plataforma ******HERRAMIENTA.1*** el usuario ******USUARIO.6***, asignado a ******EMPRESA.17.***

También se procedió a la retirada y eliminación en los sistemas de ******HERRAMIENTA.1*** los siguientes usuarios:

USUARIO	PROVEEDOR AL CUAL FUE ASIGNADO
******USUARIO.1***	******EMPRESA.13***
******USUARIO.9***	******EMPRESA.14***
******USUARIO.8***	******EMPRESA.15***
******USUARIO.3***	******EMPRESA.12 (***EMPRESA.12.)***
******USUARIO.5***	******EMPRESA.12 (***EMPRESA.12.)***

SEPTUAGÉSIMO CUARTO: El 15 de septiembre de 2022 seguían publicados en Facebook los anuncios identificados por ENDESA donde se ofrecía la venta de credenciales de acceso a *****HERRAMIENTA.1** y bases de datos (ver en el expediente el documento de Diligencia del 16 de diciembre de 2022).

SEPTUAGÉSIMO QUINTO: Según manifiesta ENDESA en su escrito de 7 de octubre de 2022, identificó en los propios anuncios y videos demostrativos publicados en la red social Facebook cuatro usuarios de la herramienta ******HERRAMIENTA.1*** (******HERRAMIENTA.1***) que estaban comprometidos.

SEPTUAGÉSIMO SEXTO: Según manifiesta ENDESA en su escrito de 7 de octubre de 2022, los usuarios comprometidos identificados habían sido asignados a alguna de las siguientes empresas proveedoras de ENDESA:

- ******EMPRESA.3***
- ******EMPRESA.12***
- ******EMPRESA.5***
- ******EMPRESA.6***
- ******EMPRESA.7***
- ******EMPRESA.8.***

SEPTUAGÉSIMO SÉPTIMO: Según manifiesta ENDESA en su escrito de 7 de octubre de 2022, el proveedor de ENDESA que prestaba servicios de venta telefónica cuya empresa subcontratista llevó a cabo la supuesta práctica irregular fue ******EMPRESA.1*** y la empresa subcontratista a la que encargó la prestación de parte de los servicios encomendados fue ******EMPRESA.9***.

SEPTUAGÉSIMO OCTAVO: Según manifiesta ENDESA en su escrito de 7 de octubre de 2022, en el análisis que se llevó a cabo para la correcta identificación de los clientes cuyos datos aparentemente habían sido sustraídos sin autorización de la herramienta ******HERRAMIENTA.3*** y, por tanto, podían eventualmente haber sido tratados sin su consentimiento, se realizaron las siguientes actuaciones:

> *"i. En primer lugar, una vez el proveedor* ******EMPRESA.1*** *puso en conocimiento de ENDESA la práctica irregular cometida por personal de* ******EMPRESA.9*** *y se realizaron las comprobaciones oportunas, se verificó que dicha práctica no se extendía a otros proveedores.*
> *ii. En segundo lugar, una vez identificado el posible origen de las contrataciones supuestamente irregulares, se procedió a acotar el alcance temporal de sus actuaciones, verificándose que a partir de 1 de julio de 2021 el volumen de ventas de Endesa Energía experimentó un aumento inusual no justificado (concretamente, las ventas se incrementaron en más del 500%) lo cual podía ser representativo de las actuaciones irregulares del personal contratado por* ******EMPRESA.9****. Con fecha 15 de octubre de 2021 se cesó la actividad de dicho subcontratista – como consecuencia de la rescisión del contrato con* ******EMPRESA.9*** *–, limitando, por tanto, el perímetro temporal de análisis de las contrataciones al período comprendido entre el 1 de julio y 15 de octubre de 2015.*
> *iii. Finalmente, se llevó a cabo un control de calidad y auditoría de las contrataciones llevadas a cabo por* ******EMPRESA.9*** *en el perímetro temporal fijado. En dicho análisis, se descartaron aquellos casos en los que los propios clientes en cuyo nombre se había efectuado una contratación en la que intervino* ******EMPRESA.9*** *– en el período de tiempo delimitado –, se habían puesto en contacto con ENDESA para realizar acciones propias de sus contratos (por ejemplo, consultas comerciales), lo cual era indicativo de que los propios clientes eran conocedores de sus contratos y no manifestaron objeción alguna."*

SEPTUAGÉSIMO NOVENO: Según consta en la diligencia realizada el día 13 de octubre de 2022, ENDESA es una sociedad anónima de nacionalidad española. Según los datos obrantes en AXESOR la empresa tiene tamaño "Grande" con XXX

empleados y en el año 2021 (último ejercicio presentado) tuvo un volumen de negocio global anual de ***CANTIDAD.1 euros y un resultado de ejercicio de ***CANTIDAD.3 euros.

OCTOGÉSIMO: Según ha manifestado ENDESA en su escrito presentado el 11 de noviembre de 2022, durante la investigación iniciada a finales del mes de agosto del año 2021, se identificaron un total de 440 anuncios en la red social Facebook en los que se ofrecía el alquiler y/o venta de credenciales de acceso a la herramienta de ENDESA ******HERRAMIENTA.1*** (en adelante "******HERRAMIENTA.1***").

Los dos usuarios identificados desde cuyos perfiles de Facebook se publicaron dichos anuncios fueron los correspondientes a "***B.B.B.***" (quien, presumiblemente, también realizó publicaciones bajo el perfil de ***C.C.C.***) y "***D.D.D.***". En el trascurso de la investigación, el área de Seguridad de la Información de ENDESA realizó un contacto con el usuario ***B.B.B.*** quien ofreció la venta de credenciales para acceder a ******HERRAMIENTA.1*** a cambio de un pago mensual. Asimismo, indicaba que disponía de diferentes usuarios para su venta.

Como consecuencia de las conversaciones mantenidas entre los responsables de ENDESA y sus proveedores y, a su vez, de éstos con sus subcontratistas, se ha tenido conocimiento de que tras el usuario "***B.B.B.***" / "***C.C.C.***" se encuentra ***C.C.C.***, quien, tal y como ha sido trasladado a esta Oficina, fue empleado hasta el año 2016 de ******EMPRESA.10***. Esta sucursal nunca ha prestado servicios para ENDESA y consecuentemente ***C.C.C.*** nunca tuvo asignado a su nombre un usuario de acceso a las aplicaciones de ENDESA.

Por su parte, el usuario "***D.D.D.***" se corresponde con la trabajadora de ******EMPRESA.11***, empresa subcontratista en ***PAÍS.1 del proveedor ******EMPRESA.12*** quien presta servicios para ENDESA, ***D.D.D.***, quien, sin embargo, se dio de baja al inicio del año 2020.

No figura en los sistemas internos de la compañía ningún registro de alta de un usuario a nombre de ***D.D.D.***.

OCTOGÉSIMO PRIMERO: Según escrito de ENDESA de 11 de noviembre de 2022, los usuarios comprometidos puestos a la venta junto con el proveedor al que fueron asignados eran los siguientes:

USUARIO	PROVEEDOR
******USUARIO.1***	******EMPRESA.13*** **(en adelante, ***EMPRESA.13)**
******USUARIO.9***	******EMPRESA.14*** **(en adelante, ***EMPRESA.14)**
******USUARIO.2***	******EMPRESA.8.*** **(en adelante, ***EMPRESA.8)**
******USUARIO.10***	******EMPRESA.15***

En relación con los proveedores ******EMPRESA.13, ***EMPRESA.14 y ***EMPRESA.8***, los tres prestaban servicios de venta a ENDESA por vía telefónica mediante llamadas salientes de la compañía. La comunicación relativa a la violación de la seguridad de los datos personales y al uso indebido de los usuarios de acceso a las aplicaciones de

ENDESA que les habían sido asignados, se llevó a cabo por medio de conversaciones y reuniones telefónicas.

En relación con el proveedor ***EMPRESA.15**, éste prestaba servicios de atención y venta telefónica a ENDESA, atendiendo las llamadas que, sin previa intervención comercial de ENDESA, realizan los interesados. El responsable de operaciones, de forma inmediata tras conocer los hechos, se puso en contacto con el proveedor para solicitarle explicaciones sobre lo ocurrido y la toma inmediata de medidas con el usuario implicado.

OCTOGÉSIMO SEGUNDO: Según ha manifestado ENDESA en su escrito de 11 de noviembre de 2022, éstos eran, para cada uno de los usuarios comprometidos, los datos relativos al alta y a la baja en la herramienta ***HERRAMIENTA.1**, así como el rol asignado a cada usuario y las funciones y permisos de acceso otorgados:

Usuario	Proveedor al que se le asignó el usuario	Fecha de petición de alta	Fecha de reseteo o deshabilitación	Fecha de retirada y eliminación en sistemas	Rol	Funciones y permisos otorgados
***USUARIO.1**	***EMPRESA.13**	11/03/2021	15/02/2022	24/08/2022	Usuario	Consulta
***USUARIO.9**	***EMPRESA.14**	09/12/2021	15/02/2022	24/08/2022	Usuario	Consulta
***USUARIO.11**	***EMPRESA.8**	26/11/2019	19/11/2021	19/11/2021	Usuario	Consulta
***USUA-RIO.10**	***EMPRESA.15**	21/12/2020	10/09/2021	24/08/2022	Usuario	Consulta
***USUA-RIO.10**	***EMPRESA.16 (***EMPRESA.12.).**	20/10/2020	03/09/2021	24/08/2022	Usuario	Consulta
***USUA-RIO.10**	***EMPRESA.15**	15/08/2021	29/11/2021	04/03/2022	Usuario	Consulta
***USUA-RIO.10**	***EMPRESA.16**	20/10/2020	21/09/2021	24/08/2022	Usuario	Consulta
***USUA-RIO.10**	***EMPRESA.17**	28/10/2020	24/08/2022	24/08/2022	Usuario	Consulta

Según consta en el Documento número 8 que acompaña el citado escrito, el usuario ***USUARIO.14** se expiró por caducidad el 04/03/2022.

OCTOGÉSIMO TERCERO: Según ha manifestado ENDESA en su escrito de 11 de noviembre de 2022, éstos eran, para cada uno de los usuarios comprometidos, los datos relativos al alta y a la baja en la herramienta ***HERRAMIENTA.2**, así como el rol asignado a cada usuario y las funciones y permisos de acceso otorgados:

Usuario	Proveedor al que se le asignó el usuario	Fecha de petición de alta	Fecha último acceso	Fecha de eliminación en sistemas	Rol	Funciones y permisos otorgados

***USUA-RIO.10	***EMPRESA.15	12/04/2021	09/09/2021	10/09/2021	***ROL.1	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
***USUA-RIO.10	***EMPRESA.16	19/02/2020	26/11/2021	12/01/2022	***ROL.3	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
***USUA-RIO.10	***EMPRESA.15	06/03/20	18/02/2022	16/03/2022	***ROL.1	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
***USUA-RIO.10	***EMPRESA.16	23/10/2020	25/11/2021	12/01/2022	***ROL.3	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).
***USUA-RIO.10	***EMPRESA.17	20/07/2020	3/12/2021	17/02/2022	***ROL.2	Consulta, creación y modificación de datos (dentro de su ámbito de negocio).

OCTOGÉSIMO CUARTO: Según ha manifestado ENDESA en su escrito de 11 de noviembre de 2022, *"los usuarios comprometidos tenían un rol de "usuario" en la herramienta* ******HERRAMIENTA.1****, con permiso asignado de consulta, por lo que únicamente podían visualizar (i) en relación con todos consumidores, clientes o no de Endesa Energía, datos técnicos – como potencia, tensión, consumos estimados – asociados al punto de suministro al introducir la dirección o el denominado Código Universal de Puntos de Suministro (en adelante "CUPS"); y (ii) en caso de que se tratara de clientes de Endesa Energía con un contrato en vigor, podían acceder a la siguiente información: nombre y apellidos del titular del punto de suministro, número de Documento Nacional de Identidad, número de contrato, CUPS, importe de facturación anual, indicador de deuda, información sobre precios, datos técnicos referentes al punto de suministro, datos de consumo y gráfica de utilización.*

El volumen aproximado de puntos de suministro que potencialmente se puede consultar – uno a uno, de manera individual – desde la herramienta ******HERRAMIENTA.1****, siempre y cuando se introduzca previamente un CUPS o una*

dirección, es de 30, 6 millones de puntos de suministro de electricidad y de 8,6 millones de puntos de suministro de gas. En el caso de clientes con un contrato en vigor, el volumen aproximado que un usuario puede consultar, bajo las mismas premisas indicadas anteriormente, es de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas.

En relación con la herramienta ******HERRAMIENTA.2****, los usuarios identificados comprometidos podían acceder a los datos relativos a clientes con un contrato en vigor con ENDESA, siendo el volumen aproximado durante el periodo comprendido entre el 1 de julio de 2021 y el 15 de octubre de 2021, de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas. En cuanto a la tipología de datos que podía visualizar, principalmente son: nombre y apellidos del titular del punto de suministro, dirección postal, número de Documento Nacional de Identidad, CUPS, teléfono, correo electrónico, productos contratados, facturas, número de cuenta bancaria, calidad del crédito, deudas con la compañía.*

En relación con los usuarios comprometidos y con el periodo en que la violación de la seguridad de los datos personales se desarrolló no se mantiene un registro (logs) del uso de las herramientas ******HERRAMIENTA.1*** *o* ******HERRAMIENTA.2****.*

Con motivo de la violación de la seguridad de los datos personales se adoptaron una serie de medidas entre las que se encuentra la ampliación de la trazabilidad (logs) de los accesos a ******HERRAMIENTA.1*** *para obtener información detallada del uso realizado por parte de los usuarios – medida que se implantó a finales del mes de diciembre de 2021"*.

OCTOGÉSIMO QUINTO: El 15 de noviembre de 2022, según consta en el Documento número 7 del escrito de ENDESA de 3 de julio de 2023 en respuesta al requerimiento de esta Agencia, se firmó un acuerdo de resolución de contrato entre ENDESA y ******EMPRESA.16***.

OCTOGÉSIMO SEXTO: Según ha manifestado ******EMPRESA.1*** en su escrito de 25 de noviembre de 2022:

- Usuarios de ******EMPRESA.1*** con acceso a ******HERRAMIENTA.4***: ******EMPRESA.1*** disponía de un único usuario de acceso (******USUARIO.11***) a la herramienta de ******HERRAMIENTA.4***.

- Usuarios de ******EMPRESA.1*** para realizar la carga masiva de solicitudes a través de la herramienta ******HERRAMIENTA.4***: ******EMPRESA.1*** disponía de un único usuario de acceso (******USUARIO.12***).

- Usuarios de ******EMPRESA.9*** autorizados para cargar solicitudes de venta en crm de ******EMPRESA.1***. Se aporta listado de todos los 46 usuarios relacionados a través de los cuales se han cargado las ventas fraudulentas.

OCTOGÉSIMO SÉPTIMO: Según ha manifestado ******EMPRESA.1*** en su escrito de 25 de noviembre de 2022:

- Cada usuario de ******EMPRESA.9*** disponía de un usuario independiente en el CRM de ******EMPRESA.1*** para realizar la carga de las solicitudes de contrataciones que hubieran formalizado a través de las llamadas de captación comercial realizadas. Una vez cargada esta información por parte de cada agente se generaba, en los sistemas de ******EMPRESA.1***, un Excel con los datos necesarios para que el Back Office de ENDESA pudiera gestionar los datos en los sistemas comerciales de ENDESA.
- Una vez realizado el procedimiento anterior, ******EMPRESA.1*** procedía, diariamente, a cargar masivamente vía ftp en la herramienta de ******HERRAMIENTA.4***, propiedad de ENDESA, toda la información. Para esta carga masiva, ******EMPRESA.1*** disponía sólo del usuario de acceso a ******HERRAMIENTA.4*** y al acceso vía ftp.
- Los subagentes (usuarios de ******EMPRESA.9***) solo podían acceder al CRM de ******EMPRESA.1***, sin que en ningún caso tuvieran acceso directo al CRM de Endesa.
- ******EMPRESA.1*** solo tenía un usuario de acceso a las siguientes herramientas de ENDESA:
  - ******HERRAMIENTA.4*** y al acceso vía FTP autorizado por ENDESA para realizar la carga masiva de las solicitudes de contratación.
  - ******PLATAFORMA.1***: Es la plataforma para la descarga de ficheros "no molestar" de ENDESA. Existía un único usuario con acceso a esta aplicación y se accedía a través de la web. ******EMPRESA.1*** solo tenía permisos en esta aplicación para realizar la descarga del fichero.
- No existe ninguna otra aplicación a la que tuvieran acceso ******EMPRESA.1*** y/o sus colaboradores en el marco de la relación contractual con ENDESA para la captación telefónica de clientes.
- Cada usuario de ******EMPRESA.9*** podía cargar en el CRM de ******EMPRESA.1*** exclusivamente las operaciones que ellos mismos habían realizado, pudiendo visualizar únicamente los estados de dichas operaciones hasta el cierre completo de la venta por parte de ENDESA. Solo tenían acceso a los datos personales que ellos mismos introducían en el CRM de ******EMPRESA.1***.
- No todos los clientes a quienes tenían acceso estos usuarios se vieron afectados por la práctica fraudulenta de ******EMPRESA.9***, ya que solo 137 operaciones fueron las afectadas cuya contratación fraudulenta se culminó.
- ******EMPRESA.1*** podía acceder con su usuario a ******HERRAMIENTA.4*** para visualizar el estado de cualquier contratación de cualquiera de sus Subagentes.

OCTOGÉSIMO NOVENO: El 3 de julio de 2023, en respuesta al requerimiento de esta Agencia, ENDESA aporta como Documento número 4 un documento denominado "Data Transfer Impact Assessment", en el que figura como persona jurídica exportadora ENDESA y como país importador ***PAÍS.2 y como persona jurídica importadora ******PLATAFORMA.1***, ******EMPRESA.15***, ******EMPRESA.16***.

En este documento se indica que ***PAÍS.2 tiene un "Data protection level" que es "3 – Parcialmente adecuado". Y que "*Este país garantiza un nivel de protección de datos parcialmente adecuado debido a la existencia de una normativa de protección de datos y de una autoridad de control independiente para la Comisarios de Protección de Datos y Privacidad*". Se acompañan los datos de domicilio y página web de la autoridad de protección de datos de ***PAÍS.2.

NONAGÉSIMO: El 3 de julio de 2023, en respuesta al requerimiento de esta Agencia, ENDESA aporta como Documento número 5 un documento denominado "Data Transfer Impact Assessment", en el que figura como persona jurídica exportadora ENDESA y como país importador ***PAÍS.1 y como persona jurídica importadora ***EMPRESA.11**.

En este documento se indica que ***PAÍS.2 tiene un "Data protection level" que es "3 – Parcialmente adecuado". Y que "*Este país garantiza un nivel de protección de datos parcialmente adecuado debido a la existencia de una normativa de protección de datos y de una autoridad de control independiente para la Comisarios de Protección de Datos y Privacidad*". Se acompañan los datos de domicilio y página web de la autoridad de protección de datos de ***PAÍS.1.

NONAGÉSIMO PRIMERO: El 3 de julio de 2023, en respuesta al requerimiento de esta Agencia, ENDESA aporta como Documento número 6 un documento denominado "DTIA- Riesgo país Análisis legislación y prácticas- ***PAÍS.2", en el que se indica que "*La información contenida en este informe debe ser considerada en la evaluación de impacto que se realice de cada transferencia internacional entre sociedades del grupo en la que *****EMPRESA.15** actúe como importador".*

Como conclusión, se indica: "*Se entiende que ***PAÍS.2 cuenta con un marco normativo que, si bien no puede considerarse como equivalente al establecido en la Unión Europea en lo que se refiere a la protección de los datos personales, sí que puede considerarse como razonablemente adecuado.*

Sin embargo, para alcanzar una conclusión definitiva sobre la idoneidad de la transferencia internacional, así como sobre la suscripción de medidas de garantía adicional para que el nivel de protección de los datos transferidos se ajuste a la norma de equivalencia esencial de la Unión Europea, es necesario tener en cuenta y evaluar el resto de los componentes, vinculados a las particularidades de cada una de las transferencias."

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones*

reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que ENDESA realiza, entre otros tratamientos, la recogida y conservación de los siguientes datos personales de personas físicas, tales como: nombre y apellido, documento de identidad, domicilio, número de teléfono, datos bancarios, datos de suministro, entre otros.

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

Por su parte, el artículo 4 apartado 12 del RGPD define, de un modo amplio, la "*violación de la seguridad de los datos personales*" como "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."*

En el presente caso, consta una violación de la seguridad de los datos personales en las circunstancias arriba indicadas, categorizada como de confidencialidad, al haberse producido un acceso indebido a datos personales tratados por ENDESA y de integridad, al haberse modificado ciertos datos para realizar altas fraudulentas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

Por último, las transferencias internacionales de datos personales se regulan en los artículos 44 y siguientes del RGPD.

III

Alegaciones aducidas

Alegaciones al acuerdo de inicio del procedimiento sancionador

En relación con las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por ENDESA:

Previa.- Concreción de determinados puntos fácticos esenciales para el análisis jurídico del expediente

Alega ENDESA la existencia, en el Acuerdo de Inicio, de algunas cuestiones que, siendo muy relevantes para el enjuiciamiento de la conducta de Endesa, no han sido interpretadas por la AEPD de manera correcta:

(a) Valor probatorio del informe de evaluación y gestión de brecha de seguridad elaborado por ******EMPRESA.1***:

Alega ENDESA que la AEPD fundamenta gran parte de su argumentación en el informe de evaluación y gestión de brecha de seguridad elaborado por ******EMPRESA.1*** el 4 de noviembre de 2021.

Y que: (i) ******EMPRESA.1*** nunca compartió dicho informe, ni las conclusiones del mismo, con Endesa (incluso cuando Endesa continuó solicitando información sobre el caso a ******EMPRESA.1***), aunque tenía obligación contractual y legal de poner en conocimiento de Endesa todos los detalles del incidente de los que tuviese constancia; y (ii) cuando ******EMPRESA.1*** facilitó el informe a la AEPD (noviembre de 2022), Endesa ya había resuelto el contrato de prestación de servicios al ***DEPARTAMENTO.6 de Endesa con este proveedor (enero de 2022), además, la relación entre dicho canal y ******EMPRESA.1*** no era “amistosa”.

Alega ENDESA que, desde la fecha de su elaboración (4 de noviembre de 2021), el mismo nunca fue actualizado por ******EMPRESA.1*** con la nueva información que se iba desprendiendo de las investigaciones de Endesa y que Endesa compartía con ******EMPRESA.1***, por lo que no refleja la realidad de las investigaciones de la violación de la seguridad de los datos ni sus consecuencias reales. Es por esta falta de rigor que Endesa también entiende que este informe debe ser excluido del elenco probatorio del Expediente y, por tanto, no debe tenerse en cuenta su contenido como base para la adopción de cualquier decisión en el marco del presente Expediente.

Remarca ENDESA que el informe aportado por ******EMPRESA.1*** debe ser considerado un informe parcial (en el sentido de informe de parte interesada), ya que ******EMPRESA.1*** estuvo implicada en el propio incidente y, de hecho, el mismo trajo causa, en parte, de su incumplimiento a la hora de controlar y supervisar el cumplimiento, por parte de ******EMPRESA.9,*** de las instrucciones de Endesa y de sus obligaciones como subencargado del tratamiento. Y que se aprecia claramente que es un informe “defensivo” confeccionado por una entidad que necesita proteger sus intereses frente a posibles reclamaciones de responsabilidad, al haber actuado como encargada del tratamiento de Endesa y poder tener algún grado de responsabilidad en el acaecimiento de los hechos que han dado lugar, en última instancia, al presente procedimiento.

Por lo tanto, entiende ENDESA que no se trata de un informe pericial ni jurídico imparcial del incidente elaborado por una parte externa sin implicación en el mismo y sin intereses en el resultado de este expediente sancionador del cual puedan sacarse conclusiones de cara a evaluar el cumplimiento de Endesa respecto de: (i) la obligación de notificar el incidente a la AEPD; y (ii) la aplicación de adecuadas medias de seguridad. Más bien al contrario, la finalidad de dicho informe es trasladar todo tipo de responsabilidad sobre el incidente a Endesa, tratando de hacer ver a esta Agencia que ******EMPRESA.1***, incluso cuando incumplió flagrantemente con sus obligaciones como encargado del tratamiento (no facilitó información adecuada a Endesa para asesorar el alcance y consecuencias del incidente, no implementó las medidas de seguridad ade-

cuadas al riesgo y no controló el cumplimiento, por parte de ***EMPRESA.9**, de sus obligaciones como subencargado), actuó siempre con la mayor diligencia y en estricto cumplimiento de la legalidad (*quad non*).

Al respecto, esta Agencia desea señalar que no es objeto del presente procedimiento la actuación por parte de ***EMPRESA.1**, si no la actuación de ENDESA en la violación de la seguridad de los datos personales notificada.

En este sentido, según consta en toda la documentación obrante en el expediente y tal como se detalla en los Antecedes, Hechos probados y Fundamentos de Derecho del presente documento, esta Agencia se basa no sólo en el informe realizado por ***EMPRESA.1** el 4 de noviembre de 2021, sino en toda la información de la que ha tenido conocimiento a largo del presente procedimiento.

Precisamente, por su posible implicación en la violación de la seguridad de los datos personales, esta Agencia requirió cierta información a ***EMPRESA.1**, en el marco de las actuaciones previas del presente procedimiento. Pero no es, ni mucho menos, la única información en la que se basa esta Agencia para proponer las correspondientes sanciones a ENDESA.

Por todo lo expuesto, se desestima la presente alegación.

(b) Interacciones con Facebook para solicitar la retirada de los anuncios a través de los cuales se ofrecía la venta/alquiler de credenciales de acceso a los sistemas de Endesa:

Alega ENDESA que, a lo largo del Acuerdo de Inicio, la AEPD le achaca una falta de diligencia a la hora de solicitar a Facebook la retirada de aquellos anuncios a través de los cuales se ofrecía la venta/alquiler de credenciales de acceso a sus sistemas puesto que: (i) no se dirigió a Facebook Ireland Limited para ello, tal y como Facebook Spain había propuesto en respuesta al primer burofax enviado por Endesa en fecha 4 de febrero de 2022; y (ii) no consiguió que Facebook retirase dichos anuncios y, por tanto, no implementó las medidas propuestas.

Indica ENDESA que yerra en esta interpretación el Acuerdo de Inicio puesto que:

(i) No es cierto que Endesa no remitiese una comunicación a Facebook Ireland Limited por falta de diligencia, sino porque conscientemente, y tras analizar las implicaciones de ello, decidió que hacerlo sería reconocer precisamente la jurisdicción irlandesa, lo que implicaría, en caso de ser necesario, tener que dirigir cualquier reclamación ante los tribunales irlandeses, lo que resultaba, y resulta, una carga inapropiada e injusta.

Este fue el motivo principal por el cual, en su lugar, Endesa decidió remitir un segundo burofax a Facebook Spain en fecha 28 de febrero de 20224 (que demuestra, a su entender, una gran diligencia por parte de Endesa) insistiendo en su requerimiento).

Manifiesta ENDESA que reconocer la jurisdicción irlandesa implicaría asumir que todos los incidentes que se produzcan en el marco de la plataforma gestionada por Facebook tendrían un carácter transfronterizo y, con ello, sería discutible cualquier actua-

ción (judicial o administrativa) que se iniciara contra Facebook si no es ante las autoridades irlandesas.

(ii) No es cierto que el hecho de que Facebook no retirase los anuncios a través de los cuales se ofrecía la venta/alquiler de credenciales de acceso a los sistemas de Endesa sea consecuencia de una falta de diligencia de la Sociedad ni implique, como indica el Acuerdo de Inicio, que las medidas de seguridad propuestas por Endesa al comienzo de la identificación de la violación de la seguridad de los datos no fuesen implementadas.

Indica ENDESA que: (a) Endesa remitió numerosos requerimientos y hasta dos burofaxes a Facebook Spain solicitando la retirada de los anuncios (no se le puede responsabilizar a Endesa de la no retirada de los anuncios puesto que Facebook es la única responsable de la gestión de la plataforma y sus publicaciones); y (b) Endesa sí implementó las medidas de seguridad propuestas desde el inicio de la brecha y adecuadas para mitigar las consecuencias de la Violación de la Seguridad de los Datos, puesto que, con anterioridad incluso al envío del primer burofax, ya había bloqueado los accesos de los usuarios comprometidos a las herramientas de Endesa, deshabilitando sus credenciales. Es decir, que dejaba de ser relevante la existencia de credenciales obsoletas en Facebook, que ya no representaban riesgo alguno para los derechos de los interesados.

Una vez deshabilitadas dichas credenciales y aunque los anuncios de Facebook se mantengan activos, se elimina el riesgo desde el punto de vista de protección de datos, puesto que desaparece la posibilidad de acceder a los datos responsabilidad de Endesa almacenados en sus herramientas (aunque las credenciales originales se vendan/alquilen). De manera adicional, puesto que Endesa procedió a implementar medidas de seguridad adicionales tales como la autenticación multifactor y la desactivación de la multisesión, se eliminó la posibilidad de que usuarios no identificados como comprometidos tuviesen acceso no autorizado a los sistemas de Endesa, independientemente de que se publicasen nuevos anuncios de Facebook o los anteriores permaneciesen publicados.

Sin perjuicio de lo anterior, explica ENDESA que, como el hecho de que los anuncios siguiesen activos en Facebook sí podía seguir implicando la comisión de una infracción o delito de revelación de secretos o de propiedad intelectual, Endesa decidió insistir con su pretensión ante Facebook, enviando un segundo burofax.

Por todo ello, destaca ENDESA que, a pesar de que algunos anuncios de Facebook se hubieran mantenido activos -por cuestiones, a su juicio, ajenas a Endesa-, las credenciales que se ofertaban a través de ese medio ya no permitían, de modo alguno, acceder a los sistemas ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** porque estaban deshabilitadas y que, como consecuencia de las nuevas medidas de seguridad implementadas por Endesa, ningún usuario adicional no autorizado conseguiría la finalidad de vender/alquilar credenciales de acceso a los sistemas de Endesa, puesto que dichas medidas se lo impedirían.

No obstante, desde ENDESA se ha encargado la elaboración, por parte de un tercero independiente, de un informe pericial que demuestre los anteriores aspectos y que pondrá a disposición de la AEPD una vez esté finalizado.

Este informe fue aportado durante el período de práctica de pruebas, mediante escrito de ENDESA de 23 junio de 2023, como Documento número 1.

Al respecto, esta Agencia desea señalar, en primer lugar, que ENDESA no puede cambiar la jurisdicción a su antojo, ni puede decidir quién es el responsable del tratamiento.

En el presente caso, tal y como indica Facebook Spain en su respuesta al burofax enviado por ENDESA, la empresa responsable del tratamiento de los datos personales a nivel europeo es Facebook Ireland Limited, una entidad constituida en Irlanda con domicilio social en Dublín. Según se informó a ENDESA, Facebook Spain no tiene capacidad alguna para decidir o tomar acción alguna en relación con lo solicitado por ENDESA, en su burofax de 7 de febrero de 2022. Por tanto, ENDESA debía comunicarse con Facebook Ireland Limited, a través de los medios facilitados por Facebook Spain (internet o postal).

La definición de «establecimiento principal» se recoge en el artículo 4.16 del RGPD. Respecto de los responsables del tratamiento el citado artículo indica, en su letra a), que el establecimiento principal es, “en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal” Por tanto, en este caso, el establecimiento principal de Facebook en la Unión es Facebook Ireland Limited, establecida en Irlanda.

Por supuesto que todos los incidentes que se producen en el marco de la plataforma gestionada por Facebook tienen carácter transfronterizo y, para su gestión, el RGPD ha habilitado un «mecanismo de ventanilla única» que permite a interesados en España presentar una reclamación por una cuestión que atañe a una empresa que tenga su establecimiento principal en otro Estado miembro como Irlanda, que será resuelta conjuntamente por la autoridad de control principal y las autoridades de control interesadas (entre ellas la autoridad de control receptora de la reclamación), a través del procedimiento previsto en el artículo 60 del RGPD.

Tanto es así, que esta Agencia recibe numerosas reclamaciones de interesados en España contra responsables con establecimiento principal en Irlanda, que efectúan un tratamiento de datos personales transfronterizo y cuya autoridad principal es la autoridad irlandesa de protección de datos. Todo ello en virtud de la normativa aplicable.

Por lo expuesto, esta Agencia se reitera en que no haber intentado siquiera una comunicación a través de la web con Facebook Ireland Limited para intentar que se retiraran los anuncios en cuestión, constituye una negligencia grave por parte de ENDESA.
En segundo lugar, esta Agencia considera que ENDESA no actuó con la debida diligencia a la hora de impedir el acceso a los sistemas por parte de los usuarios que ENDESA sabía habían sido comprometidos.

De acuerdo con los hechos probados de la propuesta de resolución:

- El 24 de agosto de 2021 la persona responsable del ***DEPARTAMENTO.1 de ENDESA envió un correo electrónico al responsable de Seguridad de la Información del Grupo Endesa, en el que se informaba de un anuncio sospechoso en Facebook, publicado por parte de "***B.B.B.***", en el que se ofertaba el acceso al ******PLATAFORMA.1***. Y este aviso fue el que inició el análisis e investigación de ENDESA de la cuestión objeto del presente procedimiento.

- El 1 de septiembre de 2021 ENDESA recibe un correo electrónico de ******EMPRESA.16***, confirmando que conocía la identidad de ***D.D.D.***, y se le facilita su nombre completo.

- El 3 de septiembre de 2021, se reseteó o deshabilitó en la plataforma ******HERRAMIENTA.1*** el usuario "******USUARIO.3***" asignado a ******EMPRESA.12***. Si bien no se eliminó este usuario en ******HERRAMIENTA.2*** hasta el 12/01/2022, siendo su último acceso a ******HERRAMIENTA.2*** el 26 de noviembre de 2021.

- El 10 de septiembre de 2021 ENDESA envió un correo electrónico a ******EMPRESA.15***, en el que se le decía que se trataba de "un empleado actualmente activo en ******EMPRESA.15***", solicitaba que se le desvinculara de sus operaciones y se indicaba que se procedería a "dar de baja el usuario con carácter inmediato".

Ese mismo día, se reseteó o deshabilitó en la plataforma ******HERRAMIENTA.1*** el usuario ******USUARIO.8***, asignado a ******EMPRESA.15***. Y se procedió a su retirada y eliminación de los sistemas de ******HERRAMIENTA.2***.

- El 21 de septiembre de 2021, ENDESA recibe un correo electrónico en el que se le confirma que ***C.C.C.*** *fue empleado de* ******EMPRESA.15*** *pero es baja de la compañía desde 2016.*

Ese mismo día, se reseteó o deshabilitó el usuario ******USUARIO.5***, de la plataforma ******HERRAMIENTA.1***, asignado a ******EMPRESA.12***. Si bien se eliminó el usuario en ******HERRAMIENTA.2*** el 12/01/2022, siendo el último acceso a ******HERRAMIENTA.2*** el 25/11/2021.

- El 27 de octubre de 2021, ******EMPRESA.1*** alertó a ENDESA mediante correo electrónico sobre el uso irregular que, algunos de sus asesores, habían realizado con ciertas credenciales de acceso a ******HERRAMIENTA.1***. En esta comunicación se identifican cinco usuarios de ******HERRAMIENTA.1*** comprometidos que fueron identificados, a su vez, por la empresa subcontratista
******EMPRESA.9***:

******USUARIO.13***
******USUARIO.14***
******USUARIO.15***

******USUARIO.16***
******USUARIO.9***

También en este correo se adjunta cuatro imágenes de anuncios de Facebook en los que se ofrecía el acceso a los sistemas de ENDESA.

Además de estos usuarios comprometidos identificados por ******EMPRESA.1***, ENDESA ha encontrado otros usuarios que también se habían visto comprometidos:

******USUARIO.1***
******USUARIO.2***
******USUARIO.10***

Respecto a los usuarios comprometidos, identificados por ******EMPRESA.1*** en su correo electrónico enviado a ENDESA el 27 de octubre de 2021:

- El usuario ******USUARIO.13,*** asignado a ******EMPRESA.12,*** ya había sido reseteado o deshabilitado en ******HERRAMIENTA.1*** el 3 de septiembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Pero recién fue eliminado del sistema ******HERRAMIENTA.2*** el 12 de enero de 2022, siendo su último acceso al sistema el 26 de noviembre de 2021.

  Es decir, que ******EMPRESA.1*** avisó a ENDESA que este usuario estaba comprometido el 27 de octubre de 2021, pero ENDESA ya había reseteado el usuario en ******HERRAMIENTA.1*** el 3 de septiembre, casi dos meses antes (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA ya conociera que ese usuario estaba comprometido, de hecho, dos días antes desde ******EMPRESA.16*** se había indicado que uno de los usuarios que publicaba los anuncios de Facebook había sido una agente de esta empresa).

  En cualquier caso, si el usuario en cuestión fue utilizado para realizar contrataciones fraudulentas, en octubre de 2021, esta Agencia considera que de poco había servido el reseteo de la contraseña en septiembre de 2021 y el riesgo para los derechos y libertades de los afectados permanecía activo. Por eso llama poderosamente la atención de esta Agencia que aun habiendo comunicado ******EMPRESA.1*** esta situación, ENDESA no hubiera realizado más acciones respecto de este usuario hasta el 24 de agosto de 2022, fecha en la que se eliminó el usuario de la plataforma ******HERRAMIENTA.1***.

  También llama la atención de esta Agencia que el usuario se hubiera reseteado en ******HERRAMIENTA.1*** el 3 de septiembre de 2021, pero recién el 12 de enero de 2022 fue eliminado de la plataforma ******HERRAMIENTA.2***, siendo su último acceso a la misma el 26 de noviembre de 2021. Es decir, que aun sabiendo que el usuario se había visto comprometido en ******HERRAMIENTA.1***, el usuario accedió libremente a ******HERRAMIENTA.2*** durante un mes más.

- El usuario ******USUARIO.15,*** asignado a ******EMPRESA.12,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 21 de septiembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Pero recién fue eliminado del sistema

***HERRAMIENTA.2** el 12 de enero de 2022, siendo su último acceso al sistema el 25 de noviembre de 2021.

Es decir, que ***EMPRESA.1** avisó a ENDESA que este usuario estaba comprometido el 27 de octubre de 2021, pero ENDESA ya había reseteado el usuario en ***HERRAMIENTA.1** el 21 de septiembre, más de un mes antes (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA ya conociera que ese usuario estaba comprometido, de hecho, ese mismo día se había indicado a ENDESA que uno de los usuarios que publicaba los anuncios de Facebook había sido un agente de ***EMPRESA.15**).

En cualquier caso, si el usuario en cuestión fue utilizado para realizar contrataciones fraudulentas en octubre de 2021, esta Agencia considera que de poco había servido el reseteo de la contraseña en septiembre de 2021 y el riesgo para los derechos y libertades de los afectados permanecía intacto. Por eso llama poderosamente la atención de esta Agencia que aun habiendo comunicado ***EMPRESA.1** esta situación, ENDESA no hubiera realizado más acciones respecto de este usuario hasta el 24 de agosto de 2022, fecha en la que se eliminó el usuario de la plataforma ***HERRAMIENTA.1**.

También llama la atención de esta Agencia que el usuario se hubiera reseteado en ***HERRAMIENTA.1** el 21 de septiembre de 2021, pero hasta el 12 de enero de 2022 no fue eliminado de la plataforma ***HERRAMIENTA.2**, siendo su último acceso a la misma el 25 de noviembre de 2021. Es decir, que aun sabiendo que el usuario se había visto comprometido en ***HERRAMIENTA.1**, el usuario accedió libremente a ***HERRAMIENTA.2** durante un mes más.

- El usuario ***USUARIO.14,** asignado ***a ***EMPRESA.15,*** fue reseteado o deshabilitado en ***HERRAMIENTA.1** el 29 de noviembre de 2021 y eliminado de los sistemas el 4 de marzo de 2022 (aunque no se deshabilitó al usuario por temas de seguridad sino porque el usuario caducó sin más). Y fue eliminado del sistema ***HERRAMIENTA.2** el 16 de marzo de 2022, siendo su último acceso al sistema el 18 de febrero de 2022.

  Es decir, que este usuario fue reseteado o deshabilitado en ***HERRAMIENTA.1** un mes más tarde de que ENDESA tuviera conocimiento por parte de ***EMPRESA.1** de que este usuario se había visto comprometido. Y aun sabiendo que el usuario se había visto comprometido en ***HERRAMIENTA.1**, el usuario accedió libremente a ***HERRAMIENTA.2** durante casi tres meses más.

  - El usuario ***USUARIO.9,** asignado a ***EMPRESA.6** fue reseteado o deshabilitado en ***HERRAMIENTA.1** el 15 de febrero de 2022 y eliminado de los sistemas el 24 de agosto de 2022.

  Es decir, que se reseteó este usuario cuatro meses después de que ***EMPRESA.1** le hubiera comunicado a ENDESA que se había visto comprometido. Y es que, además, ni siquiera se había deshabilitado con anterioridad a que se enviara el primer burofax a Facebook el 8 de febrero de

2022, tal y como afirma ENDESA en su escrito de alegaciones al acuerdo de inicio, por lo que los riesgos para los derechos y libertades de los interesados permanecían intactos.

- El usuario ******USUARIO.16***, asignado a ******EMPRESA.5*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** y eliminado de sus sistemas el 24 de agosto de 2022. No obstante, había sido eliminado del sistema ******HERRAMIENTA.2*** el 17 de febrero de 2022, siendo su último acceso al sistema el 3 de diciembre de 2021.

  Es decir, que cuatro meses después de que ******EMPRESA.1*** hubiera comunicado a ENDESA que este usuario se había visto comprometido, se eliminó de los sistemas de ******HERRAMIENTA.2***, lo cual permitió que durante mes y medio este usuario hubiera accedido libremente a tal plataforma. Si bien, cabe destacar que todo ello tampoco fue antes de que se enviara el primer burofax a Facebook Spain el 8 de febrero de 2022, tal y como afirma ENDESA en sus alegaciones al acuerdo de inicio. Además, por motivos que se desconocen, no fue reseteado de ******HERRAMIENTA.1*** hasta el 24 de agosto de 2022, más de 10 meses después de que ******EMPRESA.1*** le comunicara a ENDESA tal situación.

Respecto al resto de usuarios, se desconoce la fecha en que ENDESA supo que tales usuarios se habían visto comprometidos, pero se puede señalar lo siguiente:

- El usuario ******USUARIO.10,*** asignado ***a ***EMPRESA.15,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 10 de septiembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Y fue eliminado del sistema ******HERRAMIENTA.2*** el 10 de septiembre de 2021, siendo su último acceso al sistema el 9 de septiembre de 2021.

  Es decir, ENDESA reseteó el usuario en ******HERRAMIENTA.1 y ***HERRAMIENTA.2*** el 10 de septiembre de 2021 (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA tuviera conocimiento de que ese usuario estaba comprometido, ya que ese mismo día ENDESA envió un correo electrónico haciendo referencia a un empleado activo en ******EMPRESA.15***, cuyo usuario se iba a dar de baja con carácter inmediato).

- El usuario ******USUARIO.2 (***USUARIO.2)***, asignado a ******EMPRESA.8.,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** y eliminado de sus sistemas el 19 de noviembre de 2021.

- El usuario ******USUARIO.1,*** asignado a ******EMPRESA.13.,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 15 de febrero de 2022 y eliminado de los sistemas el 24 de agosto de 2022. Es decir, no fue reseteado antes del envío del primer burofax a Facebook el 8 de febrero de 2022, tal y como afirma ENDESA en sus alegaciones al acuerdo de inicio.

Por todo lo expuesto, esta Agencia no puede menos que disentir respecto de la afirmación de ENDESA de que había implementado las medidas de seguridad propuestas

desde el inicio de la violación de la seguridad de los datos personales y adecuadas para mitigar las consecuencias de la violación de la seguridad de los datos, puesto que no es cierto que se hubieran bloqueados los accesos de los usuarios comprometidos a las herramientas de ENDESA de forma diligente, deshabilitando sus credenciales, ni mucho menos que esto hubiera tenido lugar antes de que se hubiera enviado el primer burofax a Facebook.

En cuanto a que Endesa procedió a implementar medidas de seguridad adicionales tales como la autenticación multifactor y la desactivación de la multisesión, que eliminó la posibilidad de que usuarios no identificados como comprometidos tuviesen acceso no autorizado a los sistemas de Endesa, independientemente de que se publicasen nuevos anuncios de Facebook o los anteriores permaneciese publicados, esta Agencia se reitera en que tales medidas debieron ser adoptadas por ENDESA con anterioridad, toda vez que el riesgo de que se vieran comprometidos los usuarios que permitían el acceso a ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***, era bastante probable, en especial al no existir una autenticación multifactor y al permitirse que existieran varias sesiones abiertas en simultáneo, lo que posibilitó el descontrol de los accesos a los sistemas de ENDESA, lo cual sumado a la imposibilidad de realizar una trazabilidad en condiciones de los logs de estos sistemas resultó ser un caldo de cultivo ideal para que se produjera una situación como la del objeto del presente procedimiento, en la que ni siquiera se puede comprobar el número de accesos indebidos a estos sistemas al carecer de una trazabilidad que lo permitiera.

Por último, dado que ENDESA hizo referencia a un informe pericial por parte de un tercero independiente, que demuestra lo alegado, esta Agencia procedió a requerirle que presentara el citado informe en el período de prueba del presente procedimiento.

En este informe, de fecha 23 de junio de 2023, el equipo pericial realiza una cronología de hechos que se consideran relevantes, en la que indica (página 4) que del "*3 de septiembre de 2021 al 18 de febrero de 2022*" "*se deshabilitan las credenciales comprometidas en FB detectadas durante ese periodo*". Al respecto, esta Agencia desea señalar, en primer lugar, que ENDESA había enviado el burofax a Facebook Spain el 7 de febrero de 2022. Y que el 15 de febrero de 2022 se resetearon dos usuarios de la plataforma ******HERRAMIENTA.1*** (******USUARIO.1 y ***USUARIO.9)*** y (…) se eliminó un usuario de la plataforma ******HERRAMIENTA.2*** (******USUARIO.6***), por lo que tales usuarios no se resetearon o eliminaron antes de enviar el citado burofax, tal y como había afirmado ENDESA.

En segundo lugar, esta afirmación que se realiza en el informe pericial no es del todo correcta. Tal y como ha quedado acreditado en los hechos probados del presente procedimiento, de los usuarios comprometidos que había comunicado ******EMPRESA.1*** a ENDESA en su correo electrónico de 27 de octubre de 2021, el usuario ******USUARIO.3*** fue eliminado en agosto de 2022 (si bien había sido reseteado en septiembre de 2021, un mes antes de que ******EMPRESA.1*** avisara que era uno de los usuarios que se habían vulnerado, por lo que una vez ese usuario estuvo comprometido, no se eliminó su acceso a ******HERRAMIENTA.1*** hasta agosto 2022) y el usuario ******USUARIO.6*** fue reseteado y eliminado de ******HERRAMIENTA.1*** en agosto de 2022. Mientras que en la plataforma ******HERRAMIENTA.2*** dos usuarios se eliminaron en enero 2022 (******USUARIO.3*** y ******USUARIO.5***, uno el 17 de febrero de 2022 (******USUARIO.6***) y otro el 16 de marzo de 2022 (******USUARIO.4***). Es decir, que con posterioridad a la fecha indicada en

el informe pericial se han deshabilitado las credenciales comprometidas durante ese período.

En cualquier caso, el mero hecho de que ENDESA necesitara CINCO MESES (que es el periodo citado en el informe pericial) para resetear o eliminar unas credenciales de acceso a sus sistemas en los que constaban los datos personales de tantos clientes y no clientes, después de que su propio proveedor le informara de los usuarios comprometidos (y hasta su contraseña de acceso) evidencia por sí misma, en opinión de esta Agencia, la escandalosa falta de diligencia de la empresa a la hora de gestionar los permisos otorgados a sus proveedores y subcontratistas para el acceso a los citados datos y controlar los citados accesos y el debido uso que se hacía de esos datos.

Por todo lo expuesto, se desestima la presente alegación.

Primera.- De la improcedencia de la sanción impuesta por presunta infracción de los artículos 5.1. f) y 32 del RGPD

1. De la implementación de medidas de seguridad adecuadas al riesgo

(a) La AEPD entiende que Endesa debería haber tenido implementadas, desde un principio, las medidas de seguridad que comenzó a aplicar una vez tuvo constancia del incidente:

Cita ENDESA la Sentencia número 188/2022 del Tribunal Supremo, de 15 de febrero (ECLI:ES:TS:2022:543), que indica que la obligación de implementación de medidas de seguridad impuesta por la normativa de protección de datos tiene una naturaleza de obligación de medios y no de resultado.

Y explica ENDESA que la AEPD, a la hora de valorar el cumplimiento o incumplimiento de la obligación de implementación de medidas de seguridad por parte de Endesa, deberá analizar, únicamente, si Endesa contaba, con anterioridad al incidente, con medidas que "*conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado*" (transcripción literal de la Sentencia antes citada).

Alega ENDESA que esto no ha sido así. Y ello debido a que la AEPD no ha tenido en cuenta, en dicho acuerdo, varias de las pruebas aportadas por Endesa para justificar que las medidas de seguridad implementadas en el momento en el que se publicaron los primeros anuncios de Facebook y se produjeron las primeras contrataciones fraudulentas eran conformes con el estado de la tecnología teniendo en cuenta la naturaleza del tratamiento y de los datos tratados tal y como se desprende, entre otros: (i) del *Business Impact Analysis* y del *Risk Assessment* elaborados por Endesa respecto de las herramientas ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** y facilitados a la AEPD en el marco del Expediente; (ii) del hecho de que, en el mes de mayo de 2021, se realizase un ejercicio de *hacking* ético para detectar posibles vulnerabilidades de las herramientas ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** y se subsanasen aquellas identificadas; y (iii) del cumplimiento, por parte de ambas herramientas, de la política de gestión de acceso lógico a sistema IT.

Indica ENDESA que es en ese momento, con anterioridad a la materialización de la brecha, cuando se debe evaluar el nivel de seguridad de las medidas implementadas conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, puesto que su evaluación con posterioridad, una vez la brecha ha tenido lugar, desvirtuaría por completo la obligación de implantación de medidas de seguridad como obligación de medios y no de resultado. Achacar, a posteriori y una vez conocidas las consecuencias de la brecha, la falta de implementación de las concretas medidas que, una vez conocidas las circunstancias del caso, hubiesen evitado el incidente, convierte a la obligación contenida en el artículo 32 del RGPD en una obligación de resultado, contraviniendo lo establecido por el Tribunal Supremo.

Alega ENDESA que esto es lo que hace la AEPD en su Acuerdo de Inicio, cuando se limita a indicar que Endesa debería haber implementado las medidas de seguridad que, una vez materializado el incidente, decidió implementar para mejorar la seguridad de las herramientas (convirtiendo a la obligación del artículo 32 del RGPD en una obligación de resultado).

Al respecto, esta Agencia desea señalar que de ninguna manera considera que la obligación de implementación de medidas de seguridad impuesta por la normativa de protección de datos tenga una naturaleza de obligación de resultado y no de medios.

Pero no es menos cierto que ENDESA no contaba, antes de que se produjera el incidente, con medidas que "*conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado*".

No puede entenderse que no fuera conforme al estado de la tecnología ni del tratamiento de datos personales en cuestión que una empresa grande como podría ser ENDESA, con un volumen de negocio de miles de millones de euros y que trata continuamente datos de millones de personas, no hubiera considerado razonable implementar, como mínimo, por ejemplo, como así hizo después un sistema de autenticación de usuarios multifactor, ni que se impidiera que un usuario pudiera tener varias sesiones iniciadas a la vez, ni desactivar o resetear de forma inmediata (sin tardar meses) los usuarios que contaran con la menor sospecha de estar comprometidos, ni contara con un sistema que permitiera la trazabilidad de la actividad realizada por los citados usuarios, entre otras medidas posibles.

En cuanto a los documentos Business Impact Analysis de la aplicación ******HERRAMIENTA.2*** y ******HERRAMIENTA.1***, en la pestaña "Impact-CheckList" se le asigna un valor 4 (Impacto medio-alto) a la posibilidad de que la pérdida de confidencialidad e integridad de los datos personales pudiera resultar en multas de millones de euros, pero no se dice nada sobre posibles medidas para evitar que los usuarios de estas aplicaciones se vieran comprometidos.

En cuanto al documento "Assurance check report", con el reporte de los resultados obtenidos en el Hacking Ético para detectar posibles vulnerabilidades en la aplicación ******HERRAMIENTA.2***, tampoco se hace referencia alguna a la posibilidad de que hubiese usuarios comprometidos ni a las posibles medidas a implementar para evitar o

solucionar tal situación. Se han analizado otra serie de cuestiones, pero ninguna relativa a esta cuestión que dio origen al presente procedimiento. Además, el último Hacking Ético realizado en la aplicación data de mayo de 2021, anterior por tanto a los hechos que son objeto del presente procedimiento que ponen de manifiesto posibles vulnerabilidades. Por tanto, no puede sostenerse que fuera una medida preventiva adecuada cuando no se repitió ningún evento similar tras la publicación de los anuncios en Facebook.
Por tanto, se desestima la presente alegación.

(b) La AEPD entiende que transcurrieron varios meses desde que Endesa identificó las posibles mejoras que podía implementar respecto de las medidas de seguridad de las herramientas ******HERRAMIENTA.1 y ***HERRAMIENTA.2*** y las implementó:

Alega ENDESA que la implementación de medidas de seguridad adicionales en los sistemas no es una tarea sencilla, y que esta suele tener sus tiempos determinados y marcados, puesto que: (i) el desarrollo de nuevas funcionalidades o medidas suele tener una valoración en horas que no puede acortarse; y (ii) la implantación de nuevas medidas no suele depender solo de Endesa, sino también de sus proveedores de infraestructuras o software.

En este sentido, respecto de ******HERRAMIENTA.1***, ENDESA destaca que los proyectos de implementación de las posibles mejoras que se identificaron sumaban una valoración en horas de 1.055, por lo que es normal que la duración total de implementación durase 3 meses, a pesar de que se le diera la máxima prioridad (se adjunta, como **Documento número 1**, la explicación detallada de cada uno de los desarrollos, así como de su valoración horaria).

Explica ENDESA que, ******HERRAMIENTA.2*** está desarrollado sobre el CRM de ******PLATAFORMA.1***. ******PLATAFORMA.1*** es un SaaS (*Software as a Service*) sobre el que Endesa puede desarrollar múltiples funcionalidades, como es la desactivación del login múltiple que decidió implementar tras conocer los detalles del incidente. Esto no significa, sin embargo, que Endesa pudo desactivar dicha funcionalidad de manera inmediata, sino que fue necesario llevar a cabo un desarrollo de software específico para ello, que implicaba: (i) inventariar usuarios técnicos de integración; (ii) inventariar procesos batch y usuarios de ejecución; y (iii) analizar los casos de uso que se le pueden dar a un agente. A su vez, todo este desarrollo implica la superación de varias fases que no puede realizarse en menos de 3 meses (se adjunta, como **Documento número 2**, la explicación detallada de cada uno de los desarrollos y tareas necesarias para la implementación de esta medida de seguridad).

Alega ENDESA que el tiempo transcurrido desde que se identificaron las posibles mejoras de seguridad hasta que se implementaron las mismas no se debe a la falta de diligencia de Endesa en su desarrollo (a estos desarrollos se les dio máxima prioridad), sino al hecho de que este es el tiempo habitual y razonablemente esperado para la implementación de este tipo de mejoras.

Adicionalmente, considera ENDESA que demuestra una gran diligencia por su parte el hecho de que, pese a que la implementación efectiva de las medidas requiriese tiempo, estas ya se habían identificado con detalle y propuesto en el Comité de Endesa de

fecha 13 de septiembre de 2021, momento en el cual el incidente todavía no tenía la consideración de Violación de la Seguridad de los Datos Notificable.

Al respecto, esta Agencia reconoce que los desarrollos implementados llevan su tiempo y que un plazo de tres meses puede ser un plazo razonable para ello (si bien, no es menos cierto que según se indica en el informe pericial presentado el 3 de julio de 2023, se completó el despliegue de la autenticación multifactor de usuarios, tanto en ******HERRAMIENTA.1*** como en ******HERRAMIENTA.2***, el 23 de marzo de 2022, es decir, seis meses después de que se hubiera identificado tal medida en el informe del Comité de septiembre de 2021, el doble de tiempo de lo que se estima).

No obstante, el comportamiento gravemente negligente de ENDESA en la supuesta infracción del artículo 32 del RGPD se aprecia en todo su comportamiento antes y después de producido el incidente, toda vez que ni siquiera se había previsto siquiera la posibilidad de que se hiciera un uso indebido de los usuarios de ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***, por lo que no se habían implementado unas medidas adecuadas para asegurar una autenticación de usuarios con las debidas garantías, impidiendo que se produjesen accesos indebidos a los sistemas y posibilitando que se rastree debidamente la actividad de estos usuarios en esos sistemas.

Tampoco se resetearon ni se eliminaron de forma inmediata, ni de ******HERRAMIENTA.1*** ni de ******HERRAMIENTA.2***, los usuarios que se sabía comprometidos, y eso que para eliminarlos no hace falta implantar ningún desarrollo adicional, se tardaron meses, lo que propició que durante todo ese tiempo se pudiera acceder indebidamente a los datos personales titularidad de ENDESA y facilitó que se realizara un gran número de altas fraudulenta. Tampoco se realizó un reseteo preventivo de todos los usuarios de los sistemas, ante una posible amenaza (que luego resultó ser cierta).

En otro orden de cosas, pese a lo indicado por FB SPAIN, ENDESA no se dirigió a FACEBOOK IRELAND LIMITED por ninguno de los medios ofrecidos para que eliminara los anuncios publicados en los que se ofertaban los accesos a sus sistemas.

Por todo lo expuesto, esta Agencia considera que la actuación de ENDESA ha sido gravemente negligente, por lo que se desestima la presente alegación.

(c) La AEPD, tomando (a su juicio) como base el informe elaborado por ******EMPRESA.1,*** entiende que Endesa podía haber implementado medidas de seguridad adicionales sobre las herramientas ******HERRAMIENTA.1 y ***HERRAMIENTA.2***:

Alega ENDESA que la AEPD ha basado la gran mayoría de sus argumentos sobre la falta de medidas de seguridad implementadas por Endesa en las conclusiones y afirmaciones contenidas en el informe aportado por ******EMPRESA.1***, el cual, reitera, no debería ser tenido en cuenta a estos efectos.

Al respecto, esta Agencia se reitera en que no es objeto del presente procedimiento la actuación por parte de ******EMPRESA.1***, si no la actuación de ENDESA en la violación de la seguridad de los datos personales notificada.

Y que, según consta en toda la documentación obrante en el expediente y tal como se detalla en los Antecedes, Hechos probados y Fundamentos de Derecho del presente

documento, esta Agencia se basa no sólo en el informe realizado por ***EMPRESA.1***, sino en toda la información de la que ha tenido conocimiento a largo del presente procedimiento.

Y que, precisamente, por su posible implicación en la violación de la seguridad de los datos personales, esta Agencia requirió cierta información a ***EMPRESA.1***, en el marco de las actuaciones previas del presente procedimiento. Pero no es, ni mucho menos, la única información en la que se basa esta Agencia para proponer las correspondientes sanciones a ENDESA.

Es más, las medidas a las que hace referencia esta Agencia y que debía tener implementadas ENDESA son, precisamente, las medidas que se implementaron con posterioridad al incidente en cuestión.

Por todo lo expuesto, se desestima la presente alegación.

(d) La AEPD entiende que Endesa no fue diligente a la hora de ponerse en contacto con Facebook para la retirada de los anuncios puesto que, tras recibir la contestación en la que se le indicaba que Facebook Spain no era la entidad competente, no remitió a Facebook Ireland Limited requerimiento alguno en este sentido y, por tanto, no implementó las medidas de seguridad propuestas:

Se reitera ENDESA en que el Acuerdo de Inicio yerra a la hora de alcanzar esta conclusión puesto que: (i) la decisión de no ponerse en contacto con Facebook Ireland Limited se tomó, por parte de Endesa, conscientemente para no reconocer expresamente la jurisdicción irlandesa (no por falta de diligencia); y (ii) sí se implementaron las medidas de seguridad propuestas al proceder Endesa, con gran diligencia e incluso con anterioridad al envío del primer burofax a Facebook Spain, a deshabilitar las credenciales de los usuarios comprometidos de manera que, aunque los anuncios siguiesen activos en Facebook, los usuarios vendidos/alquilados ya no podrían acceder a los sistemas de Endesa.

Al respecto, esta Agencia se reitera en lo respondido en el apartado b) de la alegación previa del documento de alegaciones al acuerdo de inicio del presente procedimiento, por lo que se desestima la presente alegación.

(e) La AEPD entiende que Endesa tardó varios meses en eliminar las cuentas de los usuarios comprometidos de los sistemas de la Sociedad:

Alega ENDESA que, en el Acuerdo de Inicio, se achaca a Endesa que, para cada uno de los usuarios comprometidos, tardara varios meses en eliminar sus cuentas de los sistemas de la Sociedad.

En este sentido ENDESA aclara que, una vez deshabilitada o reseteada la cuenta de cada usuario, éste no puede acceder a la misma ni utilizarla para ninguna finalidad, quedando expulsado permanentemente del sistema.

El hecho, por tanto, de que la cuenta no se haya eliminado por completo de los sistemas de ENDESA obedece a la finalidad de evitar registros huérfanos y la pérdida de

información comercial crítica, sin que esto signifique que el usuario pueda volver a acceder a la misma como parece desprenderse del Acuerdo de Inicio.

Así lo indica el propio ***PLATAFORMA.1** en su manual de ayuda, en el cual se indica que: "*La eliminación de un usuario de **PLATAFORMA.1 afecta muchos procesos en la organización. Después de la salida de la organización, obviamente no desea que el usuario conserve el acceso a su cuenta. Sin embargo, la simple eliminación de un usuario puede dar como resultado registros huérfanos y la pérdida de información comercial crítica. Por estos motivos, desactivar en lugar de eliminar al usuario es la acción adecuada a realizar. La desactivación elimina el acceso de inicio de sesión del usuario, pero conserva toda la actividad y los registros históricos, lo que facilita la transferencia de propiedad a otros usuarios.*"

Es decir, explica ENDESA que, por las razones expuestas, el hecho de que transcurriera un periodo de tiempo hasta el borrado completo de las credenciales desde que se hubieran deshabilitado, no quiere decir, en ningún caso, que se pudiera seguir accediendo con estos usuarios a los sistemas ***HERRAMIENTA.1** y ***HERRAMIENTA.2**. Tampoco quiere decir otros usuarios no identificados como comprometidos pudiesen acceder a los sistemas, puesto que ENDESA procedió a implementar las medidas de autenticación multifactor así como a la desactivación de la multisesión. Todo ello hacía inviable cualquier acceso no autorizado, independientemente de que los anuncios de Facebook siguieran publicados.

Al respecto, esta Agencia por supuesto que entiende que, una vez deshabilitada o reseteada la cuenta de cada usuario, éste no puede acceder a la misma ni utilizarla para ninguna finalidad.

Pero lo que se achaca a ENDESA es que se demoró meses en deshabilitar o resetear los usuarios comprometidos, tal y como se ha explicado ampliamente en la respuesta al punto b) de la alegación previa del documento de alegaciones al acuerdo de inicio del presente procedimiento.

También desea esta Agencia destacar que se proporcionó, respecto de ***HERRAMIENTA.1**, las fechas de deshabilitación/reseteo de usuarios y de eliminación de usuarios por separado, pero que, respecto de ***HERRAMIENTA.2**, únicamente se proporcionó la fecha de eliminación de usuarios, por lo que no consta acreditado que existió reseteo o deshabilitación alguna.

En cualquier caso, y tal como ha quedado acreditado a lo largo del procedimiento, ENDESA demoró meses en deshabilitar o eliminar los usuarios comprometidos, lo que permitió que se pudiera acceder a sus sistemas durante meses, facilitando que se realizaran altas fraudulentas.

Por lo expuesto, se desestima la presente alegación.

2. De la concurrencia de infracciones

Indica ENDESA que el Acuerdo de Inicio incluye una primera propuesta de sanción por incumplimiento del artículo 5.1.f del RGPD puesto que "*se considera que ENDESA no garantizó debidamente la confidencialidad e integridad de los datos personales de su*

titularidad" y una segunda propuesta de sanción por incumplimiento del artículo 32 del RGPD porque *"se considera que ENDESA no aplicó las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de que una brecha como la que tuvo lugar se produjera*".

Alega ENDESA que, unos mismos hechos darían lugar, de mantenerse el criterio de la AEPD en dicho Acuerdo de Inicio, a la imposición de dos sanciones por infracción de dos preceptos diferentes, el artículo 5.1.f) y el artículo 32, ambos del RGPD.

Y que esta duplicidad de sanciones constituye un supuesto de concurrencia de normas punitivas en el ámbito administrativo, en concreto en lo que la doctrina denomina "concurso de normas administrativas sancionadoras". Los distintos tipos de concurso de infracciones y normas, cuya delimitación exacta presenta cierta complejidad, están vinculados a la institución del "*non bis in idem*". Se trata de principios propios del ámbito penal (p.ej. artículo 8 del Código Penal) y aplican también a la potestad sancionadora de la administración en su faceta material y al procedimiento administrativo sancionador en su vertiente procesal, inicialmente por aplicación jurisprudencial y, más adelante, por inclusión expresa en algunas de sus representaciones en el derecho positivo (p.ej. en el artículo 29.5 de la Ley 40/2015, de Régimen Jurídico del Sector Público -en adelante LRJSP-).

Indica ENDESA que el propio RGPD recoge una regulación específica de la concurrencia de infracciones en el artículo 83.3.

Explica ENDESA que el concurso de normas administrativas sancionadoras se produce cuando un sujeto, con un único hecho o conjunto de hechos y una sola lesión a un mismo bien jurídico, realiza el tipo castigado en ambas. Según la doctrina y la jurisprudencia, para que exista el concurso de infracciones debe darse una triple identidad: (i) de sujeto; (ii) de objeto; y (iii) de razón o fundamento. En el presente caso considera ENDESA que se está ante unos únicos hechos, que son considerados por la AEPD como una falta de medidas de seguridad apropiadas para proteger los datos personales de los que era responsable Endesa. Y que, incluso si se aceptara a los meros efectos dialécticos que tal consideración fuera cierta, el Acuerdo de Inicio identifica que tales hechos infringen dos preceptos diferentes, uno que contiene un principio general (principio de integridad y confidencialidad) y otro que contiene un mandato específico (medidas de seguridad adecuadas).

Resalta ENDESA no solo en la duplicidad de posibles infracciones, sino además en la extrema identidad del bien jurídico protegido en ambos preceptos. Así, mientras el artículo 5.1.f) se refiere a la obligación de garantizar una "seguridad adecuada" de los datos personales mediante la aplicación de "medidas técnicas u organizativas apropiadas", el artículo 32 es la concreción de aquel principio cuando obliga al responsable a aplicar "medidas técnicas y organizativas apropiadas" para garantizar "un nivel de seguridad adecuado".

Entiende ENDESA que las obligaciones son equivalentes, incluso adjetivadas con exactamente los mismos conceptos jurídicos indeterminados (seguridad adecuada y medidas apropiadas). Y que cabe concluir, incluso, con la afirmación de que se está ante dos preceptos equivalentes, uno con un enfoque general y otro con un contenido más específico, por lo que no podría sancionarse un mismo hecho dos veces, vulne-

rando el principio constitucional de "*non bis in idem*". La consecuencia sería la imposibilidad de sancionar unos mismos hechos por la infracción del artículo 5.1.f) y el artículo 32 del RGPD.

Explica ENDESA que, aunque el "*non bis in idem*" no aparece recogido de forma expresa en la Constitución Española, el Tribunal Constitucional ha declarado reiteradamente que debe entenderse implícito en el artículo 25.1 de la CE, por su estrecha vinculación con el principio de legalidad punitiva (por todas, Sentencia 2/1981, de 30 de enero). A diferencia de lo dispuesto en los Convenios Internacionales de derechos fundamentales, tales como la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 50.

En todo caso, incluso si no se acepta la aplicación íntegra del "*non bis in idem*" por entender que no es el mismo precepto el vulnerado (lo cual formalmente es así), entiende de ENDESA que lo que sin duda concurre en el presente caso es un concurso de normas punitivas en la que se da la triple identidad de sujeto (el actor, Endesa), objeto (la argumentada insuficiencia de medidas de seguridad apropiadas) y razón o fundamentación jurídica (la finalidad de garantizar un nivel de seguridad adecuado).

Cuando concurren dos normas punitivas, señala ENDESA que el "*non bis in idem*" material impide sancionar dos veces por los mismos hechos, si bien no está regulado cuál es la que se debería aplicar. Existen distintos criterios en la jurisprudencia para estos casos: (i) la aplicación de la norma especial sobre la norma general; (ii) la aplicación de la norma sancionadora más grave, acogiendo el criterio del artículo 8 del Código Penal; o (iii) en algún caso, los tribunales han optado por dar prevalencia a la sanción administrativa que primero se imponga, independientemente de la especialidad, criterio que no resulta aplicable al caso que nos ocupa.

En opinión de ENDESA general y, en este sentido, debería imponerse únicamente la sanción relativa al supuesto incumplimiento del artículo 32 del RGPD y no la correspondiente al supuesto incumplimiento del principio general del artículo 5.1.f) del RGPD.

Todo ello, para el hipotético caso en que la AEPD considere que sí existió infracción de tal artículo y no tenga en cuenta lo alegado anteriormente sobre la suficiencia de las medidas de seguridad.

Entiende ENDESA que este es el criterio que resulta también de la aplicación de la metodología establecida en las Directrices 4/2022 del Comité Europeo de Protección de Datos ("**CEPD**") sobre el cálculo de multas administrativas bajo el RGPD9. El CEPD señala que pueden darse distintas situaciones de concurrencia de infracciones y/o sanciones, y que es preciso realizar un análisis caso a caso. Siguiendo la metodología de las Directrices citadas, los pasos a seguir serían los siguientes (Capítulo 3):

- En primer lugar, debe analizarse si estamos ante un único hecho (relacionado con una única actividad del tratamiento o vinculadas). El criterio debe basarse en una conducta realizada por un mismo sujeto, de forma unificada (aunque tenga distintas fases), cercana en el espacio y en el tiempo de forma que un observador externo pueda considerar como una única actividad. En el presente caso entiende ENDESA que debe considerarse que estamos ante una única conducta.

- En segundo lugar, es preciso determinar si esa conducta es sancionable por dos preceptos diferentes. En el presente caso entiende ENDESA que la respuesta es afirmativa (posibles infracciones de los artículos 5.1.f) y 32 del RGPD).

- En tercer lugar, es preciso determinar cuál de las normas debe prevalecer. Explica ENDESA que, tal como cita el propio CEPD en sus Directrices, la jurisprudencia comunitaria ha optado en ocasiones por el principio de especialidad (caso C-10/18 Marine Harvest). Para la aplicación del principio de especialidad debe darse una congruencia en los objetivos perseguidos por las dos normas aplicables, como es el caso que nos ocupa. La consecuencia sería la aplicación únicamente de la norma especial, excluyendo la aplicación de la norma general.

Siguiendo con el proceso de elección de la norma a aplicar, y para el caso en que no se tuviera en cuenta el principio de especialidad, el siguiente criterio que emplea el CEPD, aunque en opinión de ENDESA no sería tan adecuado como el criterio anterior para este caso, sería el criterio que el CEPD denomina de "unidad de acto", que es el previsto en el artículo 83.3 del RGPD, según el cual "*Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves*". En el presente caso, la consecuencia sería la aplicación de la sanción correspondiente a la infracción del artículo 5.1.f) del RGPD.

En conclusión: entiende ENDESA que no se puede sancionar los hechos objeto del presente procedimiento al mismo tiempo por infracción de los artículos 5.1.f) y 32 del RGPD, por ser contrario al principio de "*non bis in idem*"; si se entiende que no concurren los requisitos para aplicar el citado principio, entiende que se estaría ante una situación de concurso de normas administrativas sancionadoras, y el criterio más adecuado para elegir cuál de ellas debe aplicarse sería el principio de especialidad ("*specialia generalibus derogant*"); por último y subsidiariamente a todo lo anterior, en todo caso deberá sancionarse únicamente por la infracción que conlleve la sanción más gravosa.

Al respecto, esta Agencia desea señalar que el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales, lo que puede producirse, o no, por ausencia o deficiencia de las medidas de seguridad.

Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita "mediante la aplicación de medidas técnicas y organizativas apropiadas", que no son estrictamente de seguridad.

Concluye ENDESA que las medidas técnicas y organizativas apropiadas a las que hace mención el art. 5.1.f) del RGPD son las medidas de seguridad del art. 32 del RGPD. Pero esto sería simplificar la esencia del RGPD cuyo cumplimiento no se limita a la implantación de medidas técnicas y organizativas de seguridad; significaría, en

este caso, reducir la garantía exigida mediante el principio de integridad y confidencialidad a su logro únicamente con medidas de seguridad.

Esta Agencia se reitera en que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el artículo 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. De seguridad. Sólo de seguridad.

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo, mientras que en el caso del artículo 5.1.f) del RGPD se debe garantizar la confidencialidad e integridad. Como se puede observar los dos artículos persiguen fines distintos, aunque puedan estar relacionados.

En cuanto al examen del *non bis in idem*, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que,

> *"(…) Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.*
>
> *Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):*
>
> a) La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa *que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.*
>
> *b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.*
>
> *c) La identidad de fundamento o causal, implica que las medidas sancionadoras no pueden concurrir si responden a una misma naturaleza, es decir, si participan de una misma fundamentación teleológica, lo que ocurre entre las penales y las administrativas sancionadoras, pero no entre las punitivas y las meramente coercitivas."*

Tomando como referencia lo anteriormente explicitado, en el presente procedimiento sancionador no se ha vulnerado el principio *non bis in idem*, puesto que, si bien enten-

dido grosso modo los hechos se detectan consecuencia de una violación de la seguridad de los datos personales, la infracción del artículo 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y de integridad, mientras que la infracción del artículo 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la violación de la seguridad de los datos personales en cuestión. De hecho, si estas medidas de seguridad (no apropiadas al riesgo, por cierto) que tenía implantadas ENDESA se hubieran detectado por esta Agencia sin que se hubiera producido la pérdida de confidencialidad y de integridad de los datos personales, ENDESA únicamente hubiera sido sancionada por el artículo 32 del RGPD.

Y todo ello frente a las alegaciones formuladas por ENDESA que considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. Ello no es cierto, puesto que el artículo 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

Como se ha indicado, mediante el artículo 5.1.f) del RGPD se sanciona una pérdida de disponibilidad y confidencialidad, únicamente, y mediante el artículo 32 del RGPD la ausencia y deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes que, en sí, infringen el RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad.

Por lo que no se considera vulnerado el principio *non bis in idem* en el presente procedimiento sancionador.

En cuanto al artículo 83.3 del RGPD, éste establece que:

"3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves."

En el presente caso, se propone una multa de 2.500.000 euros por la supuesta infracción del artículo 5.1.f) del RGPD y una multa de 1.500.000,00 euros por la supuesta infracción del artículo 32 del RGPD. En total, sumarían 4.000.000 de euros.

El volumen de negocio total anual global de ENDESA se ha establecido en ******CANTIDAD.1*** euros.

El artículo 83.2 del RGPD dispone que:

"*5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) *los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9 (…)".*

En el presente caso, el 4% del volumen de negocio total anual global de ENDESA sería de ******CANTIDAD.2*** euros. Por lo que la suma de las multas propuestas en el presente procedimiento sancionador no superaría tal importe, no habiéndose superado la regla de proporcionalidad del RGPD.

En cuanto a la referencia que hace ENDESA de lo dispuesto en las Directrices 4/2022 del Comité Europeo de Protección de Datos sobre el cálculo de multas administrativas bajo el RGPD, las mismas no resultan de aplicación al presente caso, sino a los hechos que hubieran tenido lugar con posterioridad a la adopción de las citadas Directrices.

Por todo lo expuesto, se desestima la presente alegación.

3. Vulneración del principio de tipicidad.

Indica ENDESA que el Tribunal Constitucional ha declarado que el derecho fundamental a la legalidad sancionadora recogido en el artículo 25.1 de la Constitución Española comprende una doble garantía. Una, de alcance formal y relativo, referida al rango que deben tener las normas tipificadoras (principio de legalidad); y otra, de alcance material y absoluto, relativa a la exigencia de la predeterminación normativa de las conductas ilícitas y de las sanciones correspondientes. Esta segunda garantía se identifica con el llamado principio de tipicidad.

Y que el principio de tipicidad contiene, a su vez, dos mandatos. El primero de ellos que, a estos efectos, interesa a ENDESA remarcar, es el de taxatividad (por todas, Sentencia del Tribunal Constitucional 297/2005, de 21 de noviembre). La taxatividad requiere de una descripción suficiente de las conductas tipificadas como infracción y de las sanciones que les corresponden en cada caso. El hecho de que no se pueda determinar con certeza suficiente cuál es la conducta que puede suponer un incumplimiento sería un caso de vulneración de aquel principio fundamental. Así, alega ENDESA que el artículo 5.1.f) del RGPD establece un principio general que no tiene concreción específica mediante actos positivos o limitativos claros que el sujeto obligado pueda conocer y cumplir. Al contrario, utiliza conceptos jurídicos indeterminados de forma encadenada ("seguridad adecuada", "medidas apropiadas"), que no permiten conocer de forma transparente el alcance de las obligaciones o prohibiciones.

En consecuencia, entiende ENDESA que en la aplicación de la norma la administración debe ser extremadamente cuidadosa a la hora de identificar los hechos constitutivos de infracción y de explicar el motivo por el cual esos hechos son incardinables en el tipo redactado de forma poco taxativa.

Al respecto, esta Agencia desea señalar que las infracciones en materia de protección de datos están tipificadas en los apartados 4, 5 y 6 del artículo 83 del RGPD. Es una tipificación por remisión, admitida plenamente por nuestro Tribunal Constitucional. En este sentido, también el artículo 71 de la LOPDGDD realiza una referencia a las mismas al señalar que "*Constituyen infracciones los actos y conductas a las que se*

refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

En este sentido, el Dictamen del Consejo de Estado de 26 de octubre de 2017 relativo al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal dispone que "*El Reglamento Europeo sí tipifica, por más que lo haga en un sentido genérico, las conductas constitutivas de infracción: en efecto, los apartados 4, 5 y 6 de su artículo 83 arriba transcritos contienen un catálogo de infracciones por vulneración de los preceptos de la norma europea que en tales apartados se indican. El artículo 72 del Anteproyecto asume, no en vano, la existencia de dicho catálogo, cuando dispone que "constituyen infracciones los actos y conductas que supongan una vulneración del contenido de los apartados 4, 5 y 6 del Reglamento Europeo y de la presente ley orgánica".*

En el presente caso, como ha concluido el Consejo de Estado, el modelo europeo de sanciones en el RGPD comporta un amplio arco en el importe de la sanción, en función de la concurrencia de las circunstancias del artículo 83.2, las cuales son objetivas y comprobables por los tribunales. De hecho, y como resulta de la propia STC 150/2020, de 22 de octubre, lo que se considera contrario al principio de taxatividad y lex certa, la vertiente material del artículo 25 de la Constitución Española, es:

> *encomendar por entero tal correspondencia a la discrecionalidad judicial o administrativa, «ya que ello equivaldría a una simple habilitación en blanco a la administración por norma legal vacía de contenido material propio»*

En el RGPD, norma que establece las infracciones y sanciones, no concurre dicha circunstancia no deseada por el Tribunal Constitucional, como es encomendar "por entero" (sic) a la discrecionalidad administrativa la correspondencia entre infracción y sanción. Bien al contrario. Ya el artículo 83.4 RGPD y 83.5 RGPD establecen una primera distinción en cuanto al importe de las sanciones a imponer según los preceptos infringidos. El artículo 83.6 RGPD, por otra parte, también acota debidamente la infracción. El artículo 83.2 RGPD, por otro lado, contiene las circunstancias que el legislador europeo considera que las autoridades de control han de tener en cuenta para determinar el importe de la sanción, que son circunstancias que no dependen de la "discrecionalidad administrativa", sino de una apreciación objetiva, y revisable por los tribunales.

Por tanto, se desestima la presente alegación.

Segunda.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 33 del RGPD

Alega ENDESA que resulta esencial, para el correcto entendimiento del asunto, clarificar con carácter previo tres conceptos que no pueden confundirse ni son intercambiables.

- **Brecha de Seguridad**: Hecho irregular que afecta a los sistemas y entornos tecnológicos de una sociedad desde múltiples posibles ámbitos. Una brecha de seguridad no conlleva necesariamente afectación a la información y no conlle-

va necesariamente afectación a la información personal que pueden contener los sistemas.

- **Violación de Seguridad de los Datos personales**: se produce cuando una Brecha de Seguridad afecta, además, a datos personales almacenados o tratados en los sistemas de información de la entidad. Según el artículo 4.12 del RGPD, es "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".
- **Violación de Seguridad de los Datos personales Notificable**: es aquella Violación de Seguridad de los Datos que: (i) de conformidad con el artículo 33 del RGPD, debe ser comunicada a la autoridad del control (en este caso la AEPD) por ser probable que entrañe un riesgo para los derechos y libertades de los interesados afectados; y (ii) de conformidad con el artículo 34 del RGPD, debe ser comunicada a los interesados afectados por ser probable que entrañe un alto riesgo para los derechos y libertades de éstos.

Como elemento adicional importante para la interpretación, debe tenerse en cuenta que los artículos 33 y 34 del RGPD hablan de notificaciones de violaciones de seguridad de los datos y no de brechas de seguridad.

Indica ENDESA que para determinar, por tanto, el cumplimiento o incumplimiento de la obligación contenida en el artículo 33 del RGPD, lo primero que debe examinarse es cuál es el momento en el que se entiende que un responsable o encargado del tratamiento tiene constancia de una Violación de la Seguridad de los Datos Notificable, esto es, una violación de la seguridad de los datos que pueda constituir un riesgo para los derechos y libertades de los interesados afectados. Una vez se haya determinado ese momento, se deberá determinar si la notificación se realizó dentro del plazo establecido en el artículo 33 del RGPD (72 horas).

En este sentido, y al contrario de lo que se indica en el Acuerdo de Inicio, ENDESA se reitera en que procedió a comunicar la Violación de la Seguridad de los Datos a la AEPD en el mismo momento en que tuvo un conocimiento suficiente sobre el alcance de la misma y, por tanto, tal y como indica el artículo 33 del RGPD, cuando tuvo constancia: (i) de que la misma afectaba a datos de carácter personal responsabilidad de Endesa (es decir, de que era una Violación de la Seguridad de los Datos); y (ii) de que la misma podría constituir un riesgo para los derechos y libertades de los interesados afectados (es decir, de que era una Violación de la Seguridad de los Datos Notificable).

Alega que para la mencionada determinación del momento exacto en el que se entiende que Endesa tuvo constancia de la Violación de la Seguridad de los Datos Notificable, resulta fundamental traer a colación de nuevo el *iter* cronológico de los principales hechos en los que intervienen, además de Endesa, las sociedades ******EMPRESA.1*** como proveedor externo de Endesa (encargado del tratamiento de Endesa) y ******EMPRESA.9*** como proveedor de ******EMPRESA.1*** y subcontratista de Endesa (subencargado del tratamiento de Endesa). Este *iter cronológico* es el siguiente:

Fecha	**Hecho**

24/08/2021	Endesa detecta un anuncio en Facebook a través del cual se ofertaba un código de usuario de la herramienta ******HERRAMIENTA.1*** de Endesa con posible acceso a datos de carácter personal de clientes de Endesa.
10/09/2021 a 13/09/2021	Una vez llevados a cabo los trabajos necesarios para confirmar la veracidad del anuncio, se analiza la Violación de la Seguridad de los Datos para comprobar si la misma es o no notificable de conformidad con los artículos 33 y 34 del RGPD.
14/09/2021	Endesa emite un primer informe en el que se concluye que, teniendo en cuenta la información disponible, es improbable que la Violación de la Seguridad de los Datos identificada constituya un riesgo para los derechos y las libertades de los interesados afectados puesto que no se tenía constancia de que se hubiese materializado el acceso fraudulento a ******HERRAMIENTA.1*** y que, por tanto, la Violación no es notificable.
28/09/2021	Endesa emite un nuevo informe actualizando el anterior y concluyendo de la misma manera, a la luz de la información disponible. Es decir, la Violación de la Seguridad de los Datos sigue sin ser notificable de conformidad con los artículos 33 y 34 del RGPD. De conformidad con la información facilitada a lo largo del Expediente y recogida en el Acuerdo de Inicio, en esta fecha Endesa ya había procedido al reseteo o deshabilitación de la cuenta de ******HERRAMIENTA.1*** de tres (3) usuarios comprometidos.
19/10/2021	Primera detección de un alta fraudulenta por parte de ******EMPRESA.1***, investigación del caso y comunicación a Endesa. Tras la comunicación, se lleva a cabo el cierre total de los usuarios de ******EMPRESA.9*** y el acceso a cualquier herramienta de Endesa.
20/10/2021	******EMPRESA.1*** finaliza la investigación del caso, identificando 137 contrataciones fraudulentas, 7 pendientes de validación por Endesa y 172 órdenes pendientes de validar por ******EMPRESA.9***. En este momento, y aunque todavía no contaba con toda la información sobre el incidente, Endesa, siguiendo el procedimiento que, des-

de el ***DEPARTAMENTO.6 y la Unidad Territorial de Reclamaciones de Endesa se desarrolló específicamente para este incidente, comienza a verificar las contrataciones y ponerse en contacto directamente con los interesados afectados para solventar la situación. Prueba de ello es que, tal y como se recoge en el Acuerdo de Inicio, Endesa prohibiese a ***EMPRESA.1** realizar dichas llamadas, puesto que Endesa deseaba ofrecer una atención personalizada a los interesados afectados.

27/10/2021 ***EMPRESA.1** recibe un email del gerente de ***EMPRESA.9** detallando el modus operandi de sus comerciales para llevar a cabo las contrataciones fraudulentas y lo pone en conocimiento de Endesa, adjuntando capturas de pantalla con anuncio de Facebook en los que se ofrece el alquiler y/o venta de credenciales de acceso a la aplicación ***HERRAMIENTA.1**.

Es en este momento, en el que la AEPD entiende que Endesa tuvo conocimiento de la Violación de la Seguridad de los Datos Personales (aspecto con el que Endesa está de acuerdo) y que, por tanto, debió proceder a la notificación de la brecha a la AEPD (aspecto con el que ENDESA está completamente en desacuerdo). A su entender, el Acuerdo de Inicio yerra en esta conclusión al equiparar Violación de la Seguridad de los Datos y Violación de la Seguridad de los Datos Notificable, entendiendo que todas y cada una de las primeras deben ser notificadas a la AEPD.

Basta acudir al artículo 33 del RGPD para concluir que esto no es así.

04/11/2021 Supuesta fecha de elaboración del informe sobre evaluación y gestión de brecha de seguridad elaborado por ***EMPRESA.1** y que nunca fue compartido por Endesa en incumplimiento de sus obligaciones como encargado del tratamiento.

18/11/2021 Endesa, en el marco de sus investigaciones, sigue solicitando a ***EMPRESA.1** información adicional sobre la Violación de la Seguridad de los Datos para, continuamente, reevaluar su conclusión de que la Violación no es notificable, sin que ***EMPRESA.1** ni ***EMPRESA.9** aporten información relevante a estos efectos15 (ver **Documento número 3** adjunto a

	este escrito de alegaciones).
Enero 2022	Endesa identifica nuevos anuncios publicados en Facebook donde se ofrece la venta de bases de datos de clientes de energía de varias empresas del sector. Tras su análisis, Endesa determina que la Violación de la Seguridad de los Datos identificada sigue sin ser notificable, puesto que no tiene constancia de que se haya materializado el acceso fraudulento a ******HERRAMIENTA.1***. Como se puede observar, esta es la misma conclusión a la que se llegó en septiembre de 2021. No es, como sostiene la AEPD en su Acuerdo de Inicio16, que en este momento Endesa no fuese "*capaz de advertir que existía una brecha de seguridad como tal*" o que no fuese "*consciente de que existía una brecha de seguridad que afectara a sus datos*". Antes, al contrario, Endesa sí era conocedora de la existencia de una Violación de la Seguridad de los Datos si bien consideró, tras analizar en detalle el alcance de la misma, que ésta no era notificable (de conformidad con el artículo 33 del RGPD).
07/01/2022	Endesa vuelve a requerir a ******EMPRESA.1*** para que aporte más información sobre la Violación de la Seguridad de los Datos y ******EMPRESA.1***, una vez más, facilita información incompleta (ver **Documento número 4** adjunto a este escrito de alegaciones) tras varios requerimientos de Endesa, impidiendo que Endesa reevalúe su conclusión de que la Violación no es notificable.
31/01/2022	Endesa resuelve el contrato de prestación de servicios suscrito con ******EMPRESA.1*** como consecuencia de: (i) la falta de información que recibe por parte de ******EMPRESA.1*** en relación al incidente; y (ii) el incumplimiento de las obligaciones de ******EMPRESA.1*** como encargado del tratamiento.

04/02/2022	Endesa envía un burofax a Facebook a través del cual se le informa de que ciertos usuarios de la plataforma están publicando información que podría ser constitutiva de delito y se solicita su colaboración para su eliminación. De nuevo, no es, como sostiene la AEPD en su Acuerdo de Inicio17, que "*pareciera que para el 4 de febrero de 2022 sí que Endesa era consciente de que los datos personales de su titularidad podían verse afectados por un incidente de seguridad".* Antes al contrario, Endesa, desde el 27 de octubre de 2021, es consciente de que ha sufrido una Violación de la Seguridad de los Datos, si bien no considera, hasta el momento, que esta sea notificable (de conformidad con el artículo 33 del RGPD) por entender, tras los correspondientes análisis, que no es probable que la misma suponga un riesgo para los derechos y libertades de los interesados.
08/02/2022	Seguridad de los Datos Notificable. Endesa ya tenía conocimiento de la Violación de la Seguridad de los Datos desde el 27 de octubre de 2021, si bien consideraba, tras los oportunos análisis, que la misma no era notificable.
09/02/2022	Tras completar los oportunos análisis de la Violación de la Seguridad de los Datos con el detalle relativo a que algunos de los usuarios comprometidos han tenido acceso a la herramienta ******HERRAMIENTA.2***, Endesa determina que, en este caso, dicha Violación es Notificable, por entender que ahora sí es probable que la misma suponga un riesgo (no alto) para los derechos y libertades de los interesados afectados.
10/02/2022	Endesa procede a notificar la Violación de la Seguridad de los Datos a la AEPD a través de su sede electrónica.

Explica ENDESA que, tal y como se desprende del cuadro anterior, los principales hitos del incidente sufrido por Endesa serían:

(i) 24 de agosto de 2021: Endesa detecta que puede que se haya producido una Brecha de Seguridad en sus sistemas y procede al análisis de la misma.

(ii) 10 al 13 de septiembre de 2021: Endesa confirma la Brecha de Seguridad y determina que, en el marco de la misma, se ha tenido acceso ilegítimo a datos responsabilidad de la Sociedad, por lo que se ha producido una Violación de la

Seguridad de los Datos y procede a su análisis para determinar si la misma es, o no, notificable de conformidad con los artículos 33 y 34 del RGPD.

(iii) 14 de septiembre de 2021: Endesa emite un primer informe de la Violación de la Seguridad de los Datos, concluyendo que la misma, en dicha fecha, no es probable que suponga un riesgo para los derechos y libertades de los interesados, por lo que no sería notificable.

(iv) 18 de septiembre de 2021: Endesa emite un segundo informe de la Violación de la Seguridad de los Datos, concluyendo que la misma, en dicha fecha, sigue sin ser notificable.

(v) Octubre de 2021: ******EMPRESA.1*** facilita a Endesa información adicional sobre la Violación de la Seguridad de los Datos, procediendo Endesa a analizar de nuevo la misma en detalle. Tras los análisis oportunos y con la escasa información facilitada hasta el momento por ******EMPRESA.1***, Endesa vuelve a concluir que la Violación de la Seguridad de los Datos no es notificable, puesto que, con la información facilitada, es improbable que la misma constituya un riesgo para los derechos y las libertades de los interesados afectados.

Esto es así dado que: (i) los comerciales que han llevado a cabo contrataciones fraudulentas han sido identificados y despedidos (además de denunciados ante la Policía); (ii) se han bloqueado los accesos de todos los comerciales de ******EMPRESA.9*** a las herramientas de Endesa que contienen datos de carácter personal de clientes de la Sociedad; y (iii) los interesados afectados están completamente identificados y Endesa se ha estado encargando, de manera individualizada, de contactar con ellos para conocer su situación en detalle y revertir, en su caso, la contratación fraudulenta que hubiesen podido sufrir.

(vi) Noviembre de 2021: Mientras que Endesa, en seguimiento de la Violación de la Seguridad de los Datos y en cumplimiento de sus obligaciones como responsable del tratamiento, sigue solicitando información sobre la misma a ******EMPRESA.1*** sin mucho éxito por la desidia del proveedor, este redacta y emite, supuestamente, un informe sobre la Violación de la Seguridad de los Datos que: (i) nunca comparte con Endesa en incumplimiento de sus obligaciones como encargado del tratamiento de Endesa; y (ii) concluye que la Violación de la Seguridad de los Datos podría suponer un alto riesgo para los interesados afectados cuando no dispone de la necesaria información para llegar a dicha conclusión ni conoce el alcance de las consecuencias de la misma.

De hecho, el propio informe de ******EMPRESA.1***, cuya validez y rigor Endesa impugna, y que la AEPD utiliza, entre otros argumentos, para justificar la proposición de una sanción que Endesa entiende improcedente: (i) indica claramente, en varios de sus apartados, que la brecha de seguridad sigue gestionándose por parte de Endesa, puesto que la misma no podía considerarse cerrada con la escasa información con la que se contaba en noviembre de 2021; y (ii) yerra en sus conclusiones al indicar que "*el nivel de severidad de las consecuencias para las personas afectadas puede ser considerado como alto ya que podrían enfrentarse a cortes de suministro de energía, estrés y costes adicionales*", puesto que en ningún caso estos se hubiesen enfrentado a consecuencias tan

graves como cortes de suministro de energía (estos no se producen de manera automática ni pueden realizarse sin previo aviso a los afectados).

Sin perjuicio de la escasa información de la que dispone (por falta de diligencia de ***EMPRESA.1** y ***EMPRESA.9**), Endesa reevalúa su conclusión sobre la notificación de la Violación de la Seguridad de los Datos y concluye, una vez más y a la vista de la falta de evidencias, que la misma no es notificable. Esto es así dado que Endesa, al contrario que ***EMPRESA.1**, conoce las acciones que ha ido tomando desde agosto de 2021 así como las verdaderas consecuencias a las que los interesados podrían enfrentarse como consecuencia de la Violación de la Seguridad de los Datos y, por tanto, puede determinar que es improbable que la misma suponga un riesgo para sus derechos y libertades.

(vii) Enero de 2021: Endesa sigue avanzando en la investigación de la Violación de la Seguridad de los Datos de manera interna y solicitando, sin éxito, información adicional sobre la misma a ***EMPRESA.1** para reevaluar su decisión sobre la no necesidad de notificación. A la vista de la falta de evidencias sobre un posible riesgo para los interesados, Endesa vuelve a concluir que la Violación de la Seguridad de los Datos no es notificable.

(viii) Febrero de 2021: Endesa, gracias a su propia labor de investigación del incidente (***EMPRESA.1** no fue capaz de facilitar a Endesa toda la información necesaria para realizar el correspondiente análisis sobre el alcance de la Violación de la Seguridad de los Datos), determina que los usuarios comprometidos han tenido acceso, no solo a la herramienta ***HERRAMIENTA.1**, sino también a la herramienta ***HERRAMIENTA.2**, la cual contiene categorías de datos adicionales a las contenidas en ***HERRAMIENTA.1**. En base a esta información y a que en la herramienta ***HERRAMIENTA.2** se almacenan datos de contacto de clientes de Endesa, así como datos relativos a números de cuenta bancaria y otros datos económicos, Endesa determina que la Violación de la Seguridad de los Datos debe ser notificada a la autoridad de control (la AEPD), puesto que la misma es probable que, ahora sí, constituya un riesgo para los derechos y las libertades de los interesados afectados (los interesados a cuyos datos se haya podido tener acceso ilegítimo no están completamente identificados ni concretados).

Tal y como se ha podido observar en los párrafos anteriores, la correcta diferenciación entre cada uno de los momentos y su calificación técnica de conformidad con lo indicado al comienzo de esta alegación (Brecha de Seguridad, Violación de la Seguridad de los Datos y Violación de la Seguridad de los Datos Notificable) es de suma importancia a la hora de calificar la notificación de la Violación de la Seguridad de los Datos realizada por Endesa como extemporánea o “en plazo”.

Tanto es así que, mientras que ENDESA entiende que la notificación de la Violación de la Seguridad de los Datos se realizó en tiempo y forma puesto que se realizó 24 horas después de haber concluido que la misma podía suponer un riesgo para los derechos y libertades de los interesados, la AEPD entiende que dicha notificación debió realizarse en fecha 27 de octubre de 2021, en el momento en el Endesa es conocedora, a través de un correo electrónico emitido por ***EMPRESA.1**, de que las credenciales de cinco usuarios de ***HERRAMIENTA.1** comprometidos en la violación de la seguridad

de los datos personales fueron adquiridas de forma ilícita para extraer datos de clientes de Endesa que se utilizaron para realizar contrataciones fraudulentas.

En dicho momento, tal y como se ha expuesto arriba, Endesa sí conocía, al contrario de lo que se indica en el Acuerdo de Inicio en múltiples ocasiones, que había sufrido una Violación de la Seguridad de los Datos, pero no consideraba, en aquél momento (dada la escasa información facilitada por ***EMPRESA.1**, la falta de evidencias sobre un posible riesgo para los interesados y el hecho de que Endesa ya había tomado todas las acciones posibles para hacer que fuese improbable que la Violación de la Seguridad de los Datos constituyese un riesgo para los derechos y las libertades de los interesados afectados), que la misma fuese notificable de conformidad con los artículos 33 y 34 del RGPD.

Con una diligencia máxima, Endesa reevaluó constantemente, tal y como se ha indicado, su conclusión respecto de la Violación de la Seguridad de los Datos. Dicha reevaluación culminó, el 10 de febrero de 2022, con la emisión del correspondiente informe ya facilitado a la AEPD en el marco de este Expediente en el que, tras las nuevas evidencias que ponían de manifiesto un posible acceso por parte de los usuarios comprometidos a la herramienta ***HERRAMIENTA.2**, se concluía que, en dicho momento, sí procedía notificar la Violación de la Seguridad de los Datos a la AEPD al cumplirse los requisitos establecidos para ello en el artículo 33 del RGPD.

Tal y como se ha indicado anteriormente, hasta que no se realizó dicho análisis y se emitió dicho informe, Endesa se encontraba ante una Violación de la Seguridad de los Datos que no podía ser considerada una Violación de la Seguridad de los Datos notificable al no llegar al umbral necesario para ser comunicada a la AEPD.

ENDESA procede a analizar, por tanto, ambas tesis:

(i) Tesis de la notificación tardía:

La AEPD establece, a lo largo del Acuerdo de Inicio, que: (a) Endesa niega haber sufrido una Violación de la Seguridad de los Datos hasta el mes de febrero de 2022; y (b) Endesa debería haber notificado la violación de la seguridad de los datos personales a la AEPD el 27 de octubre de 2021, fecha en la que ***EMPRESA.1** le comunica que algunos comerciales de ***EMPRESA.9** están llevando a cabo contrataciones fraudulentas.

El primer aspecto (a) es rechazado de pleno por Endesa. No es cierto que Endesa niegue haber sufrido una Violación de la Seguridad de los Datos. Endesa niega que la Violación de la Seguridad de los Datos cumpliese, hasta el mes de febrero de 2022, con los requisitos establecidos en la legislación de protección de datos aplicable para que fuese obligatoria su notificación a la AEPD.

El segundo aspecto (b) también debe ser rechazado de pleno por ENDESA. En primer lugar, porque la AEPD se apoya, para llegar a esta conclusión, en un informe elaborado por una tercera parte implicada en la Violación de la Seguridad de los Datos y, por tanto, totalmente parcial, que desconocía por completo todos los detalles de la Violación de la Seguridad de los Datos y las consecuencias que, de ella, se podían derivar para los interesados afectados. En segundo lugar, porque la AEPD toma esta fecha

como fecha en la que Endesa debería haber notificado la Violación de la Seguridad de los Datos al equiparar, contraviniendo lo indicado por el RGPD y las Guías elaboradas por las autoridades de control (incluida la AEPD) y el Comité Europeo de Protección de Datos, cualquier Violación de la Seguridad de los Datos a una Violación de la Seguridad de los Datos Notificable.

(ii) Tesis de la notificación en plazo. Por qué la tesis de Endesa sobre la notificación es la única admisible en derecho:

Al contrario de lo que sostiene la AEPD, ENDESA siempre ha alegado, a lo largo de todo el procedimiento administrativo informativo, que cumplió en tiempo y forma, con la obligación de notificación de la Violación de Seguridad de los Datos impuesta por el artículo 33 del RGPD. Y esto es así dado que únicamente transcurrieron 24 horas desde que Endesa determinó que la Violación de la Seguridad de los Datos era notificable (9 de febrero de 2022) y su efectiva notificación a través de la sede electrónica de la AEPD (10 de enero de 2022).

Tal y como indicaba la propia "*Guía para la gestión y notificación de brechas de seguridad*" publicada por la AEPD en su día, los responsables del tratamiento (en este caso, Endesa) deben seguir un plan de actuación en la gestión de las brechas de seguridad que comienza, tras la fase de preparación previa, con la fase de detección e identificación y continúa con la fase de análisis y clasificación antes de llegar, en su caso, a la fase de notificación.

Esta Guía fue posteriormente sustituida, en fecha 25 de mayo de 2021, por la actual "Guía para la notificación de brechas de datos personales".

En estas fases previas a la notificación los responsables deberán analizar las fuentes de detección del incidente, la naturaleza, clase, tipo y nivel de riesgo al que se enfrenta la organización para, en primer lugar, determinar si se encuentran ante una brecha de seguridad o no.

Y el análisis no acaba aquí. Según la propia Guía de la AEPD ya referenciada, una vez los responsables tienen constancia de que han sufrido una violación de seguridad de los datos, deberán: (i) recopilar y analizar la información relativa a la violación de seguridad de los datos; (ii) clasificar la violación de seguridad de los datos; (iii) investigar, comunicar y coordinar los medios internos y externos; (iv) poner en marcha el plan de respuesta; y, por último (v) determinar el riesgo que dicha violación de seguridad de los datos puede tener para los derechos y libertades de los interesados afectados de cara a proceder, en caso de que dicho riesgo sea alto, a comunicar la violación de seguridad de los datos a la autoridad competente.

En este mismo sentido, las propias "*Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679*" elaboradas por el Grupo de Trabajo del Artículo 29 (actual Comité Europeo de Protección de Datos), indican, a la hora de analizar cuándo se debe entender que un responsable "tiene constancia" de que se ha producido una violación de seguridad de los datos que:
"*El momento exacto en que puede considerarse que un responsable del tratamiento «tiene constancia» de una violación concreta dependerá de las circunstancias de di-*

cha violación. En algunos casos, estará relativamente claro desde el principio que se ha producido una violación, mientras que en otros puede llevar algún tiempo establecer si los datos personales se han visto comprometidos".

"Tras haber sido informado de una posible violación por una persona, un medio de comunicación u otra fuente, o cuando el propio responsable del tratamiento haya detectado un incidente de seguridad, este podrá iniciar un breve período de investigación para determinar si se ha producido o no una violación. Durante este período de investigación, no se puede considerar que el responsable del tratamiento «tenga constancia»".

De manera muy similar, el protocolo de gestión de brechas de seguridad elaborado por Endesa (ver **Documento número 5** adjunto a este escrito) establece una serie de hitos o fases diferenciadas en la gestión de las Brechas de Seguridad que, como no podía ser de otro modo, van desde el análisis de las características de la Brecha para determinar si la misma puede ser considerada una Violación de la Seguridad de los Datos, hasta el análisis y la realización de una "*evaluación del riesgo sobre los derechos y libertades de las personas físicas*" para determinar si, por su impacto y relevancia, la Violación de la Seguridad de los Datos debe ser comunicada a la autoridad de control.

En el presente caso, Endesa determinó, de manera muy temprana, que la Brecha de Seguridad sufrida en sus sistemas constituía una Violación de la Seguridad de los Datos. Tras ello, y de conformidad con la información a la que tenía acceso, evaluó y reevaluó en múltiples ocasiones el riesgo al que los interesados podrían enfrentarse como consecuencia de la Violación de la Seguridad de los Datos, determinando finalmente, el 9 de febrero de 2022, que la Violación de la Seguridad de los Datos debía ser notificada a la AEPD (como así hizo 24 horas después).

Es por todo lo anterior que entiende que Endesa procedió a comunicar la Violación de la Seguridad de los Datos a la AEPD en un brevísimo plazo desde que tuvo constancia de que efectivamente se encontraba ante una Violación de Seguridad de los Datos Notificable, ya que, hasta que no se contó con toda la información relativa al incidente y se realizó el correspondiente análisis, Endesa se encontraba, únicamente, ante una Violación de la Seguridad de los Datos respecto de la cual era improbable que constituyese un riesgo para los derechos y las libertades de los interesados afectados (tal y como se ha demostrado a posteriori). La actuación de Endesa por tanto, se encuentra avalada por la propia Guía para la notificación de brechas de datos personales actual elaborada por la AEPD, la cual indica: "*No es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas*".

Teniendo en cuenta todo lo anterior, Endesa considera que no existió, por tanto, infracción del artículo 33 del RGPD, por lo que no procedería sanción alguna.

Al respecto, esta Agencia desea señalar que el artículo 33 del RGPD es meridianamente claro al establecer que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación."

Es decir, debe comunicarse a la autoridad de control a más tardar 72 horas desde que se haya tenido constancia de ella, toda violación de la seguridad de los datos personales, excepto aquellas que sea improbable que constituyan un riesgo para los derechos y las libertades de las personas físicas.

El RGPD no hace referencia al grado de probabilidad ni de riesgo que debe existir para que esa violación de la seguridad de los datos personales sea notificable, en palabras de ENDESA. Simplemente, basta con que exista una probabilidad (la que sea) de que exista un riesgo para los derechos y libertades de las personas físicas (el que sea). Tampoco hace falta que ese riesgo se hubiera materializado para que tal incidente sea notificable, basta con que sea probable.

En el presente caso, esta Agencia considera que ENDESA no calificó correctamente el incidente al considerarlo que no era notificable y se reitera en que el incidente en cuestión era notificable desde que ENDESA tuvo conocimiento a través de los anuncios en Facebook de la posible brecha. Puede destacarse, entre otros acontecimientos, que el 1 de septiembre de 2021 ***EMPRESA.16 ya informó a ENDESA de que ***D.D.D.*** estaba implicada en la venta de credenciales; el 10 de septiembre de 2021 ENDESA ya conocía, con motivo del estudio del incidente, la veracidad del anuncio y la identificación de las credenciales usadas de forma fraudulenta para el acceso a la aplicación de Endesa ***PLATAFORMA.1.endesa.es; el 20 de octubre 2021 ***EMPRESA.1 informó a ENDESA que se habían producido altas fraudulentas; y sobre todo a partir de la comunicación de ******EMPRESA.1***, ENDESA conoció que se habían visto comprometidos cinco usuarios de ******HERRAMIENTA.1*** y que se había producido un uso indebido de los datos personales obrantes en sus sistemas, lo cual tuvo lugar el 27 de octubre de 2021. Sin embargo, la brecha no se notificó hasta el 10 de febrero de 2022. Con independencia de que se hubieran reseteado o eliminado los usuarios (lo cual ya se analizó sobradamente que no se hizo de forma inmediata ni diligentemente), la realidad es que el incidente ya había tenido lugar, se había perdido la confidencialidad de los datos personales titularidad de ENDESA y existía un riesgo probable para los derechos y libertades de las personas físicas, toda vez que ENDESA había perdido el control de los accesos a esos datos, con independencia de que se hubiera producido (o no) accesos indebidos, además, a ******HERRAMIENTA.2***. Por tanto, esta Agencia se reitera en que en el presente caso ENDESA debió notificar la violación de la seguridad de los datos personales en el plazo máximo de 72 horas desde que tuvo conocimiento de que el incidente se había producido, , pues como se afirma en las Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales, del Comité Europeo de Protección de Datos, adoptadas el 14 de diciembre de 2021, versión 2.0, al describir la brecha producida por la copia de datos comerciales de la base de datos de la empresa por su empleado:

> *"74. Aunque el único objetivo del antiguo empleado que copió los datos de forma maliciosa puede limitarse a obtener la información de contacto de la clientela de la empresa para sus propios fines comerciales, el responsable del tratamiento no está en condiciones de considerar que el riesgo para los interesados afectados sea bajo, ya que el responsable del tratamiento no tiene ningún tipo de garantía sobre las intenciones del empleado. Así pues, aunque las consecuencias de la violación de la seguridad podrían limitarse a la exposición a la auto comercialización no solicitada del antiguo empleado, no se excluye un uso indebido adicional y más grave de los datos robados, en función de la finalidad del tratamiento establecido por el antiguo empleado".*

Sobre este particular ha de tenerse en cuenta que la notificación de la brecha no debe realizarse después de que el responsable del tratamiento haya realizado un examen detallado de la situación sino cuando el responsable detecta que la brecha se ha producido, pudiendo realizase este análisis en paralelo con la notificación, como así se declara en las citadas Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales:

> "*8. Las violaciones de la seguridad de los datos son problemas de por sí, pero también pueden ser síntomas de un régimen de seguridad de datos vulnerable y posiblemente obsoleto; también pueden indicar deficiencias del sistema que deben abordarse. Como verdad general, siempre es mejor prevenir las violaciones de la seguridad preparándose por anticipado, ya que varias de sus consecuencias son, por naturaleza, irreversibles. Antes de que un responsable del tratamiento pueda evaluar plenamente el riesgo derivado de una violación causada por algún tipo de ataque, debe identificarse la causa principal del problema, a fin de determinar si las vulnerabilidades que dieron lugar al incidente siguen presentes y, por tanto, es posible seguir aprovechándose de ellas. En muchos casos, el responsable del tratamiento puede determinar que el incidente puede dar lugar a un riesgo, por lo que debe notificarlo. En otros casos, no es necesario posponer la notificación hasta que se haya evaluado plenamente el riesgo y la repercusión de la violación, ya que la evaluación del riesgo completa puede producirse en paralelo a la notificación y la información así obtenida puede facilitarse a la AC por fases sin más dilación indebida.*
>
> *. 9. La violación debe notificarse cuando el responsable del tratamiento considere que es probable que entrañe un riesgo para los derechos y libertades del interesado. Los responsables del tratamiento deben realizar esta evaluación en el momento en que tengan conocimiento de la violación. El responsable del tratamiento no debe esperar a un examen forense detallado y a medidas (tempranas) de mitigación antes de evaluar si es probable que la violación de datos entrañe un riesgo y, por tanto, debe notificarse.*
>
> *10. Si un responsable del tratamiento autoevalúa el riesgo como improbable, pero resulta que el riesgo se materializa, la autoridad de control competente puede hacer uso de sus poderes correctivos y decidir aplicar sanciones*."

Y se reitera en la Guía para la notificación de brechas de datos personales de la AEPD

"(…) cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información necesaria, el RGPD prevé que la información se facilitará de manera gradual, a la mayor brevedad y sin dilación. De forma general la Agencia Española de Protección de Datos prevé la posibilidad de realizar una notificación de tipo "inicial", antes de las 72 horas señaladas, rellenando el formulario con la información preliminar que se disponga, o en su caso las estimaciones preliminares sobre la brecha de datos personales. Antes del plazo máximo de 30 días desde la notificación inicial, el responsable de tratamiento deberá completar toda la información mediante una "modificación" de la notificación anterior, incluida la decisión tomada sobre la comunicación de la brecha de datos personales a los afectados (…)"
Asimismo, tal notificación debió tener lugar sin dilación indebida y a más tardar dentro de las 72 horas desde que se tenga constancia de la brecha de datos personales para que así esta Agencia pudiera ejercer las funciones que tiene encomendadas.

Según el Considerando 87 del RGPD:

> *"(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento*".

Cuestión que también se contempla en la Guía para la notificación de brechas de datos personales de la AEPD al especificar que, tras notificar una brecha de datos personales, el responsable de tratamiento puede recibir por parte de la AEPD diversas comunicaciones o notificaciones electrónicas, por ejemplo:

> *"• Comunicación con información relativa al registro de la brecha de datos personales notificada.*
> *• Notificación con un requerimiento de información adicional sobre la brecha de datos personales o el tratamiento de datos personales en cuestión en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD, así como el artículo 58 del RGPD.*
> *• Notificación con una orden para comunicar a los afectados la brecha de datos personales en virtud del artículo 34.4 al considerar que el riesgo para los afectados es alto, en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD, así como el artículo 58 del RGPD."*

Por todo lo expuesto, se desestima la presente alegación.

Tercera.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 34 del RGPD

Indica la AEPD, en el Acuerdo de Inicio, que Endesa, a la hora de realizar la correspondiente notificación sobre la violación de la seguridad de los datos personales a los

interesados afectados, no facilitó toda la información requerida por el artículo 34 del RGPD.

En primer lugar, Endesa remarca que la notificación realizada a los interesados afectados se realizó únicamente en cumplimiento del correspondiente requerimiento de la AEPD de fecha 4 de marzo de 2022, puesto que, del análisis del incidente realizado por Endesa, se determinó que la brecha de seguridad no constituía un alto riesgo para los derechos y libertades de los individuos afectados, como así se demostró a posteriori (a su juicio).

De hecho, tal y como ha quedado acreditado (a su juicio), Endesa únicamente recibió una única respuesta a la notificación realizada y ninguno de los interesados afectados sufrió inconvenientes importantes o consecuencias muy significativas o irreversibles como consecuencia de la brecha, puesto que: (i) Endesa implementó mecanismos suficientes para revertir las consecuencias de la brecha asumiendo todos los costes de gestión; y (ii) todos los interesados afectados fueron atendidos de manera personalizada por parte del equipo de Endesa e informados convenientemente del alcance de la brecha, sus consecuencias y las posibles medidas de mitigación que, de manera individualizada y concreta en función de las características del usuario, podían implementar.

Una vez más, el informe facilitado por ******EMPRESA.1***, cuya validez y rigor Endesa impugna, y que la AEPD utiliza, entre otros argumentos, para justificar la proposición de una sanción que Endesa entiende improcedente, yerra en sus conclusiones al indicar que "*el nivel de severidad de las consecuencias para las personas afectadas puede ser considerado como alto ya que podrían enfrentarse a cortes de suministro de energía, estrés y costes adicionales*". Incluso si no se tuviese en cuenta que, como ha quedado acreditado (a su juicio), Endesa actuó diligentemente para minorar al máximo las consecuencias que de la brecha podían derivarse para los interesados, en ningún caso estos se hubiesen enfrentado a consecuencias tan graves como cortes de suministro de energía, tal y como describe en el informe de ******EMPRESA.1***, puesto que, de conformidad con la regulación energética aplicable, estos no se producen de manera automática ni pueden realizarse sin previo aviso a los afectados.

De hecho, a la fecha de recepción del requerimiento de la AEPD, Endesa ya había tomado medidas ulteriores para garantizar que ya no existiese la probabilidad de que se concretizase el alto riesgo para los derechos y libertades del interesado que había apreciado la AEPD (por ejemplo, había rescindido el contrato con ******EMPRESA.1*** y sus subcontratistas de manera que no pudiesen realizar contrataciones fraudulentas adicionales) y estaba en contacto con muchos de los interesados afectados para solventar sus dudas y atender sus peticiones, cumpliendo así con la condición prevista en el artículo 34.3 b) del RGPD para determinar que la comunicación a los interesados no es necesaria. Sin perjuicio de lo anterior y con la finalidad de mostrar su máxima colaboración con esta Agencia y en un ejercicio de transparencia a todas luces innecesario desde el punto de vista normativo, Endesa decidió atender el requerimiento de la AEPD y facilitar la información requerida a los interesados afectados.

Para ello, y puesto que la intención de Endesa era atender de manera individualizada a cada uno de los interesados afectados (como había ido haciendo desde que tuvo conocimiento de las primeras contrataciones fraudulentas y continuó haciendo tras el en-

vío de las notificaciones de la Violación de la Seguridad de los Datos), Endesa optó, como se desprende del contenido de la notificación, por facilitar la información relativa a la Violación de la Seguridad de los Datos requerida por el artículo 34 del RGPD en un formato de dos capas, similar al validado por la LOPDGDD.

En una primera capa (la propia notificación), se facilita información de utilidad para los interesados como es la descripción de la Violación de la Seguridad de los Datos y su naturaleza ("*acceso indebido a determinados sistemas comerciales de Endesa"*), la confirmación de que Endesa ha implementado, ya con anterioridad al momento de la notificación, "*las oportunas medidas de seguridad, técnicas y organizativas, para evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades*" de los interesados (tal y como hemos mencionado en los párrafos anteriores, en el momento de la notificación ya no podría existir el alto riesgo apreciado por la AEPD puesto que ya se habían tomado las medidas oportunas para mitigarlo), y la dirección de contacto del ***PUESTO.2 a través de la cual se puede "*conocer el detalle de las medidas adoptadas u obtener más información*".

En una segunda capa, a la que los interesados: (i) podían acceder, si así lo deseaban, poniéndose en contacto con el ***PUESTO.2; o (ii) tendrían acceso una vez Endesa se pusiese en contacto con ellos para atender, de manera individualizada, su situación y revertir, en su caso, la contratación fraudulenta que hubiesen podido sufrir, la Sociedad proporcionaría a los interesados la información restante requerida por el artículo 34 del RGPD de manera individualizada, puesto que no todos los interesados podrían sufrir las mismas consecuencias tras la Violación de Seguridad de los Datos ni se vieron afectados de la misma manera, por lo que las posibles medidas de mitigación del riesgo serían distintas en función del caso concreto.

A través de este sistema de información por capas Endesa se aseguraba, no solo que la información sobre posibles consecuencias y medidas de mitigación se facilitara de manera individualizada y adecuada al caso concreto tal y como se ha mencionado arriba, sino también que los interesados afectados fuesen atendidos por un equipo, el de ***DEPARTAMENTO.4 de Endesa especializada en el ámbito comercial, especializado en materia de protección de datos y conocedor de las posibles consecuencias que para los derechos y libertades de los interesados podría tener la Violación de la Seguridad de los Datos.

En este sentido, resulta de suma importancia destacar que cualquier comunicación o consulta que los afectados hubieran remitido al buzón del DPO facilitado en la comunicación (***EMAIL.1) sería atendida de manera particular e individualizada por ***DEPARTAMENTO.4 de Endesa especializada en el ámbito comercial (en adelante, "***DEPARTAMENTO.4"). Ello demuestra la proactividad y la diligencia desplegada por Endesa a la hora de facilitar a los afectados toda la información necesaria relativa a la Violación de Seguridad, cuya tarea centralizó en ***DEPARTAMENTO.4. Este departamento estaba habilitado para atender y responder de manera individualizada las consultas que, en su caso, hubieran dirigido los afectados. Si bien, cabe señalar que, tal y como acreditó Endesa en la respuesta al requerimiento recibido el 27 de junio de 2022, ***DEPARTAMENTO.4 tan sólo recibió una comunicación cuya consulta no llegó a plantearse por parte del interesado.

Es por esta razón que Endesa decidió realizar una notificación de la Violación de Seguridad de los Datos en dos capas, para evitar trasladar a todos los interesados infor-

mación genérica que podría no ser de aplicación en su caso concreto. En cualquier de los dos casos anteriores (actuación proactiva por parte del interesado en un primer momento o posterior actuación proactiva por parte de Endesa), los interesados tendrían acceso al resto de la información requerida por el artículo 34 del RGPD, como es el detalle de las tipologías de datos afectados, la descripción de las medidas de seguridad concretas implementadas por Endesa para mitigar los posibles efectos adversos y la descripción de las posibles consecuencias que la Violación de Seguridad de los Datos sufrida por Endesa podría causarles. Como se puede observar, ninguno de estos puntos es extrapolable a todos los interesados afectados, y es por esta razón por la que Endesa, para lograr una comunicación efectiva del incidente, decidió realizarla en dos capas (una más genérica y otra individualizada).

En este sentido, la propia AEPD, en su infografía sobre cómo realizar las correspondientes notificaciones de brechas de datos personales a los interesados, indica que es preciso tener en cuenta que la notificación "no implica una única acción o acto" y que, por tanto, "*puede ejecutarse en distintas acciones atendiendo a la información que tenga el responsable sobre la magnitud de la brecha y las personas afectadas*" (el subrayado y la negrita son nuestros).

Así lo hizo Endesa en este caso para lograr una comunicación más efectiva con los interesados afectados atendiendo a las características de la Violación de Seguridad de los Datos.

A mayor abundamiento, conviene poner de manifiesto que tanto el ***DEPARTAMENTO.6 de Endesa, como ***DEPARTAMENTO.7, llevaron a cabo un procedimiento de auditoría y revisión de todas las contrataciones que gestionó ******EMPRESA.9*** durante el periodo comprendido entre el 1 de junio y el 15 de octubre de 2021. Y es que, teniendo en cuenta que tal y como ha quedado acreditado, ******EMPRESA.1*** no facilitaba a Endesa la información completa y detallada sobre la Violación de Seguridad, como medida de control y siendo altamente garantista, Endesa tomó la decisión de revisar todas las contrataciones tramitadas por ******EMPRESA.9*** durante un periodo de tiempo generoso.

Por tanto, en aras de la objetividad y en términos de estricta defensa jurídica, ante las manifestaciones que hace ******EMPRESA.1*** en su respuesta al requerimiento de la AEPD en cuanto a que propuso "*a Endesa realizar llamadas a los clientes que hayan podido verse afectados para confirmar tanto la legalidad de la contratación como la comprobación del número de cuenta facilitado*", pero, "*Endesa se lo prohibió*" cabe señalar que Endesa sí llevó a cabo la revisión y atención individualizada de cada contratación que tramitó ******EMPRESA.9***.

Estas tareas se delegaron en proveedores independientes a ******EMPRESA.1*** y en ***DEPARTAMENTO.7.

Al respecto, esta Agencia desea señalar que la necesidad o no de comunicar la violación de la seguridad de los datos personales en cuestión ya fue objeto de análisis y se concluyó que era necesaria comunicarla a los afectados, razón por la que se dictó resolución de fecha 7 de marzo de 2022 en la que se ordenó a ENDESA que así lo hiciera, en cumplimiento de lo dispuesto en el artículo 34 del RGPD. Por tanto, la

comunicación a los interesados de este incidente por parte de ENDESA era de obligado cumplimiento y no un ejercicio de “colaboración” por su parte.

Del hecho de que se hubiera recibido una única respuesta al envío de tal comunicación (por cierto, en la que se indica que esa persona no tenía relación alguna con ENDESA) no puede inferirse que el incidente en cuestión no constituía un alto riesgo para los derechos y libertades de los afectados. Más bien podría inferirse que no se recibió respuesta alguna de los afectados porque la comunicación fue deficiente y no dejó en claro debidamente que tal se había producido una violación de la seguridad de los datos personales de estos afectados lo cual podría acarrearles una serie de consecuencias por ellos no deseadas.

No puede afirmarse tajantemente tampoco como lo hace ENDESA que “ninguno de los interesados afectados sufrió inconvenientes importantes o consecuencias muy significativas o irreversibles como consecuencia de la brecha”, toda vez que ENDESA misma reconoció que no era capaz de saber el número concreto de accesos indebidos ni el alcance de los mismos. Simplemente, no hay constancia de que se hubieran producido.

En cuanto a la afirmación que realiza ENDESA de que “todos los interesados afectados fueron atendidos de manera personalizada por parte del equipo de Endesa e informados convenientemente del alcance de la brecha, sus consecuencias y las posibles medidas de mitigación que, de manera individualizada y concreta en función de las características del usuario, podían implementar”, pareciera que ENDESA se refiere a los afectados por la actuación de ******EMPRESA.1/***EMPRESA.9***. No obstante, el alcance del incidente en cuestión superó tales actuaciones, ya que la realidad es que se vieron comprometidos más usuarios de los que comunicaron estos proveedores y que los datos personales obrantes en ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** quedaron expuestos a más personas, no únicamente a aquellos que trabajaban en estas empresas. Por tanto, no es cierto que se hubiera atendido a todos los interesados afectados. A mayor abundamiento, ENDESA misma afirma que sólo se recibió una única comunicación producto de la comunicación realizada a los afectados, por lo que pareciera que la atención personalizada únicamente se habría producido respecto de aquellas personas en las que se detectó un alta fraudulenta como producto de la actuación de ******EMPRESA.1/***EMPRESA.9***. En cualquier caso, tampoco se ha acreditado a lo largo del presente procedimiento que tal atención personalizada hubiera tenido lugar.

En cuanto a la referencia al informe de ******EMPRESA.1*** en el que se afirma que una de las consecuencias podría ser que se cortase el suministro de energía, además del estrés y costes adicionales, si bien es cierto que no puede cortarse tal suministro de forma automática o sin previo aviso, no es menos cierto que aun habiendo avisado, si la persona en cuestión no abona lo adeudado, aunque el alta se hubiese producido de forma fraudulenta, el corte del suministro sí se produciría. Y también es cierto que, en cualquier caso, una vez esa persona tuviera conocimiento de que ENDESA le reclama una determinada deuda por un servicio que no solicitó, ese individuo estaría sometido a una situación de estrés y tendría que hacer frente a una serie de gastos que, de no haberse producido la violación de la seguridad de sus datos personales, no habrían tenido lugar. Todo ello sin olvidar que los datos podían ser sometidos a otros usos cuyas consecuencias desconocía ENDESA, por lo que el riesgo para los derechos y libertades de las personas era elevado.

En cuanto a que ENDESA ya había tomado medidas ulteriores para garantizar que ya no existiese la probabilidad de que se concretizase el alto riesgo para los derechos y libertades del interesado, rescindir el contrato con ******EMPRESA.1*** y sus subcontratistas y estar en contacto con muchos de los interesados afectados por las actuaciones de tales empresas, no puede entenderse que fueran medidas que eliminaran por sí el alto riesgo para los interesados, toda vez que el alcance del incidente ha sido mayor que lo que los empleados de esas empresas habían realizado, por lo que ni todos los accesos indebidos fueron a través de ******EMPRESA.1*** y sus subcontratistas ni sólo se vio en riesgo la confidencialidad de los datos de aquellos individuos a los que se dio de alta de forma fraudulenta, sino que se trata de que se vio vulnerada la confidencialidad de todos los datos personales de los sistemas ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** de ENDESA, razón por la cual esta Agencia ordenó a ENDESA que se enviara la citada comunicación a todos los afectados.

En cuanto a la información facilitada por ENDESA, sin entrar a valorar la conveniencia o no de utilizar un modelo por capas, se le proporcionó a los afectados la siguiente información:

> *"Nos ponemos en contacto contigo para informarte que hemos detectado un posible acceso indebido a determinados sistemas comerciales de Endesa Energía y que desde el mismo momento que hemos sido conocedores de este hecho, hemos adoptado las oportunas medidas de seguridad, técnicas y organizativas, para evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades de nuestros clientes, con lo que la confidencialidad y la integridad de tus datos personales no se ha visto comprometida."*

Esta información proporcionada no es veraz, toda vez que como mínimo la confidencialidad de los datos personales de los afectados ya se había visto comprometida (y quizás en algún caso la integridad también). Tampoco es cierto que con las medidas adoptadas se evitara producir una afectación de alto riesgo a los derechos y libertades de los afectados. Lo único que podía prevenir ENDESA era evitar, como mucho, una contratación fraudulenta con ENDESA. Pero los datos personales a los que se hubiera accedido podían ser utilizado para otras finalidades, como obtener más datos personales de estos afectados a través de ingeniería social y suplantar su identidad en otras situaciones.

En todo caso, parece ENDESA olvidar que el artículo 34 del RGPD no se trata de que deba haberse producido un daño, sino que se trata de comunicar a los afectados que podría existir un riesgo para sus derechos y libertades, por ejemplo, ser víctima de *phishing*, de otro ciberataque o de cambio de compañía de suministros. Existe un riesgo muy elevado de ser víctima de suplantación de identidad y fraude, tal y como esta Agencia está más que acostumbrada a ver en su día a día. Y esta información no se desprende de la comunicación realizada por ENDESA.

Por último, en cuanto a que ENDESA revisó todas las contrataciones que gestionó ******EMPRESA.9*** entre el 1 de junio y el 15 de octubre de 2021, esta Agencia entiende que eso era lo que debía hacer como responsable de tratamiento y no tiene más que añadir.

Por lo expuesto, se desestima la presente alegación.

Cuarta.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 44 del RGPD

Alega ENDESA que, cuando trabaja con proveedores ubicados fuera del Espacio Económico Europeo y, por tanto, realiza transferencias internacionales de datos, implementa garantías adecuadas para ello de conformidad con los artículos 44 y 46 del RGPD, al contrario de lo que se indica en el Acuerdo de Inicio.

Indica ENDESA que le resulta verdaderamente sorprendente que la AEPD, en su Acuerdo de Inicio, proponga la imposición de una presunta infracción del artículo 44 del RGPD, cuando en ninguno de los cuatro (4) requerimientos de información enviados a Endesa (tres dirigidos directamente a la Sociedad y uno a su DPO) a lo largo de los más de siete (7) meses que han durado las actuaciones previas de investigación del presente caso, esta Agencia ha solicitado a Endesa prueba alguna de la implementación de garantías adecuadas para la realización de las correspondientes transferencias internacionales.

De haberlo hecho, Endesa, tal y como hace a través del escrito de alegaciones al acuerdo de inicio del presente procedimiento, le hubiera facilitado a esta Agencia las correspondientes Cláusulas Contractuales Tipo suscritas con sus proveedores ubicados fuera del Espacio Económico Europeo, en cumplimiento de su procedimiento interno para la realización de transferencias internacionales (Documento número 6).

Sin perjuicio de lo anterior y a fin de probar la adecuada implementación de garantías suficientes para la realización de transferencias internacionales de conformidad con los artículos 44 y siguientes del RGPD, se adjunta al citado escrito de alegaciones, como Documentos números 7, 8 y 9, las correspondientes Cláusulas Contractuales Tipo suscritas con los proveedores ******EMPRESA.15*** (...), ******EMPRESA.12*** (...) y ******EMPRESA.9.*** (...).

A este respecto se adjuntan: (i) las Cláusulas Contractuales Tipo suscritas en el momento de la contratación; y (ii) las Cláusulas Contractuales Tipo actualizadas de conformidad con la Decisión de Ejecución (UE) 2021/94 de la Comisión, de 4 de junio de 2021 que se han suscrito con posterioridad.

Alega ENDESA que, con anterioridad a la realización de las correspondientes transferencias internacionales de datos identificadas en el Acuerdo de Inicio, implementó garantías suficientes de conformidad con la normativa de protección de datos aplicable. En concreto, suscribió con sus encargados y subencargados del tratamiento ubicados en ***PAÍS.2 y ***PAÍS.1 las correspondientes cláusulas contractuales tipo aprobadas por la Comisión Europea previstas en el artículo 46.2 c) del RGPD.

Por todo ello, Endesa considera improcedente la propuesta de sanción por presunta infracción del artículo 44 del RGPD contenida en el Acuerdo de Inicio.

Al respecto, esta Agencia desea señalar que el artículo 67 “Actuaciones previas de investigación” de la LOPDGDD establece que “1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la

Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento". Es decir, que estas actuaciones no son en modo alguno obligatorias, sino que son facultad de esta Agencia el llevarlas a cabo no.

Por lo demás, en el presente caso, ENDESA ha realizado transferencias internacionales a ***PAÍS.1 y ***PAÍS.2, y continúa realizando transferencias a ***PAÍS.2, países respecto de los cuales la Comisión no ha declarado que garanticen un nivel de protección adecuado, en los términos que fija el artículo 45 del RGPD.

El artículo 46 del RGPD trata de las «transferencias sujetas a garantías adecuadas» y dispone en su apartado 1 que, a falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Añade el artículo 46, apartado 2, del RGPD que las «garantías adecuadas» podrán ser aportadas, sin necesidad de autorización expresa de una autoridad de control, entre otras, por cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2. (artículo 46, apartado 2, letra c).

En este sentido, la Comisión Europea ha adoptado la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Estas cláusulas contractuales tipo adoptadas por la Comisión Europea constituyen un método para proporcionar «garantías adecuadas» en ausencia de una decisión de adecuación con arreglo al artículo 46, apartado 2, letra c), del RGPD, estableciendo nuevas cláusulas contractuales tipo que pueden ser utilizadas tanto por el responsable como por el encargado a fin de ofrecer garantías adecuadas en el sentido del artículo 46, 1 del RGPD, quedando derogadas las anteriores decisiones de 2001 y 2010, a partir del 27 de septiembre de 2021. Ahora bien a tenor de su cláusula 4.4 se considera que los contratos celebrados antes del 27 de septiembre de 2021 con arreglo a la Decisión 2001/497/CE o la Decisión 2010/87/UE ofrecen garantías adecuadas en el sentido del artículo 46, apartado 1, del RGPD hasta el 27 de diciembre de 2022, siempre que las operaciones de tratamiento que sean objeto del contrato permanezcan inalteradas y que las cláusulas contractuales tipo garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas.

Sentado lo anterior conviene resaltar que la cláusula 14 de la decisión se refiere al «Derecho y prácticas del país que afectan al cumplimiento de las cláusulas». Esta cláusula contiene cuatro módulos relativos a la transferencia de responsable a responsable; transferencia de responsable a encargado; transferencia de encargado a encargado; y transferencia de encargado a responsable, a los que resultan de aplicación las disposiciones que contiene. Así establece lo siguiente:

"*MÓDULO UNO: transferencia de responsable a responsable*

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:

i)las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;

ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables (12);

iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador *de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.*

d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a). [Módulo tres: El exportador de datos notificará al responsable.]

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres:, si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).”

De este modo, la cláusula 14 establece una obligación para el exportador e importador de elaborar una evaluación que tenga en cuenta todas las cuestiones que la propia cláusula determina.

El artículo 46.2.c) debe interpretarse a la luz de la doctrina del TJUE recogida en su sentencia Schrems II:

“132 Dado que, como se desprende del apartado 125 de la presente sentencia, es inherente al carácter contractual de las cláusulas tipo de protección de datos que estas no pueden vincular a las autoridades públicas de países terceros, pero que los artículos 44 y 46, apartados 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta, exigen que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea comprometido, puede resultar necesario completar las garantías recogidas en esas cláusulas tipo de protección datos. A ese respecto, el considerando 109 del referido Reglamento dispone que «la posibilidad de que [los] responsable[s] […] del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión […] no debe obstar a que los responsables […] añadan otras cláusulas o garantías adicionales» y precisa, en particular, que «se debe alentar a los responsables […] a ofrecer garantías adicionales […] que complementen las cláusulas tipo de protección de datos».

133 Resulta, por tanto, evidente que las cláusulas tipo de protección de datos adoptadas por la Comisión en virtud del artículo 46, apartado 2, letra c), del mismo Reglamento tienen únicamente como finalidad proporcionar a los responsables o encargados del tratamiento establecidos en la Unión garantías contractuales que se

apliquen de manera uniforme en todos los países terceros y, por tanto, independientemente del nivel de protección garantizado en cada uno de ellos. En la medida en que esas cláusulas tipo de protección de datos no pueden proporcionar, debido a su naturaleza, garantías que vayan más allá de una obligación contractual de velar por que se respete el nivel de protección exigido por el Derecho de la Unión, tales cláusulas pueden necesitar, en función de cuál sea la situación de un país tercero determinado, la adopción de medidas adicionales por parte del responsable del tratamiento con el fin de garantizar el respeto de ese nivel de protección.

134 A este respecto, tal como ha señalado el Abogado General en el punto 126 de sus conclusiones, el mecanismo contractual previsto en el artículo 46, apartado 2, letra c), del RGPD se basa en la responsabilización del responsable o del encargado del tratamiento establecidos en la Unión, así como, con carácter subsidiario, de la autoridad de control competente. Corresponde, por tanto, ante todo, a ese responsable o encargado del tratamiento comprobar, caso por caso y, si es preciso, en colaboración con el destinatario de la transferencia, si el Derecho del tercer país de destino garantiza una protección adecuada, a la luz del Derecho de la Unión, de los datos personales transferidos sobre la base de cláusulas tipo de protección de datos, proporcionado, cuando sea necesario, garantías adicionales a las ofrecidas por dichas cláusulas."

En este orden de ideas han de tenerse también en cuenta las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020, en las que al interpretar la citada sentencia del TSJUE declaran que "*el Tribunal deja abierta la posibilidad de que los exportadores apliquen medidas complementarias que palíen estas lagunas de protección, a fin de que esta alcance el nivel exigido por el Derecho de la Unión. El Tribunal no especifica qué medidas podrían ser. Sin embargo, el Tribunal subraya que los exportadores tendrán que determinarlas caso por caso. Tal extremo concuerda con el principio de responsabilidad proactiva del artículo 5, apartado 2, del RGPD, que exige que los responsables del tratamiento sean responsables y capaces de demostrar el cumplimiento de los principios del RGPD relativos al tratamiento de datos personales (…)*"

Ha de recordarse que Endesa ha aportado, respecto de la transferencia a ***PAÍS.1, realizada a través de ***EMPRESA.12,** resolución de contrato entre Endesa y ***EMPRESA.16**, de fecha 15 de noviembre de 2022. Asimismo, ha aportado comprobante de baja de ***EMPRESA.9**. como proveedor de Endesa, con fecha 2 de noviembre de 2021. Por tanto, estos contratos se rescindieron antes del 27 de diciembre de 2022.

Respecto de la transferencia a ***PAÍS.2, ENDESA ha aportado la Evaluación de Impacto sobre Transferencias a ***PAÍS.2 que tiene por objeto evaluar, en relación con la transferencia de datos personales del exportador al importador, el nivel de adecuación del tercer país de destino, así como la adopción de medidas de seguridad técnicas y organizativas adecuadas para mitigar el riesgo de dicha transferencia.

Así las cosas, esta evaluación se limita a valorar las medidas de seguridad técnicas y organizativas aplicadas por el importador de datos, sin abordar la necesidad o no de

adoptar otras medidas contractuales complementarias a las cláusulas contractuales tipo que pudieran ser necesarias.

En este orden de ideas cabe destacar que, en cuanto a la evaluación legislativa del país importador, la evaluación arroja el resultado “3 – Parcialmente adecuado”, limitándose a contemplar la existencia de una normativa de protección de datos y de una autoridad de control independiente en el tercer país, pero ni siquiera se analizan las funciones y poderes de esta autoridad.

Asimismo, aporta el documento denominado “análisis legislación y prácticas” de ***PAÍS.2, destinado a evaluar si los datos personales que se transfieren están adecuadamente protegidos en relación con el potencial acceso de las autoridades de los países a los que se transfieren los datos. En este documento se recoge que la Constitución de ***PAÍS.2 garantiza el derecho fundamental a la intimidad personal y familiar y que recoge la necesidad de orden judicial para la interceptación de las comunicaciones. También se tiene en cuenta, en este documento, la existencia de una ley de protección de datos.

Del análisis de esta documentación no puede afirmarse que la evaluación contemple un análisis del derecho y las prácticas de ***PAÍS.2 suficiente que permita valorar si el tercer país de destino ofrece un nivel de protección adecuado. De este modo no contiene ninguna evaluación sobre la existencia de normas que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades, así como las limitaciones y garantías aplicables. Según la citada STJUE este análisis debería incluir los elementos que se recogen en el artículo 45.2. del RGPD, que incluye el análisis sobre la existencia de tratados internaciones firmados por el tercer país u otros compromisos internacionales adoptados (art. 45.2.c) RGPD), el estudio de la legislación nacional del tercer país en el sentido pretendido por el artículo 45.2.a) del RGPD:

“*el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos*”

Análisis que también recoge el considerando (20) de la Decisión de Ejecución (UE) 2021/914 de la Comisión.

“Las partes deben tener en cuenta, en particular, las circunstancias específicas de la transferencia (como el contenido y la duración del contrato, la naturaleza de los datos transferidos, el tipo de destinatario y la finalidad del tratamiento), el Derecho y las prácticas del tercer país de destino que sean de aplicación dadas las circunstancias de la transferencia y las garantías establecidas para complementar las garantías contempladas en las cláusulas contractuales tipo (como medidas contractuales,

técnicas y organizativas pertinentes que sean de aplicación a la transferencia y al tratamiento de los datos personales en el país de destino). Por lo que se refiere al efecto del Derecho y prácticas mencionados sobre el cumplimiento de las cláusulas contractuales tipo, pueden valorarse diferentes elementos en una evaluación global; por ejemplo, información fiable sobre la aplicación del Derecho en la práctica (jurisprudencia, informes de organismos de supervisión independientes, etc.), la existencia o ausencia de solicitudes en el mismo sector y, en condiciones estrictas, la experiencia práctica documentada del exportador y/o el importador de datos."

Las deficiencias observadas en la Evaluación de Impacto de Protección de Datos de ***PAÍS.2 como país importador de datos personales impiden que pueda considerarse aportada la garantía de la citada cláusula 14.

Por todo lo expuesto, se desestima la presente alegación.

Quinta.- Sobre la graduación de la sanción impuesta a Endesa y la falta de proporcionalidad relativa del Acuerdo de Inicio de Procedimiento sancionador

Alega ENDESA, en primer lugar, la extrañeza en relación con el criterio que la AEPD ha seguido a la hora de analizar y finalmente proponer sancionar a Endesa en comparación con otros casos relativos a violaciones de seguridad de los datos frente a los que se ha iniciado procedimientos sancionadores o de investigación.

Por ejemplo:

a. La resolución de la AEPD relativa al procedimiento E/08809/2019 finalizó con el archivo de las actuaciones, indicando la AEPD que la entidad investigada "*disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo*", cuando dicha Violación de Seguridad de los Datos:

> - afectó a aproximadamente 22 millones de registros mundialmente (frente a los 760 interesados afectados por la Violación de la Seguridad de los Datos de Endesa que ahora nos ocupa);
> - implicó la extracción por parte de los atacantes de datos básicos y datos económico-financieros tales como información de tarjetas de crédito, además de otros datos que no fueron comprometidos en el incidente que afectó a Endesa como nombres de usuario y contraseñas de los interesados;
> - trajo consigo la recepción, por parte del responsable del tratamiento, de hasta ochenta (80) solicitudes de información por parte de los afectados, frente a la **única** recibida por Endesa y aportada en el marco del Expediente; y
> - se produjo aun con la implantación de medidas de seguridad.

b. La resolución de la AEPD relativa al procedimiento PS/00118/2020 finalizó con la imposición de una sanción de apercibimiento considerando la AEPD que "*en atención a la complejidad de los sistemas de información afectados, así como las acciones tomadas tendentes a minimizar las consecuencias negativas de la citada brecha de seguridad de los datos personales de sus clientes, se considera conforme a derecho no imponer sanción consistente en multa administrativa*", cuando en dicha Violación de la Seguridad de los Datos:

- la notificación de la violación de seguridad de los datos a la AEPD se realizó el 28 de agosto de 2019 cuando la entidad investigada tuvo constancia de que su sistema de información de clientes había sido objeto de acceso indebido el 10 de julio de 2019 (casi dos meses después);
- la entidad investigada en este supuesto no aportó a la AEPD el análisis de riesgos de los tratamientos de los que es responsable mientras que Endesa sí lo hizo, respondiendo en tiempo y forma a esta Agencia hasta en cuatro (4) ocasiones en las que se le trasladaron otros tantos requerimientos de información; y
- la entidad investigada declaró que "*la máquina afectada por los incidentes de seguridad estaba técnicamente obsoleta*", por lo que no contaba con medidas de seguridad adecuadas al riesgo que conllevaba el tratamiento.

c. La resolución de la AEPD relativa al procedimiento E/05937/2021 finalizó con la imposición de una sanción de apercibimiento considerando la AEPD que "*no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos*", cuando en dicha Violación de la Seguridad de los Datos:

- la notificación de la violación de seguridad de los datos a la AEPD se notificó, de conformidad con lo indicado por la AEPD en su resolución, "*en un plazo superior a las 72 horas desde que se tuvo conocimiento de que se había producido*". En este caso, la AEPD señala que se han acreditado correctamente los motivos de tal dilación, ya que la entidad investigada alegó que la notificación se retrasó "*debido a las investigaciones llevadas a cabo para esclarecer si hubo acceso de datos y/o actividad fraudulenta, lo que requirió múltiples análisis por parte de los equipos de seguridad*". Este motivo podría ser considerado parecido al alegado por Endesa. En este caso, sin embargo, a pesar del reconocimiento del transcurso del plazo de notificación por la entidad afectada por el incidente, la existencia de investigaciones sí pareció ser suficiente en esta ocasión para evitar la sanción económica; y
- la entidad investigada en este supuesto trata categorías de datos tales como nombre, número de identificación, dirección de correo electrónico, datos económicos y financieros, etc. al tratarse de un emisor de tarjetas de crédito. Por lo tanto, el impacto del incidente parece similar al del sufrido Endesa.

d. La Resolución de la AEPD relativa al procedimiento PS/00254/2019 finalizó con la imposición de una sanción de apercibimiento considerando la AEPD que, la entidad investigada, al haber solucionado las vulnerabilidades detectadas y mejorado el nivel seguridad con posterioridad a la violación de la seguridad de los datos personales, "*se considera conforme a derecho no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento*", cuando en dicha Violación de la Seguridad de los Datos:

- supuso el acceso indebido a los datos personales de hasta 30.000 interesados (frente a los 760 interesados afectados por la Violación de la Seguridad de los Datos de Endesa que ahora nos ocupa); y
- la AEPD consideró que, de las investigaciones llevadas a cabo, se apreciaba una falta de diligencia del responsable en la implementación de medidas de se-

guridad relevantes, indicando incluso que "*la ausencia de consideración del riesgo que puede suponer el acceso no autorizado por terceros a datos de suscriptores de información relacionada con un partido político, y su posterior difusión pública, agrava el reproche culpabilístico y sancionador de la conducta*".

Teniendo en cuenta lo anterior, sorprende a ENDESA que la AEPD considere que únicamente la Violación de la Seguridad de los Datos sufrida por Endesa merece la imposición de una sanción que supera, con creces, el importe de las sanciones impuestas hasta la fecha.

Indica que resulta llamativo, por ende, la disparidad de criterios que la AEPD aplica a la hora de analizar las medidas de seguridad implementadas por las entidades investigadas por la AEPD, así como las consecuencias que, en materia de sanciones administrativas, se derivan de las presuntas infracciones contenidas en el Acuerdo de Inicio.

En segundo lugar, remarca ENDESA cómo la AEPD, en el Acuerdo de Inicio, le aplica, en relación con todas las presuntas infracciones contenidas en el mismo, las agravantes de:

(i) "*grave falta de diligencia*": Como se ha expuesto a lo largo de este escrito, la apreciación de esta falta de diligencia se apoya, principalmente, en los siguientes elementos fácticos que no se corresponden con la calificación que la AEPD les atribuye:

(a) el informe sobre evaluación y gestión de brecha de seguridad elaborado por ******EMPRESA.1***, cuando ENDESA lo impugna expresamente por las razones mencionadas a lo largo de este escrito;

(b) el supuesto retraso en la implementación de las medidas de seguridad identificadas por Endesa con anterioridad a la notificación de la Violación de la Seguridad de los Datos, cuando el mismo ha sido totalmente justificado, de conformidad con lo indicado en este escrito, en base a la complejidad de la implementación de las mismas;

(c) el hecho de que Endesa no se dirigiese a Facebook Ireland Limited para exigir la retirada de los anuncios identificados, cuando se ha justificado dicha decisión, se ha probado que Endesa, en contraposición, se dirigió en múltiples ocasiones (y a través de 2 burofaxes) a Facebook Spain con dicha finalidad y se ha demostrado que, con anterioridad al envío de los burofaxes, Endesa ya había deshabilitado las credenciales de los usuarios comprometidos, de manera que estos ya no podían acceder a sus cuentas en los sistemas de Endesa;

(d) el supuesto retraso a la hora de notificar la Violación de la Seguridad de los Datos a la AEPD, cuando Endesa ha demostrado, en el marco de este escrito, que procedió a realizar la notificación en el plazo de 24 horas desde que tuvo constancia de que la Violación de la Seguridad de los Datos podría suponer un riesgo para los derechos y libertades de los interesados (con anterioridad a este momento Endesa no consideraba que la Violación de la Seguridad de los Datos fuese Notificable);

(e) el hecho de que Endesa no identificó, por su cuenta, la necesidad de notificación de la brecha a los interesados y no facilitó toda la información requerida por el artículo 34 del RGPD, cuando Endesa ha demostrado, en el marco de este escrito, que no podía, en ningún caso, derivarse de esta Violación de la Seguridad de los Datos un alto riesgo para los derechos y libertades de los interesados, que se cumplía con uno de los supuestos del artículo 34 del RGPD (art. 34.3 b) del RGPD) para determinar que la notificación no era necesaria y que sí procedió a facilitar a los interesados, en formato de dos capas, toda la información requerida por el artículo 34 del RGPD; y

(f) el hecho de que Endesa no ha implementado, tras más de cuatro (4) de aplicación del RGPD, las garantías adecuadas para la realización de transferencias internacionales de datos, cuando Endesa ha demostrado, en el marco de este escrito, que siempre lo ha hecho, facilitando a esta Agencia las correspondientes Cláusulas Contractuales Tipo aprobadas por la Comisión Europea suscritas con sus proveedores ubicados fuera del Espacio Económico Europeo.

(ii) "*vinculación de la actividad del infractor con la realización de tratamientos de datos personales*": Considerar la actividad de Endesa (comercializadora de energía eléctrica) como una agravante resulta (a juicio de ENDESA) totalmente inexplicable, salvo que se argumente y justifique la relación entre la actividad y la agravación que se pretende.

La actividad de comercialización de energía eléctrica supone, por supuesto que esta esté habituada "*al tratamiento de datos personales*", pero que ello suponga una agravación cuando la mayoría de empresas a nivel mundial tratan datos de clientes y terceros y realizan una actividad que conlleva estar en permanente contacto con ellos resulta difícil de percibir, puesto que, de ser este el caso, se estaría aplicando esta circunstancia agravante (que debería ser excepcional) a la gran mayoría de los casos analizados por la AEPD, desvirtuando completamente la naturaleza de dicha agravante (como así está sucediendo fruto de la aplicación, a su juicio desmesurada, que la AEPD está llevando a cabo de esta circunstancia agravante).

Por último, tal y como se desprende del Acuerdo de Inicio, alega ENDESA que la AEPD no ha considerado, a la hora de graduar las sanciones propuestas, la aplicación de todas las circunstancias atenuantes que se dan, a su juicio, en las conductas de Endesa objeto de este procedimiento.

Todo ello teniendo en cuenta que, desde el primer momento en que Endesa tuvo conocimiento del incidente, la Sociedad puso todos los medios a su alcance para: (i) evaluar el impacto de la Brecha de Seguridad y, posteriormente, de la Violación de la Seguridad de los Datos; (ii) paliar los efectos del incidente; (iii) tomar las medidas oportunas de cara a evitar que incidentes como el que tuvo lugar vuelvan a suceder en el futuro; (iv) colaborar con la AEPD realizando las comunicaciones oportunas y respondiendo a todos los requerimientos de información en tiempo y forma; y (v) paliar los mínimos efectos que los interesados sufrieron como consecuencia del incidente.

Por todo ello, Endesa considera que, de entenderse por esta Agencia que ha cometido las infracciones descritas en el Acuerdo de Inicio, resultarían de aplicación las siguientes circunstancias atenuantes a todas las presuntas infracciones:

(i) Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados, prevista en el artículo 83.2 c) del RGPD.

A este respecto es preciso indicar que:

(a) Antes de que Endesa recibiese reclamación alguna como consecuencia de la Violación de Seguridad de los Datos, la Sociedad procedió a realizar un seguimiento y auditoría de las contrataciones realizadas por ******EMPRESA.9***, a fin de atajar y solventar, con la mayor rapidez posible, cualquier efecto perjudicial que de la Violación de la Seguridad de los Datos se podía desprender para los interesados;

(b) Endesa adoptó las medidas de protección técnicas y organizativas apropiadas tras tener constancia de la Violación de la Seguridad de los Datos para garantizar que no se materializara riesgo alguno para los derechos y libertades de los interesados afectados.

(ii) Cooperación con la autoridad de control, prevista en el artículo 83.2 f) del RGPD.

En relación a la atenuante relativa a el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción, es preciso indicar que:

(a) Únicamente transcurrieron 24 horas desde que Endesa tuvo conocimiento de que se trataba de una Violación de Seguridad de los Datos notificable y la notificó a la AEPD; y

(b) Endesa, tal y como ha quedado acreditado y se desprende del Expediente, contestó a todos y cada uno de los requerimientos de información que recibió por parte de la AEPD (3 dirigidos a Endesa y 1 dirigido a su DPO) en tiempo y forma, colaborado y cooperado plenamente con esta Agencia.

(iii) Falta de beneficios obtenidos, prevista en el artículo 76.2 c) de la LOPD-gdd.

Por último, Endesa considera que debería serle de aplicación la circunstancia atenuante recogida en el artículo 76.2 c) de la LOPD-gdd relativo a la falta de beneficios obtenidos como consecuencia de la presunta comisión de la infracción. Esto es así debido a que en ningún momento se ha obtenido ningún beneficio económico por parte de Endesa a resultas de la brecha de seguridad sufrida.

> Más bien al contrario, ha sido la clara perjudicada, puesto que ha visto como terceros extraños a la organización accedían a sus sistemas y a los datos en ellos contenidos con una finalidad ilegítima.
>
> Entre algunos de los efectos perjudiciales que ha sufrido Endesa como consecuencia de la Violación de la Seguridad de los Datos se encuentran: (i) Endesa ha tenido que dedicar importantes recursos para la evaluación, análisis y gestión de la Violación de la Seguridad de los Datos y; (ii) ha requerido la implementación, por parte de Endesa, de mayores medidas de seguridad tanto técnicas como organizativas de cara a tratar de evitar que un ataque de estas características vuelva a suceder, con la inversión que dicha implementación conlleva.
>
> A su juicio, Endesa no se ha beneficiado lo más mínimo de la Violación de la Seguridad de los Datos sino que ha sido, junto con los interesados afectados, la principal perjudicada del mismo. En este sentido, Endesa considera que este hecho debería apreciarse por la AEPD como circunstancia atenuante de la conducta de la entidad firmante de cara a la graduación de la sanción a imponer por la presunta infracción del artículo 32.1 del RGPD.

En primer lugar, respecto a la alegada disparidad de criterios de la AEPD, esta Agencia desea señalar que cada caso es distinto y debe analizarse cada caso concreto según sus propias circunstancias.

El artículo 32.1 del RGPD establece que *"(…) el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (…)".* Es decir, que se debe evaluar la probabilidad y gravedad de los riesgos que entrañan los tratamientos de datos personales que se realicen en el caso concreto, para los derechos y libertades de los interesados, a fin de adoptar las medidas que sean apropiadas a ese caso concreto. No existe para ello una fórmula universal, ni siquiera general, ni tampoco se trata de que se vulnere automáticamente el artículo 32 del RGPD en caso de producirse una violación de la seguridad de los datos personales. Se trata en cada caso de analizar qué riesgos podría acarrear para los interesados un tratamiento determinado y analizar qué medidas se habrían implementado para evitar que tal riesgo se produjera, a fin de determinar si tales medidas serían o no las apropiadas para ese caso concreto.

Teniendo esto en cuenta, esta Agencia decidió archivar las actuaciones en los citados procedimientos E/008809/2019 y E/05937/2021, dado que en ninguno había evidencias de que las medidas adoptadas por los responsables de tratamiento, antes del incidente y una vez producido éste, no fueran las apropiadas en función del riesgo existente en esos tratamientos. En el caso de ENDESA, esto no es así, las medidas adoptadas con anterioridad no eran las apropiadas en función del riesgo para los derechos y libertades de los interesados, por lo que esta Agencia decidió iniciar un procedimiento sancionador a fin de sancionarle por una posible infracción del artículo 32 del RGPD, entre otras.

En cuanto a la dilación en la notificación a esta Agencia de la violación de la seguridad de los datos personales, en el procedimiento E/05937/2021, el artículo 33.1 del RGPD dispone que: *"(…) Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación*". En el

citado procedimiento la responsable de tratamiento indicó debidamente los motivos de la dilación en la notificación a la autoridad de control, por lo que no se consideró infringido tal artículo, a contrario de lo que ocurre con ENDESA en el presente procedimiento, que transcurrieron meses desde que debió notificarse el incidente a esta Agencia sin que hubiera un motivo que justificara tal retraso, tal y como se razonó fundadamente en la respuesta a la alegación segunda del escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador.

En cuanto al procedimiento PS/00118/2020, el incidente (que duró solo tres días y afectó a 75.000 interesados máximo, frente al incidente de ENDESA que duró meses y afectó a millones de interesados, contrariamente a lo que sostiene ENDESA) y se consideró que el grado de reprochabilidad de la actuación del responsable de tratamiento permitía sustituir la imposición de una multa por un apercibimiento, lo cual no ocurre en el presente procedimiento sancionador contra ENDESA.

Respecto al procedimiento PS/00254/2019, ocurre algo similar, toda vez que el incidente en cuestión no afectó a millones de personas y las circunstancias de la brecha difieren de la actuación tan gravemente negligente de ENDESA,

En segundo lugar, en cuanto a la aplicación de los agravantes, la grave falta de diligencia por parte de ENDESA ha quedado acreditada a lo largo del expediente no con el informe de ******EMPRESA.1***, sino con toda la documentación obrante, todo lo cual se ha reseñado detalladamente en los hechos probados y se ha explicado ampliamente en los fundamentos de derecho, en especial, en la respuesta a las alegaciones aducidas al acuerdo de inicio.

Respecto de la supuesta infracción del artículo 5.1.f) del RGPD, la conducta de ENDESA ha sido gravemente negligente en tanto tardó meses en resetear o eliminar los usuarios comprometidos, lo que permitió que durante meses se pudiera acceder a los datos personales obrantes en los sistemas de ENDESA y se dieran de alta usuarios de forma fraudulenta. También ha sido gravemente negligente a la hora de solicitar a Facebook que se eliminaran los anuncios en cuestión, toda vez que no se dirigió a FACEBOOK IRELAND LIMITED, tal y como se le indicó que era el cauce correcto.

Respecto de la supuesta infracción del artículo 32 del RGPD, la conducta gravemente negligente de ENDESA se aprecia en todo su comportamiento antes y después de producido el incidente, toda vez que ni siquiera se había previsto siquiera la posibilidad de que se hiciera un uso indebido de los usuarios de ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***, por lo que no se había implementado unas medidas adecuadas para asegurar una autenticación de usuarios con las debidas garantías, impidiendo que se produjesen accesos indebidos a los sistemas y posibilitando que se rastree debidamente la actividad de estos usuarios en esos sistemas.

Tampoco se resetearon ni se eliminaron de forma inmediata, ni de ******HERRAMIENTA.1*** ni de ******HERRAMIENTA.2***, los usuarios que se sabía comprometidos, se tardaron meses, lo que propició que durante todo ese tiempo se pudiera acceder indebidamente a los datos personales tratados por ENDESA y facilitó que se realizara un gran número de altas fraudulenta. Tampoco se realizó un reseteo preventivo de todos los usuarios de los sistemas, ante una posible amenaza (que luego resultó ser cierta).

Además, pese a lo acordado el 13 de septiembre de 2021 por el Comité de Brechas de Seguridad y de la medida adoptada en agosto de 2021 de solicitar la baja de los anuncios de Facebook donde se ofrecen accesos, ENDESA no siguió o indicado por FB SPAIN, y no se dirigió a FACEBOOK IRELAND LIMITED por ninguno de los medios ofrecidos para que elimine los anuncios publicados en los que se ofertaban los accesos a sus sistemas.

Respecto de la supuesta infracción del artículo 33 del RGPD, la negligencia grave por parte de ENDESA se aprecia en que tardó meses en identificar la violación de la seguridad de los datos personales en cuestión como notificable a la autoridad de control.

Y respecto de la supuesta infracción del artículo 34 del RGPD, la negligencia grave por parte de ENDESA se aprecia en que no identificó debidamente que el incidente en cuestión debía ser comunicado a los afectados. ENDESA ni siquiera comunicó la quiebra a los afectados por las posibles altas fraudulentas y, además, una vez esta Agencia le ordenó emitir el correspondiente comunicado, ni siquiera se informó debidamente.

En cuanto a la afirmación de ENDESA de que cuando se había dirigido a Facebook Spain ya se habían deshabilitado las credenciales de los usuarios comprometidos, ello no es correcto, tal y como se ha contestado en la respuesta al apartado b) de la alegación previa del escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador.

Respecto a que ENDESA demostró que realizó la notificación del incidente a esta Agencia en el plazo de 24 horas desde que tuvo constancia de que podía suponer un riesgo para los derechos y libertades de los interesados, esta Agencia se remite a lo contestado a la alegación tercera del escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador.

Tampoco ha demostrado ENDESA que no podía derivarse de este incidente un alto riesgo para los derechos y libertades de los interesados ni que hubiera facilitado debidamente a los interesados la información requerida por el artículo 34 del RGPD, tal y como se ha contestado a las alegaciones segunda y tercera del escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador.

En tercer lugar, respecto a que se considere como agravante el hecho de que la actividad de ENDESA esté vinculada a la realización de tratamientos de datos personales, esta Agencia desea señalar que el artículo 83.2 del RGPD dispone que "*Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: (…) k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso…".*

En este sentido, el legislador español ha considerado incluir en el artículo 76 de la LOPDGDD que: "*2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:*

(…)

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

Esta Agencia simplemente toma en consideración esa circunstancia, prevista por el legislador, a la hora de decidir la imposición de la multa administrativa.

Cabe destacar que, por supuesto, no puede tener a los efectos de decidir la imposición de una multa administrativa la misma consideración una infracción producida por una persona física o una empresa pequeña no habituada al tratamiento de datos personales, que una gran empresa como ENDESA, acostumbrada al tratamiento de datos personales de millones de clientes y no clientes, con una larga trayectoria a sus espaldas al respecto. Por supuesto que se considera que la infracción es más grave a los efectos de imponer una multa si el responsable del tratamiento se encuentra entre los segundos, como es el caso de ENDESA. Así lo ha señalado la Audiencia Nacional en su SAN 65/2017, de siete de febrero de dos mil diecisiete, al recoger la doctrina del Tribunal Supremo, "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 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 exquisito cuidado por ajustarse a las prevenciones legales al respecto".

En cuarto lugar, haber revisado las contrataciones realizadas por ******EMPRESA.9*** para evitar nuevas altas fraudulentas, no puede ser considerado una atenuante, cuando es una obligación impuesta por la normativa. Por su parte, el hecho de haber adoptado a posteriori determinadas medidas de seguridad para mitigar los riesgos, ya se ha valorado como una atenuante de la supuesta infracción del artículo 32 del RGPD.

En quinto lugar, no resulta de aplicación la atenuante relativa al grado de cooperación con la autoridad de control, toda vez que ya se ha explicado ampliamente que habían transcurrido más de 24 horas (meses, de hecho) desde que ENDESA tuvo conocimiento de que se había producido una violación de la seguridad de los datos que era notificable (esta Agencia se remite a la respuesta a la alegación segunda del escrito de alegaciones al acuerdo de inicio del presente procedimiento sancionador).

En cuanto a que ENDESA ha contestado cada uno de los requerimientos de información enviados por esta Agencia, no se considera atenuante dado que se trata de una obligación contemplada en la normativa aplicable.

En este sentido, el artículo 52 "*Deber de colaboración*" del RGPD dispone que: "1*. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación. (…)"*

Y el artículo 72 "*Infracciones consideradas muy graves*" establece que: "*1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una de esta ley orgánica cuando la misma sea exigible.*

> *(…)*
> *ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación. (…)"*

Por último, esta Agencia desea señalar que no puede considerarse la falta de beneficios obtenidos por parte de ENDESA como una atenuante.

Ello de acuerdo con la Sentencia de la Audiencia Nacional, de 05/05/2021, rec. 1437/2020, que indica: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante*". Aplicado al presente procedimiento sancionador, la falta del presupuesto para su aplicación respecto del art. 76.2.c) de la LOPDGDD, esto es, obtener beneficios consecuencia de la infracción, no permite su aplicación como atenuante.

Este criterio de graduación se establece en la LOPDGDD de acuerdo con lo previsto en el artículo 83.2.k) del RGPD, según el cual las multas administrativas se impondrán teniendo en cuenta cualquier "factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción", entendiéndose que evitar una pérdida tiene la misma naturaleza a estos efectos que la obtención de beneficios.

Si a esto se añade que las sanciones deberán ser "en cada caso individual" efectivas, proporcionadas y disuasorias, conforme a lo previsto en el artículo 83.1 del RGPD, admitir la ausencia de beneficios como una atenuante, no solo es contrario a los presupuestos de hecho contemplados en el artículo 76.2.c), sino también contrario a lo establecido en el artículo 83.2.k) del RGPD y a los principios señalados.

Así, valorar la ausencia de beneficios como una atenuante anularía el efecto disuasorio de la multa, en la medida en que minora el efecto de las circunstancias que inciden efectivamente en su cuantificación, reportando al responsable un beneficio al que no se ha hecho merecedor. Sería una rebaja artificial de la sanción que puede llevar a entender que infringir la norma sin obtener beneficios, financieros o del tipo que fuere, no le producirá un efecto negativo proporcional a la gravedad del hecho infractor.

En todo caso, las multas administrativas establecidas en el RGPD, conforme a lo establecido en su artículo 83.2, se imponen en función de las circunstancias de cada caso individual y no se estima que la ausencia de beneficios sea un factor de graduación adecuado y determinante para valorar la gravedad de la conducta infractora.

Por todo lo anteriormente expuesto, se desestima la presente alegación.

Alegaciones a la propuesta de resolución del procedimiento sancionador

En relación con las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por ENDESA:

Previa.- Concreción de determinados puntos fácticos esenciales para el análisis jurídico del expediente

Se reitera ENDESA en que en la citada propuesta de resolución esta Agencia existen cuestiones que, siendo muy relevantes para el enjuiciamiento de la conducta de Endesa, no han sido interpretadas por la AEPD de manera correcta.
a
(a) De la importancia que tuvo y tiene tanto el incidente como la protección de los datos de carácter personal para Endesa

Se alega que el incidente y violación de la seguridad de los datos sufrida por Endesa, que tuvo como consecuencia la notificación de la misma a la AEPD, fue tratada desde el primer momento con el máximo rigor y seriedad, y se le prestó la máxima atención en todos los análisis que se realizaron. La seguridad de la información es un asunto de vital importancia para Endesa.

Aunque la Propuesta de Resolución hace referencia a una "*escandalosa falta de diligencia*" de Endesa a la hora de gestionar e implementar medidas de remediación de la violación de la seguridad de los datos y a pesar de que el órgano instructor del expediente sigue aplicando a las sanciones propuestas la agravante de "*grave falta de diligencia*", el control de los datos de sus clientes es, para Endesa, una cuestión estratégica fundamental y a la que dedica una enorme cantidad de recursos económicos y humanos.

La importancia y seriedad con que se afrontó el incidente se refleja, no solo ya en la notificación de la violación de la seguridad a la AEPD y en la colaboración que Endesa ha venido prestando a la AEPD desde el inicio del expediente, sino también en las medidas de investigación, contención y remediación que se desplegaron en su momento. Minusvalorar estos esfuerzos y estas medidas tal y como, a juicio de esta parte, hace la Propuesta de Resolución por el mero hecho de que la AEPD no comparta la interpretación, completamente razonable, que Endesa ha hecho de la normativa de protección de datos aplicable, atenta contra el principio de responsabilidad que debe regir el procedimiento administrativo sancionador.

En este sentido es requisito esencial, y así lo viene recogiendo la jurisprudencia, que en la conducta de Endesa concurra el elemento subjetivo de la culpabilidad, sea a título de dolo (intencionalidad) o de negligencia (imprudencia). Lo que no cabe ni es admisible es sancionar sin que concurra ninguna culpabilidad, por simple responsabilidad objetiva, como hace la Resolución Sancionadora en algunos puntos que más adelante se expondrán.

Adicionalmente, se señala la importancia de que, en el marco de un expediente sancionador como el que nos ocupa, se realice, con anterioridad a la propuesta de imposición de sanciones económicas tan cuantiosas como las que AEPD propone imponer a Endesa, un análisis jurídico riguroso y objetivo respecto de la obligación de notificación, la calificación jurídica de unas determinadas medidas de seguridad implementadas antes y después del incidente y los hechos, para determinar si éstos constituyen o no una infracción administrativa de incumplimiento del RGPD, que no es una consecuencia automática de un incidente.

ENDESA ha intentado en todo momento argumentar con rigor jurídico y de forma objetiva sobre todo lo anterior, por lo que entiende que no resulta procedente frivolizar sobre este aspecto y confundir lo que es la defensa jurídica legítima en un procedimiento como el presente con la importancia o seriedad que la entidad le asigna a los hechos subyacentes que, como se ha dicho, es máxima.

Al respecto, esta Agencia desea señalar que no cuestiona que la seguridad de la información no sea un asunto importante para ENDESA. Simplemente se trata de que, en el presente caso, esta Agencia considera que ENDESA no ha obrado con la debida diligencia con que debía.

Tampoco esta Agencia minusvalora los esfuerzos realizados por ENDESA, pero el hecho de notificar la violación de la seguridad de los datos a la AEPD, así como contestar a los requerimientos de información enviados por esta Agencia y las medidas de "investigación, contención y remediación" adoptadas por ENDESA, no son sino obligaciones que la normativa aplicable al tratamiento de datos personales impone a ENDESA y no un reflejo de "la importancia y seriedad con que se afrontó el incidente".

En cuanto a que esta Agencia pretende sancionar a ENDESA por simple responsabilidad objetiva, tal afirmación no puede ser más que rechazada. La existencia del requisito del elemento subjetivo de la infracción ha quedado debidamente acreditada en el expediente, así como en la respuesta a las alegaciones de ENDESA al acuerdo de inicio del presente procedimiento sancionador y se detallará en la respuesta a las presentes alegaciones así como en los fundamentos de derecho de la presente resolución.

También desea señalar esta Agencia que por supuesto que en el presente caso realizó un análisis jurídico riguroso y objetivo respecto de la obligación de notificación, la calificación jurídica de unas determinadas medidas de seguridad implementadas antes y después del incidente y los hechos, para determinar si éstos constituyen o no una infracción administrativa de incumplimiento del RGPD.

Por último, esta Agencia remarca que en ningún momento ha frivolizado sobre la presente cuestión ni le resta importancia o seriedad a los hechos subyacentes, que es máxima.

Por lo expuesto, se desestima la presente alegación.

a (b) De la impugnación expresa, de nuevo, de la totalidad del informe de evaluación y gestión de brecha de seguridad elaborado por ***EMPRESA.1 ("***EMPRESA.1"):

b

Se reitera ENDESA en la impugnación del informe aportado por la entidad ***EMPRESA.1**, dado que considera que dicho informe no se puede tomar en consideración a efectos del presente expediente sancionador.

Indica que no se trata de un informe pericial, ni de un informe jurídico, ni técnico, objetivo, sino de un informe parcial (en el sentido de informe de parte interesada), ya que ***EMPRESA.1** estuvo implicada en el propio incidente y, de hecho, el mismo trajo causa, en parte, de su incumplimiento a la hora de controlar y supervisar el cumpli-

miento, por parte de ***EMPRESA.9 (“***EMPRESA.9”), de las instrucciones de Endesa y de sus obligaciones como subencargado del tratamiento. De hecho, ***EMPRESA.1 nunca acreditó que ese informe existiese o fuese compartido con Endesa en la fecha en que supuestamente fue firmado y, viéndolo en perspectiva, se aprecia claramente (a su juicio) que es un informe “defensivo” confeccionado por una entidad que necesita proteger sus intereses frente a posibles reclamaciones de responsabilidad, al haber actuado como encargada del tratamiento de Endesa y poder tener algún grado de responsabilidad en el acaecimiento de los hechos que han dado lugar, en última instancia, al presente procedimiento.

Por lo tanto, aunque en la Propuesta de Resolución la AEPD indica que sus conclusiones se basan, “*no sólo en el informe realizado por* ***EMPRESA.1 *el 4 de noviembre de 2021, sino en toda la información de la que ha tenido conocimiento a largo (sic) del presente procedimiento*”, vuelve mencionar este informe (impugnado por ENDESA) en el antecedente trigésimo primero (páginas 38 a 40), incluyéndolo como parte del expediente, y vuelve a utilizar el mismo para apoyar (apenas sin otro fundamento objetivo) su tesis de que una de las consecuencias del incidente podía ser el corte de suministro (“*quod non*” puesto que, no solo la rápida actuación de Endesa, sino los propios procesos existentes de acuerdo con la normativa del sector, determinan la imposibilidad de un corte de suministro en los términos que sorprendentemente señala ***EMPRESA.1 y acoge de forma acrítica e infundada la AEPD).

Por último, interesa a Endesa aclarar que el objeto de esta alegación no es tratar que la AEPD enjuicie las acciones de ***EMPRESA.1 ni reprochar la propia actuación de ***EMPRESA.1 como parece indicar la Propuesta de Resolución al inicio de su página 67 y en su página 78 (quien debe hacerlo, si así lo considera necesario, es la propia AEPD), sino: (i) exponer la parcialidad y falta de rigor de un documento obrante en el expediente en el que la AEPD, tal y como ha quedado acreditado, se apoya para reforzar o justificar la imposición a Endesa de las sanciones propuestas; e (ii) impugnar la totalidad de su contenido.

Al respecto, en primer lugar esta Agencia desea señalar que por supuesto que corresponde a la AEPD valorar si la actuación de ***EMPRESA.1 fue conforme a la normativa de protección de datos personales. Y que la interpretación que realiza ENDESA sobre la actuación de ***EMPRESA.1 y sobre el sentido de lo manifestado por la AEPD en la propuesta de resolución no deja de ser una interpretación.

En segundo lugar, esta Agencia desea aclarar que el citado informe se menciona en los antecedentes toda vez que, en el marco de las actuaciones previas realizadas por esta Agencia a fin de determinar la existencia de una posible infracción de la normativa de protección de datos personales por parte de ENDESA en lo que respecta al incidente objeto del presente procedimiento, se le requirió información a ***EMPRESA.1, la cual fue debidamente proporcionada a esta Agencia. Por eso este informe forma parte del expediente, dado que fue una de las actuaciones realizadas por esta Agencia en el marco de la investigación que dio lugar al presente procedimiento sancionador.

El hecho de que el citado informe fuera compartido por ***EMPRESA.1 con ENDESA, resulta irrelevante a tales fines. La valoración de ENDESA sobre el informe en cuestión, en cuanto a su imparcialidad e interés de parte, en nada modifican las conclusiones de esta Agencia que no se basan exclusivamente en el referido informe.

Así, la posibilidad que ha tenido en cuenta esta Agencia, de un corte de suministro por impago al realizar un alta fraudulenta, no es una conclusión a la que esta Agencia no hubiera llegado de no existir el informe de ***EMPRESA.1**. No se trata de que dicho corte fuera inmediato, pero es una posibilidad más que evidente y a la que cualquier análisis habría llegado, de que podría haberse llegado a tal situación, de no abonarse las facturas de los suministros dados de alta fraudulentamente.

Por lo expuesto, se desestima la presente alegación.

(c) Interacciones con Facebook para solicitar la retirada de los anuncios a través de los cuales se ofrecía la venta/alquiler de credenciales de acceso a los sistemas de Endesa:

Alega ENDESA que, de conformidad con la Propuesta de Resolución, el hecho de que Endesa no remitiese ninguna comunicación a Facebook Irlanda "*constituye una negligencia grave por parte de ENDESA*". Incluso, la AEPD reitera, a lo largo de la Propuesta de Resolución, que el hecho de que Endesa no se dirigiese a Facebook Irlanda por ninguno de los medios ofrecidos para que esta eliminase los anuncios a través de los cuales se ofertaban los accesos a los sistemas de Endesa constituye una actuación "*gravemente negligente*" que incluso es merecedora de una circunstancia agravante.

Se sorprende ENDESA de que la AEPD utilice esta decisión de Endesa, tomada conscientemente y de forma totalmente razonada (a su juicio), para tratar de justificar que la actuación de Endesa ha sido gravemente negligente. Y ello por dos razones principalmente:

i) La decisión se tomó de manera consciente y razonada por Endesa, por razones ajenas a las expuestas por la AEPD en la Propuesta de Resolución. Es decir, aunque la AEPD utilice la Propuesta de Resolución para presentar un análisis sobre el rol que desempeñan, desde un punto de vista de protección de datos, Facebook España y Facebook Irlanda respecto de los datos que tratan, llegando a concluir que Facebook Irlanda sería el responsable del tratamiento de los datos personales a nivel europeo, lo cierto es que: (a) en ningún momento Endesa ha negado este hecho ni pretende decidir quién es el responsable del tratamiento (como da a entender la Propuesta de Resolución en su página 69); y (b) en ningún caso Endesa se ha planteado presentar una reclamación de protección de datos contra Facebook, por lo que el análisis realizado por la AEPD en la Propuesta de Resolución carece totalmente de relevancia para el enjuiciamiento de este caso.

   En este sentido, cuando desde Endesa se indicaba, en el escrito de alegaciones al Acuerdo de Inicio, que no deseaba reconocer "*la jurisdicción irlandesa, lo que implicaría, en caso de ser necesario, tener que dirigir cualquier reclamación ante los tribunales irlandeses, lo que resultaba, y resulta, una carga inapropiada e injusta"*, no se hacía a efectos de protección de datos, sino a efectos de una posible reclamación judicial o administrativa frente a Facebook por la posible comisión de una infracción o delito de revelación de secretos o de propiedad intelectual.

Sin perjuicio de que, tal y como se ha indicado anteriormente, el análisis sobre quién ostentaría el rol de responsable del tratamiento respecto de los datos tratados por Facebook (Facebook Irlanda o Facebook España) que hace la AEPD en la Propuesta de Resolución no debería ser tenido en cuenta a efectos de enjuiciar la conducta de Endesa puesto que dicho análisis resulta del todo irrelevante a los efectos de la decisión tomada por Endesa en su día y, por tanto, no se le puede achacar la realización de dicho análisis de manera errónea, resulta sorprendente que la AEPD siquiera insinúe que dicho análisis debería ser realizado por Endesa.

Da la impresión de que la AEPD, en una cuestión tan sumamente compleja y que ha sido objeto de numerosos debates jurisprudenciales tanto a nivel nacional como europeo como es la determinación sobre quién actúa como responsable del tratamiento de los datos personales que Facebook recaba a nivel europeo, achaca a Endesa no haber realizado el correspondiente análisis cuando exigir su realización sería una carga totalmente desproporcionada e injusta.

ii) La eliminación de los anuncios de Facebook, tal y como ya se expuso en las alegaciones al Acuerdo de Inicio, no tenía ninguna utilidad práctica de cara a la protección de los derechos y libertades de los interesados afectados, puesto que las credenciales de ******HERRAMIENTA.2*** y ******HERRAMIENTA.1*** comprometidas, excepto una, ya habían sido deshabilitadas (como se expondrá en la alegación primera, a continuación). Tras dicha deshabilitación, desaparecería la posibilidad de acceder a los datos responsabilidad de Endesa almacenados en sus herramientas (aunque las credenciales originales se vendan/alquilen), por lo que el efecto que tiene la desaparición de los anuncios de Facebook sobre los derechos y libertades de los interesados afectados sería nulo.

En este sentido, considera Endesa que no se le puede achacar una grave falta de diligencia desde el punto de vista de la protección de los datos por el mero hecho de no dirigirse ante Facebook Irlanda para exigir la retirada de los anuncios, puesto que su retirada no hubiese tenido (en su opinión) efecto alguno sobre los interesados afectados por la violación de la seguridad de los datos.

En resumen, Endesa considera que la AEPD sustenta gran parte de su argumentación sobre la presunta falta de diligencia de Endesa en un aspecto del incidente que, de haberse realizado tal y como la AEPD propone, no hubiese supuesto ningún beneficio adicional para los derechos y libertades de los interesados.

En primer lugar, esta Agencia desea señalar que sólo es competente para valorar si ENDESA cumplió con la normativa de protección de datos personales. No para valorar cuestiones vinculadas a la propiedad intelectual. En este sentido, en el presente caso, se había publicado una serie de anuncios ofreciendo acceso a los sistemas de ENDESA, que permitía el acceso a datos personales titularidad de ENDESA, que trataba en su calidad de responsable de tratamiento. Y como tal, debió adoptar una serie de medidas, entre otras, que tales anuncios fueran retirados, tal y como se decidió en agosto de 2021, debido al riesgo que entrañaban. Sin embargo, Endesa no acudió a Facebook Irlanda. Ha de tenerse en cuenta que en esa fecha no se encontraba habilitada la autenticación multifactor que no se adopta hasta abril de 2022.

En segundo lugar, en ningún momento se pretende que ENDESA realice ningún análisis sobre el rol de Facebook como responsable de tratamiento de los datos personales, toda vez que los datos objeto del incidente en cuestión es ENDESA. Además, conviene recordar que es la propia Facebook Spain la que le indica que esta cuestión es competencia de Facebook irlanda

Simplemente se trataba de retirar los anuncios publicados, lo cual debió solicitarse a Facebook Irlanda, lo cual ni siquiera se intentó en ningún momento.

En tercer lugar, se le achaca a ENDESA una negligencia grave en su conducta, pero no únicamente por no contactar con Facebook Irlanda, lo cual ha sido ampliamente explicado en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento y detallado en los fundamentos de derecho de la presente resolución.

Por último, en cuanto a la irrelevancia de que siguieran publicados los citados anuncios, esta Agencia estaría de acuerdo si no fuera porque ENDESA no desactivó los usuarios comprometidos hasta pasado más de un mes y porque tampoco tenía la certeza de que los usuarios comprometidos fueran únicamente aquéllos de los que tenía conocimiento (como se ha indicado anteriormente no se encontraba habilitada la autenticación multifactor ni otra medida equivalente, por lo que resultaba necesario el auxilio de Facebook para retirar los anuncios en cuestión.

Por todo lo expuesto, se desestima la presente alegación.

Primera.- De la improcedencia de la sanción impuesta por presunta infracción de los artículos 5.1. f) y 32 del RGPD

1. De la implementación de medidas de seguridad adecuadas al riesgo

La AEPD, en la Propuesta de Resolución, achaca a Endesa un retraso a la hora de resetear o deshabilitar ciertos usuarios cuando, de conformidad con la información facilitada en el expediente del caso, Endesa ya conocía que habían sido comprometidos.

Sin embargo, alega ENDESA que esto no es así. Y no es así porque:

(i) A juicio de ENDESA, se ha demostrado que muchas de las cuentas de usuario comprometidas se deshabilitaron casi inmediatamente después de tener constancia de que dichos usuarios podían haberse visto comprometidos.

A modo únicamente de ejemplo y acudiendo a la sección de “Hechos Probados” de la Propuesta de Resolución, se comprueba que:

a (a) El 1 de septiembre de 2021, ******EMPRESA.16*** informa a Endesa de que ha reconocido a una de las personas que ha publicado un anuncio en Facebook a través del cual se ofrecen credenciales de acceso a ******HERRAMIENTA.1*** y Endesa, solo 2 días después, el 3 de septiembre, procede a deshabilitar a dicho usuario “******USUARIO.3***”;

b (b) El 10 de septiembre de 2021, Endesa envía un correo a ***EMPRESA.15** a través del cual le informa de que ha identificado a un empleado como presunto usuario que publica anuncios en Facebook y Endesa, ese mismo día, procede a deshabilitar a dicho usuario "***USUARIO.8**", así como a eliminar el mismo de los sistemas de ***HERRAMIENTA.2**; y

c (c) El 21 de septiembre de 2021, Endesa recibe un correo a través del cual se le informa de la identificación de una de las personas que estaba poniendo a la venta credenciales de Endesa en Internet y Endesa, ese mismo día, procede a deshabilitar a dicho usuario "***USUARIO.5**".

Respecto de los puntos (a) y (c) anteriores, y aunque la AEPD señale que estos usuarios no se eliminaron de ***HERRAMIENTA.2** hasta el 12 de enero de 2022, reitera ENDESA, tal y como señaló en el escrito de alegaciones al Acuerdo de Inicio, que una vez deshabilitada o reseteada la cuenta de cada usuario, éste no puede acceder a la misma ni utilizarla para ninguna finalidad, quedando expulsado permanentemente del sistema, por lo que aunque la cuenta no se haya eliminado, al usuario se le impide acceder a la misma.

Lo mismo ocurre con la fecha de último acceso. El hecho de que la fecha de último acceso sea posterior a la fecha de deshabilitación o reseteo del usuario no significa que la persona cuyo usuario se ha reseteado haya vuelto a acceder a los sistemas de Endesa, si no que puede responder a posibles accesos al usuario por parte de los propios equipos de Endesa que se encuentran investigando el incidente o por parte de nuevos comerciales a los que se les ha asignado dicho usuario.

Al respecto, esta Agencia desea señalar que, en la información proporcionada a esta Agencia y que obra en el expediente, no figura la fecha en que los usuarios de ***HERRAMIENTA.2** comprometidos fueron deshabilitados o reseteados, sino la fecha en que fueron eliminados del sistema.

Tal y como indica el apartado 2 del artículo 5 "Principios relativos al tratamiento" del RGPD, "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).*" En base a este principio, ENDESA ha debido ser capaz de acreditar, a lo largo de los más de 9 meses que duraron las actuaciones previas de investigación y los casi 9 meses de duración del presente procedimiento sancionador, la fecha en que los usuarios de ***HERRAMIENTA.2** comprometidos habían sido deshabilitados o reseteados (tal y como sí se hizo respecto de los usuarios de ***HERRAMIENTA.1**), y no simplemente facilitar la fecha en que tales usuarios fueron eliminados del sistema. Por tanto, esta Agencia desconoce si se deshabilitaron a la vez los usuarios comprometidos de ***HERRAMIENTA.1** y de ***HERRAMIENTA.2**, cuestión que no consta acreditada.

En cualquier caso, esta Agencia considera que la actuación de ENDESA a la hora de deshabilitar y eliminar los usuarios comprometidos (tanto de ***HERRAMIENTA.2** como de ***HERRAMIENTA.1**) ha sido negligente, tal y como se detallará más adelante.

En cuanto a la fecha de último acceso a los sistemas, es cierto que no puede determinarse quién accedió a los sistemas en esa fecha facilitada a esta Agencia. No obstante, esto mismo no hace más que reforzar precisamente la existencia de la infracción

del artículo 32 del RGPD, toda vez que no es posible conocer quién accedió por última vez a los sistemas, al no haber estado configurado debidamente un sistema de logs que permitiera conocer esta información de forma fiable, y el sistema existente permitía mantener varias sesiones iniciadas a la vez, todo lo cual es el objeto del presente procedimiento sancionador.

(i) Alega ENDESA que, en relación con los usuarios comunicados por ******EMPRESA.1*** a Endesa como fraudulentos en fecha 27 de octubre de 2021 (******USUARIO.13, ***USUARIO.14, ***USUARIO.15, ***USUARIO.16 y ***USUARIO.9***), Endesa ha comprobado, tras revisar de nuevo todas las actuaciones realizadas en el marco del incidente, que realmente el primer reseteo de los mismos se produjo el día 29 de noviembre de 2021. Se adjunta, como **Documento número 1**, el email enviado por el equipo de Endesa al ***EMPRESA.18 (…) solicitando, en fecha 29 de noviembre de 2021, el reseteo urgente de estos usuarios.

Como se puede comprobar, ese mismo día 29 de noviembre de 2021 el ***EMPRESA.18 confirma a Endesa que los usuarios han sido reseteados con éxito, adjuntando prueba de ello. Debido a que dicho reseteo, como se ha demostrado, no se llevó a cabo directamente por Endesa sino que se solicitó al ***EMPRESA.18, este no aparecía en la información facilitada a la AEPD en el marco de este expediente.

Por lo tanto, al contrario de lo que indica la AEPD en su Propuesta de Resolución, Endesa no necesitó "*CINCO MESES (sic)*" para resetear o deshabilitar los usuarios comprometidos tras la comunicación de ******EMPRESA.1***, sino que realizó dicho reseteo en el plazo de 1 mes, que fue el necesario para realizar internamente los correspondientes análisis sobre la veracidad de la información proporcionada por ******EMPRESA.1***.

Yendo al detalle de cada de una de las aseveraciones que hace la AEPD en relación a estos usuarios, interesa a Endesa aclarar lo siguiente:

(a) Usuario ******USUARIO.13***: Este usuario fue, tal y como indica la Propuesta de Resolución, inicialmente reseteado por Endesa en fecha 3 de septiembre de 2021 (recordemos, solo 2 días después de que ******EMPRESA.16*** informase a Endesa que el mismo podía estar comprometido). Posteriormente a dicho reseteo, el usuario fue asignado a otro comercial de ******EMPRESA.16***, el cual utilizó este mismo usuario para la realización de contrataciones fraudulentas en octubre de 2021, volviendo a ser reseteado, tal y como ha quedado acreditado, el 29 de noviembre de 2021.

Es decir, al contrario de lo que indica la Propuesta de Resolución, no es que sirviese de poco el reseteo del usuario realizado de manera inicial en septiembre de 2021, sino que ese mismo usuario fue utilizado por un nuevo empleado de ******EMPRESA.16*** para realizar contrataciones fraudulentas en octubre de 2021. Tampoco es cierto que Endesa no volviese a resetear el usuario hasta el 24 de agosto de 2022, sino que, tal y como ha quedado acreditado, lo hizo el 29 de noviembre de 2021.

Una vez más, conviene aclarar, respecto de la eliminación de los usuarios en ******HERRAMIENTA.2***, que esta no se producía en el momento del reseteo del usuario, sino meses más tarde con la finalidad de evitar registros huérfanos y la pérdida

de información comercial crítica, sin que esto signifique que el usuario pueda volver a acceder a la plataforma como parece desprenderse de la Propuesta de Resolución.

(b) Usuario ******USUARIO.15*****: Con este usuario ocurre lo mismo que ocurría con el usuario ******USUARIO.13***** anterior. Es decir, el primer reseteo se produjo el 21 de septiembre de 2021, siendo posteriormente utilizado por un nuevo comercial para la realización de contrataciones fraudulentas. Tras el descubrimiento de estas, se procedió a realizar un nuevo reseteo en fecha 29 de noviembre de 2021. Reitera ENDESA también en este caso lo indicado anteriormente en relación a la eliminación de los usuarios en ******HERRAMIENTA.2*****.

(c) Usuarios ******USUARIO.14, ***USUARIO.16 y ***USUARIO.9*****: Tal y como ha quedado acreditado, estos usuarios se resetearon por primera vez el 29 de noviembre de 2021 (y no el 24 de agosto de 2022 como indica la Propuesta de Resolución), un mes después de que ******EMPRESA.1***** le comunicase a Endesa que a través de dichos usuarios se podrían estar realizando contrataciones fraudulentas. Tal y como se ha indicado anteriormente, este fue el plazo necesario la veracidad de la información proporcionada por ******EMPRESA.1***** y proceder al reseteo de los usuarios identificados.

Lo anterior sirve para acreditar (a juicio de ENDESA), adicionalmente, que, tal y como Endesa indicó anteriormente, todos los usuarios afectados excepto uno ("******USUARIO.1*****") habían sido deshabilitados por Endesa con anterioridad al envío, por parte de ésta, del primer burofax dirigido a Facebook España y que, por tanto, el envío de un nuevo requerimiento a Facebook Irlanda, además de contrario a los intereses de Endesa por lo que se ha expuesto en la alegación previa anterior, carecía de utilidad práctica de cara a la protección de los derechos y libertades de los interesados afectados.

De lo anterior se desprende, a todas luces, que la opinión de la AEPD sobre la "*escandalosa falta de diligencia*" de Endesa es, dicho sea con el mayor respeto y en estrictos términos de defensa, infundada, al no estar soportada, tal y como ha quedado acreditado, por los hechos que tuvieron lugar en el marco de este incidente. Tal y como se ha demostrado en la presente alegación, la mayoría de los usuarios fueron reseteados o deshabilitados casi inmediatamente (el mismo o algunos días después de ser identificados) y el resto un mes después de que ******EMPRESA.1***** le comunicase a Endesa que los mismos podrían estar siendo utilizados para la realización de contrataciones fraudulentas. Estas actuaciones realizadas por Endesa, por tanto, resultan a todas luces diligentes, chocando frontalmente con la interpretación que de las mismas hace, de manera errónea (a juicio de esta parte y dicho sea con todo el respeto), la AEPD (la Propuesta de Resolución menciona retrasos de 4 y 5 meses en el reseteo de usuarios cuando ha quedado demostrado que esto no es así).

Al respecto, esta Agencia desea señalar que el hecho de que la falta de diligencia de ENDESA a la hora de gestionar el incidente en cuestión no se clasifique "escandalosa" a la vista de la nueva información proporcionada junto con las alegaciones a la propuesta de resolución del presente procedimiento sancionador, no implica que la actuación de ENDESA hubiera sido lo suficientemente diligente según lo exigido por la normativa aplicable. Más bien al contrario. En el mejor de los casos, ENDESA misma de-

fiende que tardó UN MES en realizar una acción tan sencilla como el reseteo de los usuarios que su propio proveedor le ha indicado han sido comprometidos (al punto de que se acompañó hasta una denuncia policial junto con los citados correos electrónicos). Aunque se tardara un mes en realizar las investigaciones pertinente para comprobar la veracidad de las informaciones proporcionadas por ***EMPRESA.1, esta Agencia considera que ENDESA debió proceder con la mayor diligencia posible, teniendo en cuenta el volumen de los datos personales objeto de tratamiento así como sus características, en especial cuando ya en la primera reunión del Comité de Brechas de 13 de septiembre de 2021 se había decidido resetear los usuarios que estuvieran comprometidos y se había detectado una serie de vulnerabilidades, para las cuales se proponía ***(…)***, entre otras. Por tanto, conocedora de esta situación, ENDESA debió resetear cuanto antes los usuarios que ******EMPRESA.1*** sabía le comunicó estaban comprometidos, en vez de esperar todo un mes para ello, conducta que entraña una grave falta de diligencia.

En cuanto al envío de ENDESA del burofax a Facebook Irlanda solicitando la retirada de los anuncios que vendían credenciales para acceder a los sistemas de ENDESA, la misma ENDESA reconoce que no se habían reseteado todos los usuarios comprometidos, sino que quedaba al menos uno sin resetear, del cual ENDESA tuviera conocimiento. Y aquí radica el *quid* de la cuestión. El hecho de que ENDESA supiera que un número determinado de usuarios se había visto comprometido y que había sido a través de la venta de credenciales por Facebook mediante anuncios publicados en esa red social, no aseguraba que esos usuarios fueran TODOS los usuarios comprometidos. Es decir, ENDESA desconocía si había más usuarios comprometidos que aquellos comunicados por ***EMPRESA.1 y los que había conocido por su cuenta. Por lo que esta Agencia considera que ENDESA debió realizar todos los esfuerzos a su alcance para solicitar la retirada de estos anuncios y dirigirse a Facebook Irlanda si ello era necesario, tal y como le había indicado Facebook Spain. Y que esto debió hacerse a la brevedad, en cuanto se tuvo conocimiento, y no esperar unos cuantos meses, hasta febrero del año siguiente para ello.

Alega ENDESA, de manera adicional a lo anterior, y aunque la AEPD evite mencionarlo en la Propuesta de Resolución (lo que a todas luces causa indefensión a Endesa), algunas de las conclusiones a las que se llega en el informe pericial de fecha 23 de junio de 2023 aportado a este Expediente, las cuales concuerdan a la perfección con lo alegado por Endesa en este escrito y ponen de manifiesto la máxima diligencia con la que actuó Endesa. Y es que dicho informe, elaborado por un tercero imparcial y con amplios conocimientos del estado de la tecnología y las medidas de seguridad de aplicación en la industria (al contrario de lo que ocurre con el informe aportado por ******EMPRESA.1*** al que la AEPD, como ha indicado, parece dar tanta credibilidad y que esta parte impugna), concluye que:

(i) Durante gran parte del incidente ******HERRAMIENTA.1*** contaba con "*un sistema de recopilación de eventos exhaustivo que permite realizar una traza detallada sobre los datos a los que ha tenido acceso el usuario, e incluso en ocasiones hasta qué elementos de la interfaz ha seleccionado*", lo que le permitía a Endesa tener un mayor control sobre los usuarios y las acciones que estos realizaban en la plataforma;

(ii) "*De acuerdo con las evidencias [Capturas_Borrado****HERRAMIENTA.1**] los usuarios se desactivaron tan pronto como se detectaba que pudieran estar comprometidos*" (el subrayado es nuestro);

(iii) *"…la propia gestión del incidente hasta su categorización como brecha de datos ha sido correcta*" (el subrayado es nuestro);

(iv) *"La implantación de la autenticación multifactor (MFA) se ha completado correctamente en ****HERRAMIENTA.2 y ****PLATAFORMA.1**, así como en otras aplicaciones de ENDESA que gestionan datos de usuarios (como ****USUARIO.17**) impidiendo el acceso de usuarios no autorizados a estos sistemas"* (el subrayado es nuestro); y

(v) *"La gestión de usuarios es correcta, y sistemática, las bajas de usuarios se gestionan en tiempo y forma. Se ha verificado que los usuarios identificados durante la gestión de la incidencia han sido desactivados y que, a partir de dicho momento, no era posible usar estos usuarios para acceder a las aplicaciones, aunque los anuncios publicados siguieran activos en las redes sociales"* (el subrayado es nuestro).

Resulta sorprendente comprobar como la Propuesta de Resolución omite por completo las anteriores conclusiones, las cuales demuestran el buen hacer de Endesa en la gestión del incidente y la máxima diligencia desplegada por esta parte. De hecho, el propio informe acaba concluyendo que: (a) "*la desactivación inmediata de los usuarios comprometidos cuya venta se anunciaba en las publicaciones de FB para el acceso a ****HERRAMIENTA.1** *y/o ****HERRAMIENTA.2** supone la imposibilidad, desde ese momento, de acceder a los sistemas incluso aunque los anuncios de FB siguieran estando activos*" (el subrayado es nuestro); (b) "*la implantación del sistema de autenticación multifactor es una medida de seguridad adicional que previene un posible acceso no autorizado a ****HERRAMIENTA.1** *y/o ****HERRAMIENTA.2***"; y (iii) que las medidas anteriores "*son suficientes para prevenir violaciones similares a la notificada ante la AEPD por parte de ENDESA (sin entrar a valorar las conductas ilícitas que puedan llevar a cabo terceros de mala fe)*" (el subrayado es nuestro).

Como se puede observar, las anteriores conclusiones reflejadas en el informe pericial demuestran, una vez más, lo precisas y veraces que son las alegaciones que, en materia de implementación de medidas de seguridad, ha venido realizando y realiza esta parte en el marco de este expediente. Es por ello que sorprende a Endesa que la AEPD, tras solicitarle el envío de dicho informe forense, no solo no se haga eco de las conclusiones del mismo en la Propuesta de Resolución, sino que contradiga las mismas de manera tan flagrante, manteniendo la propuesta de imposición de una sanción, totalmente desproporcionada, de 1.500.000 euros.

En primer lugar, esta Agencia desea señalar que en ningún momento se le ha causado indefensión a ENDESA. Simplemente esta Agencia se limita a reseñar los apartados del informe pericial en cuestión que resulta pertinente a los fines de la presente resolución.

En cuanto a la observación de ENDESA sobre el informe de ***EMPRESA.1, esta Agencia se remite a lo ya contestado anteriormente.

En cuanto a los apartados que ENDESA ha destacado:

(i) Tal y como ha quedado acreditado a lo largo del presente procedimiento, el sistema ***HERRAMIENTA.1** no contaba con un sistema de recopilación de eventos que permitiera conocer suficientemente las acciones realizadas por los distintos usuarios. De hecho, ya en el primer comité de brechas de septiembre de 2021 se propuso ampliar los logs del sistema para mejorar este aspecto, precisamente. Además, el hecho de que se permitieran varias sesiones activas en simultáneo y la falta de una autenticación multifactor favorecieron precisamente que no se pudiera realizar un seguimiento en condiciones de qué persona detrás de cada usuario estaba realizando según qué cosas.

(ii) En cuanto a que los usuarios se desactivaron tan pronto como se detectó que estaban comprometidos, esto ha quedado acreditado que no fue así. Y la misma ENDESA reconoce que se tardó más de un mes en resetear los usuarios que ***EMPRESA.1** había comunicado que estaban comprometidos. Y que el usuario ***USUARIO.1** se reseteó recién el 15 de febrero de 2022.

(iii) En cuanto a que la gestión del incidente hasta su categorización como brecha de datos ha sido correcta, esta Agencia se limita a comprobar si la actuación de ENDESA ha sido diligente en lo referido a adoptar las medidas de seguridad apropiadas en materia de protección de datos, lo cual no ha ocurrido en el presente caso.

(iv) Esta Agencia no discute que se implantó la autenticación multifactor con posterioridad al incidente en cuestión, más bien al contrario, considera que era una medida necesaria que debió adoptarse por parte de ENDESA muchísimo antes, a fin de evitar incidentes como el que es objeto del presente procedimiento.

(v) Tampoco se discute que una vez los usuarios se desactivaban, no podían acceder a las aplicaciones. Lo que esta Agencia considera es que debieron desactivarse los usuarios con mayor celeridad.

ENDESA entiende que no se puede concluir, como hace la Propuesta de Resolución, que las medidas de Endesa anteriores a la violación de la seguridad incumpliesen el RGPD (prueba de que tal afirmación no es correcta es que tales medidas han estado implantadas durante años con plena eficacia), ni que las medidas de seguridad implementadas con posterioridad al incidente no fueron eficaces para limitar al máximo el impacto que el incidente tuvo sobre los derechos y libertades de los interesados afectados y para evitar que un incidente como el que sufrió Endesa vuelva a producirse. Según una visión finalista, si las medidas de seguridad implementadas por Endesa con anterioridad al incidente fueron suficientes, durante 5 años en el caso de ***HERRAMIENTA.1** y casi 3 años en el caso de ***HERRAMIENTA.2**, para evitar que se produjese una violación de la seguridad de los datos, el hecho de que se produjera una violación con carácter posterior no quiere decir, dado que la garantía de indemnidad de las medidas no existe y el riesgo cero no existe, que las medidas no fueran suficientes.

Al respecto, esta Agencia desea señalar que es consciente que el riesgo cero no existe y desea aclarar que no se está realizando una interpretación finalista. Hay que tener en cuenta que las medidas de seguridad deben adoptarse en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento. Estas circunstancias varían en el tiempo, sobre todo en el momento actual

en el que la evolución de las tecnologías de la información comporta nuevos retos para la seguridad, así las amenazas y los riesgos para los derechos y libertades de los interesados no son los mismas que hace cinco años por eso se hace necesario que el responsable evalúe los nuevos riesgos y aplique medidas para mitigarlos.

En este caso, no existía una autenticación multifactor, era posible que existieran varias sesiones abiertas en simultáneo, no era posible realizar el control de los accesos a los sistemas de ENDESA ni la trazabilidad a través de los logs. Por tanto, no puede afirmarse que las medidas adoptadas por Endesa fueran las adecuadas para evitar accesos indebidos, teniendo en cuenta, ente otras circunstancias, la cantidad de datos que trata, la cantidad de afectados por el tratamiento, la participación de encargados en el tratamiento e incluso el contexto tecnológico.

Además, en cuanto a las medidas relacionadas con la seguridad de los accesos, según consta en el procedimiento Endesa tenía implementada una medida basada en contraseñas. Sin embargo, no implantó un sistema de autenticación complementario hasta abril de 2022 a pesar de que en 13 de septiembre de 2021 el Comité de Brechas de Seguridad, y como consecuencia haber comprobación la veracidad del anuncio publicado en Facebook propuso el establecimiento de un múltiple factor de autenticación, y a pesar de que se publicaran nuevos anuncios en Facebook.

Si ENDESA hubiera tenido adoptadas unas medidas apropiadas para reducir el impacto o evitar que el riesgo se materialice, no existiría infracción por su parte. Es más, si ENDESA hubiera tenido implementadas las medidas que implantó como consecuencia de la violación de la seguridad de los datos personales en cuestión, posiblemente ésta no se hubiera producido y la infracción podría no haber existido. Pero ello no era así, razón por la que se inició el presente procedimiento sancionador. Por lo demás, el hecho de hubieran transcurrido 3 o 5 años sin que se produjera una violación de la seguridad de los datos personales, no implica que las medidas fueran las apropiadas, sino simplemente que no se habían producido accesos indebidos, que es otra cuestión muy distinta.

Por todo lo anteriormente expuesto, se desestima la presente alegación.

2. La eventual imposición de dos sanciones por la supuesta infracción de los artículos 5.1.f) y 32 del RGPD sería contraria a derecho por vulneración del principio de *non bis in idem* o, en su caso, de las normas aplicables en supuestos de concursos de normas punitivas

2.1.- Planteamiento

La Propuesta de Resolución notificada mantiene la imputación simultánea a Endesa de la infracción del artículo 5.1.f) del RGPD y la de su artículo 32, y plantea la imposición de una sanción que asciende, en total, a 4.000.000 de euros.

Alega ENDESA que dichos preceptos consagran, por un lado, el principio de integridad y confidencialidad, que se traduce en la obligación de tratar los datos *"de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o*

daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas" [artículo 5.1.f) del RGPD], y, por otro, la obligación de adoptar *"medidas técnicas y organizativas apropiadas"* para garantizar, entre otros, *"un nivel de seguridad adecuado"* (artículo 32 del RGPD).

Opina ENDESA que, cuanto se ha alegado hasta este momento, unido al material probatorio aportado al expediente, acredita debidamente que las medidas técnicas y organizativas con las que contaba Endesa en el momento en el que se produjo el incidente del que trae causa el presente procedimiento cumplían lo establecido en el artículo 32 del RGPD. Lo que no cabe es exigir que fueran infalibles, que es lo que (a su juicio) pretende la Propuesta de Resolución para justificar el mantenimiento de la imputación realizada a este precepto.

Al respecto, esta Agencia desea señalar que no se pretende que las medidas de seguridad que se adopten para proteger los datos personales sean infalibles, sino que se trata de que sean apropiadas en función del riesgo para los derechos y libertades de los interesados, lo cual no ha ocurrido en el presente caso.

Sin perjuicio de lo anterior, alega ENDESA que, incluso admitiendo a efectos puramente argumentativos que se produjo una infracción del artículo 32 del RGPD, lo que no cabría es, además de sancionar a Endesa por la misma, imponer una sanción adicional por la supuesta infracción del artículo 5.1.f) de dicha norma. Por decirlo de forma gráfica: no cabría imponerle una sanción por supuestamente carecer de medidas adecuadas para garantizar la seguridad de los datos y, además, por no haberse garantizado efectivamente dicha seguridad.

De lo contrario, entiende que se estarían imponiendo dos sanciones por unos hechos que en este caso concreto guardan tal íntima conexión entre sí, por lo que cabe afirmar que ambos se tratan de lo mismo. Y se estarían imponiendo esas sanciones, además, con base en dos normas punitivas que tienen por objeto la protección del mismo bien jurídico, esto es, la garantía de la seguridad de los datos.

Lejos de lo que a este respecto afirma la Propuesta de Resolución en el sentido de que ambos preceptos perseguirían fines distintos (afirmación que, a su juicio, se expone sin el menor respaldo argumentativo), alega ENDESA que, si se examina el RGPD, se extrae fácilmente la conclusión de que siempre sigue la dinámica consistente en que todos los principios relativos al tratamiento de los datos que se contienen en el artículo 5 del RGPD tienen posteriormente su concreción en las obligaciones específicamente impuestas al responsable del tratamiento y el encargado del tratamiento, siendo así que, por lo que se refiere a la seguridad, el principio plasmado en el apartado 1.f) de dicho artículo 5 se materializa en las obligaciones establecidas en el artículo 32 para garantizar un nivel de seguridad adecuado al riesgo.

Afirma ENDESA que el bien jurídico protegido por ambos preceptos es, en suma, exactamente el mismo. Y que nada hay en el artículo 5.1.f) que no se trate de proteger con las obligaciones impuestas al responsable y al encargado del tratamiento en el artículo 32.

Precisamente por ello ENDESA sostiene que, en el caso de imponerse las dos sanciones propuestas, la resolución sancionadora vulneraría frontalmente el principio *non bis*

in idem, lo que determinaría su nulidad de pleno derecho por vulneración del derecho fundamental a la legalidad sancionadora consagrado en el artículo 25 de la Constitución.
Todo ello fue expuesto profusamente en las alegaciones frente al Acuerdo de Inicio, que se dan aquí por reproducidas en aras de una mayor concreción, en las que también se dejó constancia de que, incluso si existieran dudas sobre si concurre o no la triple identidad de sujeto, hecho y fundamento que exige la aplicación del citado principio, lo que es evidente a ojos de ENDESA es que como mínimo nos encontraríamos ante un concurso de normas punitivas que obligatoriamente tendría que resolverse conforme a las reglas normativa y jurisprudencialmente fijadas al efecto, que nunca darían lugar a la imposición de dos sanciones independientes.

Y alega que ninguna de las razones esgrimidas en la Propuesta de Resolución para rechazar estas alegaciones es correcta desde una perspectiva jurídica ni, por tanto, permite mantener el pretendido doble castigo sancionador al que se ha venido haciendo referencia.

Al respecto, esta Agencia desea señalar que no puede estar más en desacuerdo con el análisis realizado por ENDESA respecto a que el principio plasmado en el artículo 5.1.f) del RGPD se materializa en las obligaciones del artículo 32 del RGPD.

Si ello fuera así, no se tipificarían las infracciones a dichos artículos como infracciones diferentes.

Sobre la tipificación de estas infracciones, cabe aclarar, con carácter previo, que la confidencialidad y la seguridad de los datos tienen su reflejo fundamentalmente en dos preceptos independientes del RGDP: en el art. 5.1.f) y en el art. 32 del RGPD.

El artículo 5.1.f) del RGPD es uno de los principios relativos al tratamiento. Los principios relativos al tratamiento son, por un lado, el punto de partida y la cláusula de cierre del ordenamiento jurídico de protección de datos, constituyendo verdaderas reglas informadoras del sistema con una intensa fuerza expansiva; por otro lado, al tener un alto nivel de concreción, son normas de obligado cumplimiento susceptibles de ser infringidas.

Pues bien, el art. 5.1.f) del RGPD recoge el principio de integridad y confidencialidad y determina que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Por ejemplo, la concienciación de los empleados de un responsable del tratamiento respecto de lo que supone e implica para los derechos y libertades de los interesados la garantía del derecho fundamental a la Protección de Datos de Carácter personal no es una medida de seguridad. Es una medida de gestión de cumplimiento normativo que claramente coadyuva a la garantía de la confidencialidad.

Anudar la garantía de la confidencialidad y de la integridad únicamente a medidas de seguridad es una comprensión simplista de lo que impone y significa el RGPD. Y ello porque significa reducirlo a medidas de seguridad, cuando las medidas de seguridad constituyen el último eslabón del círculo, antes de comenzar de nuevo.

Por supuesto que las medidas técnicas u organizativas adecuadas a las que hace mención el artículo 5.1.f) del RGPD pueden ser medidas de seguridad, pero no únicamente.

Por otra parte, el artículo 32 del RGPD reglamenta cómo ha de articularse la seguridad del tratamiento en relación con las medidas de seguridad concretas que hay que implementar, de tal forma que teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluya entre otras cuestiones, pero no sólo, la capacidad de garantizar la confidencialidad de los datos.

Como se puede ver, este precepto, el artículo 32 del RGPD, aunque relacionado con el artículo 5.1.f) del RGDP, como muchos de los artículos del RGPD que también están relacionados, no circunscribe el principio en su totalidad. El artículo 5.1.f) del RGPD exige taxativamente que se garantice la confidencialidad, y requiere para su aplicación una pérdida de confidencialidad. Puede haber supuestos en que existan medidas técnicas y organizativas de seguridad inapropiadas sin que por ello haya una pérdida de integridad y confidencialidad. Pero también puede darse el caso contrario, unas medidas técnicas y organizativas de seguridad apropiadas, y que se haya producido una pérdida de integridad y confidencialidad de los datos personales.

De hecho, la vulneración de cualquiera de dichos preceptos se encuentra tipificada de manera independiente y autónoma en distintos apartados del artículo 83 del RGPD, por lo que la vulneración de ambos preceptos a la vez, tal y como acontece en este supuesto, es posible y algo previsto por el legislador, sin que la vulneración de uno de ellos impida la del otro, lo que además no supone per se conculcar el principio de *non bis in idem*. Además, uno de ellos, el artículo 5.1.f) del RGPD, prevé multas administrativas de hasta 20 millones de euros, quedando esa cantidad reducida a la mitad en el caso del artículo 32 del RGPD.

De igual forma, en la LOPDGDD al recoger la calificación de las infracciones a los solos efectos de la prescripción se encuentran claramente diferenciadas las infracciones muy graves y graves a los efectos de la prescripción bien se trate de la vulneración del artículo 5.1.f) del RGPD o bien se trate de la vulneración del artículo 32 del RGPD respectivamente.

En cuanto a que todos los principios relativos al tratamiento de datos personales y que se citan en el artículo 5 del RGPD tienen su concreción en otro artículo del Reglamento, ello no ocurre con el artículo 5.1.c) del RGPD, que contempla el principio de minimización de datos, y que no tiene su “reflejo” en otro apartado del Reglamento.

Por lo demás, esta Agencia se reitera en lo ya contestado en la propuesta de resolución a las citadas alegaciones al acuerdo de inicio del presente procedimiento sancionador.

Por todo lo expuesto, se desestima la presente alegación.

2.2.- Las razones esgrimidas en la Propuesta de Resolución no pueden conducir a la inaplicación del principio *non bis in idem* o, en su defecto, de las reglas sobre el concurso de normas punitivas

Alega ENDESA que basta una mera lectura de los dos preceptos reputados infringidos por esa Agencia para apreciar su íntima conexión en cuanto al bien jurídico protegido por ambos.

No se trata de que *"puedan estar relacionados"*, como afirma con cierta ligereza (en su opinión) la Propuesta de Resolución, sino de preceptos íntimamente relacionados (a juicio de ENDESA), hasta el punto de que uno representa el planteamiento de un principio y el otro la concreción de las obligaciones para cumplirlo.

En efecto, entiende ENDESA que, mientras el artículo 5.1.f) se refiere a la obligación de garantizar una *"seguridad adecuada"* de los datos personales mediante la aplicación de *"medidas técnicas u organizativas apropiadas"*, el artículo 32 busca la concreción de aquel principio mediante la imposición al responsable y al encargado del tratamiento de la obligación de aplicar *"medidas técnicas y organizativas apropiadas"* para garantizar *"un nivel de seguridad adecuado"*.

Visto de otra perspectiva, pero que, en todo caso, lleva a la misma conclusión, explica ENDESA que el artículo 32 establece una obligación de medios para evitar que se produzca un resultado, y esa obligación consiste en contar con las medidas técnicas u organizativas adecuadas, mientras que el artículo 5.1.f) consagra precisamente el resultado que se pretende conseguir con tales medios, que es garantizar la seguridad e integridad de los datos.

Precisamente por ello difiere ENDESA de lo que afirma la Propuesta de Resolución en el sentido de que la vulneración del artículo 5.1.f) *"puede producirse, o no por ausencia o deficiencia de las medidas de seguridad"*, puesto que cualquier eventual infracción de ese concreto precepto siempre dependerá del tipo de medidas de seguridad que estuvieran implantadas. De hecho, para llegar a esta conclusión lógica basta con reparar en que si las medidas de seguridad fueran infalibles (lo que, obviamente, ni siquiera el RGPD exige, al hacerlas depender de factores como el estado de la técnica, los costes de aplicación, los riesgos, etc.), desde luego nunca se podría vulnerar el citado artículo 5.1.f) del RGPD.

Y si ello es así desde un punto de vista estrictamente jurídico basado en una interpretación integradora del RGPD y respetuosa con la mecánica que éste adopta de plantear principios y establecer las correspondientes obligaciones para garantizarlos, alega ENDESA que más aún lo es en un caso como el que nos ocupa, en el que desde un punto de vista fáctico -y siempre a juicio de esa Agencia- el presunto incumplimiento del artículo 5.1.f) habría respondido a que, supuestamente, las medidas de seguridad eran *"no apropiadas al riesgo"*, es decir, a un presunto incumplimiento del artículo 32.

Ninguna duda puede caber, en supuestos así, de que la eventual infracción del principio de integridad y confidencialidad no sería más que una consecuencia de la previa infracción de la obligación de contar con medidas técnicas y organizativas apropiadas (asumiendo el planteamiento de la Instrucción).

Y precisamente por ello tampoco es correcto a juicio de ENDESA lo que afirma la Propuesta de Resolución notificada en el sentido de que cabe la posibilidad de que una compañía no cuente con medidas adecuadas y que, sin embargo, ello no implique una infracción del artículo 5.1.f) del RGPD, sino solo del artículo 32. Explica ENDESA que un incumplimiento del artículo 32 podrá materializarse o no en una pérdida de confidencialidad y de integridad, pero siempre representará un incumplimiento del artículo 5.1.f), puesto que implicará faltar al principio fundamental de garantizar una seguridad adecuada.

Al respecto, esta Agencia desea señalar que en ningún momento de la citada propuesta de resolución se ha afirmado que el incumplimiento del artículo 5.1.f) del RGPD por parte de ENDESA hubiera respondido a que las medidas de seguridad no eran apropiadas al riesgo. Lo que se afirmó textualmente fue: "*Tomando como referencia lo anteriormente explicitado, en el presente procedimiento sancionador no se ha vulnerado el principio non bis in idem, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una violación de la seguridad de los datos personales, la infracción del artículo 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y de integridad, mientras que la infracción del artículo 32 del RGPD se reduce a la ausencia y deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la violación de la seguridad de los datos personales en cuestión. De hecho, si estas medidas de seguridad (no apropiadas al riesgo, por cierto) que tenía implantadas ENDESA se hubieran detectado por esta Agencia sin que se hubiera producido la pérdida de confidencialidad y de integridad de los datos personales, ENDESA únicamente hubiera sido sancionada por el artículo 32 del RGPD".*

Al contrario, esta Agencia desliga completamente lo que sería la infracción del artículo 5.1.f) del RGPD por no haber garantizado debidamente la confidencialidad e integridad de los datos personales, de lo que es la infracción del artículo 32 del RGPD por no contar con las medidas de seguridad apropiadas (medidas sólo de seguridad). Todo lo cual fue ampliamente explicado en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento sancionador, al cual esta Agencia se remite.

Alega ENDESA que la equivalencia entre el artículo 5.1.f) y el artículo 32 es total, y no puede establecerse entre ambos la forzada independencia o separación que la Propuesta de Resolución sostiene dándola por hecho y sin argumento alguno que lo demuestre. Ambos preceptos protegen (a juicio de ENDESA) el mismo bien jurídico, el primero desde el plano conceptual de los principios y el segundo desde el plano de la especificación de los medios para garantizar su observancia.

Por ello, entiende ENDESA que sancionar su incumplimiento de forma separada supone sancionar dos veces lo mismo, de ahí que la tesis que sigue la Propuesta de Resolución sea contraria al principio *non bis in idem*, que -debería ser innecesario recordarlo- desde un punto de vista material prohíbe que un mismo sujeto sea sancionado dos veces por el mismo hecho; o, cuando menos, contraria a las reglas relativas al concur-

so de normas punitivas, dado que, incluso en el supuesto de que se entendiera que el bien jurídico protegido por ambos preceptos es distinto (*quod non*), lo que jamás cabría poner en duda es que la supuesta infracción del artículo 5.1.f) sería consecuencia inmediata de la infracción del artículo 32 y obedecería a ella, única y exclusivamente, con lo que un solo hecho habría dado lugar a dos infracciones indisolubles.

Afirma ENDESA que lo anterior se ve respaldado por el criterio reiteradamente aplicado por nuestros Tribunales en supuestos en los que han enjuiciado si cabía o no sancionar a un expedientado dos veces por dos infracciones cuando una no era más que la consecuencia de la otra, como -insiste- esa Agencia debería aceptar que sucedería en este caso si no aceptase que no cabe sancionar separadamente el incumplimiento del artículo 5.1.f) y el del artículo 32 del RGPD.

Un criterio jurisprudencial que -en opinión de ENDESA- es plenamente trasladable al supuesto que nos ocupa, pues es la propia Propuesta de Resolución la que reconoce que la supuesta pérdida de confidencialidad e integridad determinante del presunto incumplimiento del artículo 5.1.f) del RGPD obedeció a que las medidas de seguridad implantadas por Endesa no eran apropiadas y, por tanto, al presunto incumplimiento de su artículo 32.

Cita ENDESA como primer ejemplo de esta consolidada jurisprudencia a la Sentencia 2/2003, de 16 de enero, del Tribunal Constitucional, que, siguiendo la línea doctrinal marcada por el Tribunal Europeo de Derechos Humanos, declaró que cuando el examen detenido de unos hechos arroje la conclusión de que un ilícito abarca por sí solo los elementos de los demás ilícitos que una persona haya podido cometer, únicamente cabrá perseguir el primero:

*"(…) existen casos en los que un acto, a primera vista, parece constituir más de un ilícito, mientras que un examen más ***EMPRESA.15 muestra que únicamente debe ser perseguido un ilícito porque abarca todos los ilícitos contenidos en los otros (…)*. *Un ejemplo obvio sería un acto que constituyera dos ilícitos, uno de los cuales contuviera precisamente los mismos elementos que el otro más uno adicional*".

La cita de este precedente viene al caso porque esto mismo sería exactamente lo que ocurriría en el presente supuesto a juicio de ENDESA, en el que es evidente que el presunto incumplimiento del principio de integridad y confidencialidad que se reprocha sería una consecuencia directa del supuesto carácter inapropiado de las medidas de seguridad implantadas por Endesa, con lo que el incumplimiento del artículo 32, que sería previo, absorbería el subsiguiente incumplimiento del artículo 5.1.f). Y ello en la hipótesis de que se considere finalmente por esa Agencia que se trata de preceptos que protegen bienes jurídicos distintos, lo que ENDESA no puede compartir por las razones ya señaladas.

Invoca ENDESA, igualmente, la Sentencia de 30 de junio de 2021, del Tribunal Superior de Justicia de Madrid (ECLI:ES:TSJM:2021:774), en la que se analizaba si era posible sancionar a un sujeto por incumplir una orden de cese de actividad de un local y, al mismo tiempo, porque ese incumplimiento implicó tener abierto dicho local sin licencia de funcionamiento.

El Tribunal consideró que esa dualidad de sanciones no era jurídicamente válida, pues bajo ningún concepto cabe nunca sancionar simultáneamente tanto un resultado (en ese caso, abrir un local careciendo de los permisos necesarios) como la acción de la que ese resultado realmente deriva (incumplir una orden de cese abriendo al público un local sin licencia):

"Esto es, al abrir el establecimiento sin la preceptiva licencia de funcionamiento se está coetáneamente, desobedeciendo la orden de cese y clausura. En definitiva, la comisión de la infracción tipificada en el artículo 37.5 no puede cometerse sin, a la vez, cometer la infracción tipificada en el artículo 37.2, ambos de la LEPAR, y viceversa".

Lo anterior conduce al Tribunal a la conclusión de que existe un *"concurso medial entre ambas infracciones"* y que la imposición de la doble sanción *"resulta vulneradora del principio non bis in idem"*.

Trasladando este criterio a nuestro supuesto de hecho, incluso en la hipótesis de que tuviera que aceptarse que los artículos 5.1.f) y 32 del RGPD no son equivalentes y que, por tanto, sus incumplimientos representarían infracciones distintas (lo que ENDESA bajo ningún concepto puede compartir), de lo que no cabría duda es de que en este caso uno sí habría sido consecuencia del otro, con lo que necesariamente habría que alcanzar igual conclusión que el Tribunal, en el sentido de que la imposición de dos sanciones, en lugar de su castigo conforme a las reglas del concurso medial, vulneraría el principio *non bis in idem*.

Cabe recordar, asimismo, la Sentencia de 13 de mayo de 2004, del Tribunal Superior de Justicia de Madrid (ECLI:ES:TSJM:2004:6240), en la que se enjuició las sanciones impuestas a una empresa por incumplir con las determinaciones de un plan de emergencia y, al mismo tiempo, por haber vertido fuel en las aguas de un puerto como consecuencia de lo anterior.

Dice ENDESA que se trata de un supuesto con el que puede establecerse un absoluto paralelismo porque se había sancionado tanto un concreto resultado (el vertido, equivalente en este caso a la brecha de seguridad) como el hecho que había dado lugar al mismo (en aquella ocasión, el incumplimiento del plan de emergencia, equivalente al incumplimiento de la obligación de disponer de medidas técnicas y organizativas adecuadas).

Pues bien, explica ENDESA que lo relevante a estos efectos es que el Tribunal rechazó la posibilidad de sancionar ambas conductas de forma separada al entender que la conexión existente entre las mismas obligada a considerarlas como una sola a efectos punitivos:

"La lectura detallada de ambos expedientes pone de manifiesto que la conexión entre los hechos perseguidos en ambos es absoluta y que, en todo caso, el incumplimiento del plan de contingencias y la presencia de fuel en el tanque de lastre constituyen los presupuestos fácticos y culpabilísticos de ambas sanciones."

A juicio del Tribunal *"lo relevante no es tanto que puedan identificarse dos conductas distintas, sino qué grado de relación o conexión existe entre las mismas"*, siendo así que, al derivar un hecho del otro, existía una *"evidente relación medial entre una con-*

ducta y otra (el vertido se produjo porque había fuel-oil en un tanque de lastre y la presencia del combustible en dicho tanque tuvo lugar porque se incumplió el plan de contingencias)".

Esto es exactamente lo mismo que ocurre en este supuesto, a juicio de ENDESA.

Alega ENDESA que, más allá de la discusión jurídica sobre si los preceptos cuya infracción se imputa a ENDESA son equivalentes -como esta parte defiende desde el más absoluto convencimiento- o, por el contrario, pueden teóricamente vulnerarse de manera autónoma -como sostiene la Propuesta de Resolución notificada-, a lo que debe atenderse desde una perspectiva sancionadora en supuestos como este es a si existe o no una conexión o relación consecuencial entre las conductas que se reputan ilícitas.

Y en este caso, en opinión de ENDESA, dicha conexión es más que evidente, porque, incluso si el principio de integridad y confidencialidad realmente se hubiera visto lesionado, habría sido porque, supuestamente, se habría incumplido la obligación de contar con medidas adecuadas para garantizarlo, existiendo así una *"evidente relación medial entre una conducta y la otra"*, utilizando las mismas palabras que el Tribunal Superior de Justicia de Madrid.

Alega ENDESA que todo lo expuesto, en definitiva, acredita la imposibilidad de que en el presente expediente se sancione por separado la supuesta infracción de los artículos 5.1.f) y 32 del RGPD, pues la primera no sería más que la consecuencia de la segunda y, por tanto, conforme a la jurisprudencia expuesta, se estaría vulnerando el principio *non bis in idem* o, como mínimo, las reglas propias del concurso de normas punitivas.

Alega ENDESA que, más allá de la discusión jurídica sobre si los preceptos cuya infracción se imputa a ENDESA son equivalentes -como esta parte defiende desde el más absoluto convencimiento- o, por el contrario, pueden teóricamente vulnerarse de manera autónoma -como sostiene la Propuesta de Resolución notificada-, a lo que debe atenderse desde una perspectiva sancionadora en supuestos como este es a si existe o no una conexión o relación consecuencial entre las conductas que se reputan ilícitas.

Y en este caso, en opinión de ENDESA, dicha conexión es más que evidente, porque, incluso si el principio de integridad y confidencialidad realmente se hubiera visto lesionado, habría sido porque, supuestamente, se habría incumplido la obligación de contar con medidas adecuadas para garantizarlo, existiendo así una *"evidente relación medial entre una conducta y la otra"*, utilizando las mismas palabras que el Tribunal Superior de Justicia de Madrid.

Al respecto, esta Agencia desea señalar que la jurisprudencia citada por ENDESA no resulta aplicable al caso. No se trata en el presente caso de un ilícito que abarca por sí solo los elementos de los demás ilícitos (como en la Sentencia 2/2003, de 16 de enero, del Tribunal Constitucional), toda vez que, tal y como se explicó en la respuesta a las alegaciones al acuerdo de inicio, se trata de cuestiones distintas: mediante el artículo 5.1.f) del RGPD se sanciona una pérdida de integridad y confidencialidad, únicamente, y mediante el artículo 32 del RGPD la ausencia y deficiencia de las medidas de

seguridad implantadas por el responsable del tratamiento. Medidas de seguridad ausentes o deficientes que, en sí, infringen el RGPD independientemente de que no se hubiera producido la pérdida de confidencialidad.

Tampoco se trata de sancionar un resultado y la acción de la que ese resultado deriva (Sentencia de 30 de junio de 2021, del Tribunal Superior de Justicia de Madrid), ya que la pérdida de confidencialidad e integridad de los datos personales no está únicamente sujeta a la adopción de medidas de seguridad. Esta Agencia se reitera en que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el artículo 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. De seguridad. Sólo de seguridad.

Por idénticas razones tampoco se trata en el presente caso de que la conducta que infringe el artículo 5.1.f) del RGPD y la conducta que infringe el artículo 32 del RGPD deban ser consideradas como una sola conducta a efectos punitivos (como en la Sentencia de 13 de mayo de 2004, del Tribunal Superior de Justicia de Madrid), ya que no derivó un hecho del otro.

Esta Agencia se reitera en que el artículo 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad de los datos personales, lo que puede producirse, o no, por ausencia o deficiencia de las medidas de seguridad.

Y que este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad, integridad o disponibilidad cuando explicita “mediante la aplicación de medidas técnicas y organizativas apropiadas”, que no son estrictamente de seguridad (como sí lo es la obligación a que refiere el artículo 32 del RGPD).

Añade ENDESA que se trata de unas reglas que en este caso se contienen en las Directrices 4/2022, del Comité Europeo de Protección de Datos (*“**CEPD**”*), sobre el cálculo de multas administrativas bajo el RGPD, cuya aplicación debería dar lugar, conforme al principio de especialidad, a que únicamente pudiera sancionarse la supuesta infracción del artículo 32 del RGPD.

Alega ENDESA que la Propuesta de Resolución se limita a afirmar en este punto -de nuevo sin sustento alguno- que las referidas Directrices sólo serían de aplicación a los hechos que hubieran tenido lugar con posterioridad a su adopción y que, por tal motivo, no podrían aplicarse en este caso. Sin embargo, lo cierto es que nada impide aplicar las Directrices a expedientes que se encuentren en curso (aun cuando los hechos puedan ser anteriores), pues no son más que reglas y criterios para el cálculo de las sanciones y porque, además, es lo único realmente coherente con el objetivo de armonización que dichas Directrices expresamente recogen y que es lo que ha motivado su aprobación por el CEPD. De hecho, siendo más beneficiosa en este caso su aplicación atendiendo a los diferentes importes de las sanciones propuestas para las supuestas infracciones, su aplicación vendría exigida por lo establecido en el artículo 9.3 de la Constitución.

Añade ENDESA que, si pese a ello esa Agencia considerase que las citadas Directrices no resultan aplicables (lo que para esta parte sería una grave infracción del principio constitucional que exige la retroactividad favorable en materia sancionadora), necesariamente habría que estar al artículo 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), con lo que sólo cabría la sanción por el incumplimiento del artículo 5.1.f) del RGPD.

Al respecto, esta Agencia se reitera en que las citadas Directrices no resultan de aplicación al presente supuesto. No obstante, aun si lo fueran, esta Agencia considera que se trata de dos conductas infractoras distintas, por lo anteriormente expuesto en la contestación a las alegaciones al acuerdo de inicio y a la propuesta de resolución del presente procedimiento sancionador, por lo que tampoco sería de aplicación el capítulo 3 de las citadas Directrices.

Por último, en cuanto a la aplicabilidad del artículo 29.5 de la LRJSP que alega ENDESA, esta Agencia desea señalar que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD.

Y ello porque el RGPD es un sistema cerrado y completo.

El RGPD es una norma comunitaria directamente aplicable en los Estados miembros, que contiene un sistema nuevo, cerrado, completo y global destinado a garantizar la protección de datos de carácter personal de manera uniforme en toda la Unión Europea.
En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne su finalidad última que es la garantía efectiva y real del derecho fundamental a la Protección de Datos de Carácter Personal. Lo contrario determinaría la merma de las garantías de los derechos y libertades de los ciudadanos.

De hecho, una muestra específica de la inexistencia de lagunas en el sistema del RGPD es el artículo 83 del RGPD que determina las circunstancias que pueden operar como agravantes o atenuantes respecto de una infracción (art. 83.2 del RGDP) o que especifica la regla existente relativa a un posible concurso medial (art. 83.3 del RGPD).
A lo anterior se ha de sumar que el RGPD no permite el desarrollo o la concreción de sus previsiones por los legisladores de los Estados miembros, a salvo de aquello que el propio legislador europeo ha previsto específicamente, delimitándolo de forma muy concreta (por ejemplo, la previsión del art. 83.7 del RGPD). La LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que este le permite y con el alcance que éste le permite.

Ello es así porque la finalidad pretendida por el legislador europeo es implantar un sistema uniforme en toda la Unión Europea que garantice los derechos y libertades de las personas físicas, que corrija comportamientos contrarios al RGPD, que fomente el cumplimiento, que posibilite la libre circulación de estos datos.

En este sentido, el considerando 2 del RGPD determina que:

"(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".(el subrayado es nuestro)

Sigue indicando el considerando 13 del RGPED que:

"(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". (el subrayado es nuestro)

En este sistema, lo determinante del RGPD no son las multas. Los poderes correctivos de las autoridades de control previstos en el art. 58.2 del RGPD conjugado con las disposiciones del art. 83 del RGPD muestran la prevalencia de medidas correctivas frente a las multas.

Así, el art. 83.2 del RGPD dice que "*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j).".*

De esta forma las medidas correctivas, que son todas las previstas en el art. 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.

Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

Por ello, el artículo 83.1 del RGPD previene que "*Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente*

artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasoria".

Las multas han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

Para que dicho sistema funcione con todas sus garantías en necesario que varios elementos se desplieguen de forma íntegra y completa. La aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español-, ya sea por la aplicación de un concurso medial distinto del dispuesto en el RGPD, restaría efectividad al sistema que perdería su sentido, su finalidad teleológica, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

El RGPD está dotado de su propio principio de proporcionalidad que ha de ser aplicado en sus estrictos términos.

Por tanto, no hay laguna legal, no hay aplicación supletoria del art. 29 del RGPD.

Amén de lo expuesto, cabe significar que no hay laguna legal respecto de la aplicación del concurso medial. Ni el RGPD permite ni la LOPDGDD dispone la aplicación supletoria de las previsiones del art. 29 de la LRJSP.

En el Título VIII de la LOPDGDD relativo a "Procedimientos en caso de posible vulneración de la normativa de protección de datos", el artículo 63 que abre el Título se dispone 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.".* Si bien existe una remisión clara a la LPACAP, no se establece en absoluto una aplicación subsidiaria respecto de la LRJSP que no contiene en su articulado disposición alguna relativa a procedimiento administrativo alguno.

De igual forma que la AEPD no está aplicando los agravantes y atenuantes dispuestos en el art. 29 de la LRJSP, puesto que el RGPD establece los suyos propios, por ende, no hay laguna legal ni aplicación subsidiaria del mismo, tampoco cabe la aplicación de apartado relativo al concurso medial y por idénticas razones.

Por todo lo expuesto, se desestima la presente alegación.

2.3.- Conclusión: improcedencia de sancionar por separado los supuestos incumplimientos de los artículos 5.1.f) y 32 del RGPD

A juicio de ENDESA, cuanto antecede evidencia el error en el que incurre la Propuesta de Resolución al pretender sancionar a Endesa de forma separada por los supuestos incumplimientos de los artículos 5.1.f) y 32 del RGPD.

Por ello, entiende ENDESA que dicha Propuesta de Resolución debe ser rectificada y, en caso de que, a pesar de cuanto en el presente escrito se argumenta, esta Agencia entendiera concurrente una infracción de las obligaciones en materia de seguridad, sólo podría sancionarse a Endesa por el presunto incumplimiento del artículo 32 del RGPD (si se aplica el criterio de especialidad contenido preferentemente en las Directrices) o, a lo sumo, del artículo 5.1.f) del RGPD (si se considera de aplicación la regla general contenida en la LRJSP), sin perjuicio de que el artículo 9.3 de la Constitución obligaría a aplicar el principio de especialidad contenido en las citadas Directrices.

Al respecto, esta Agencia se reitera en lo ya expuesto en su contestación a las alegaciones al acuerdo de inicio y a la propuesta de resolución del presente procedimiento sancionador, por lo que se desestima la presente alegación.

3. Vulneración del principio de tipicidad

Al respecto de la alegación de ENDESA en el escrito de alegaciones al Acuerdo de Inicio, la AEPD viene a responder que el principio de tipicidad no se ve vulnerado porque el RGPD permite a la autoridad de supervisión concretar el importe de la sanción utilizando una serie de elementos valorativos incluidos en el artículo 83 RGPD, tales como las circunstancias modificativas de la responsabilidad del punto 2 o la definición de tipos de los puntos 3 y 4.

Alega ENDESA que lo anterior no resuelve la cuestión planteada, ya que la tipicidad en el presente caso no se ve vulnerada por la estructura del RGPD, sino por la ausencia de concreción de la actividad infractora que se contiene tanto en el Acuerdo de Inicio como en la Propuesta de Resolución. En este sentido, a pesar de lo extenso del expediente, incluyendo los requerimientos previos, la AEPD no ha concretado cuáles serían las medidas específicas que Endesa no ha cumplido que permitirían: (i) evitar o reducir el riesgo de que hubiera ocurrido el incidente en causa, y (ii) defender la adecuación de las medidas desplegadas por Endesa al RGPD.

Se reitera, por tanto, la alegación expresada por vulneración del principio de tipicidad en este aspecto y, en particular, lo expuesto en la conclusión de aquel escrito cuando se decía que "*En consecuencia, en la aplicación de la norma la administración debe ser extremadamente cuidadosa a la hora de identificar los hechos constitutivos de infracción y de explicar el motivo por el cual esos hechos son incardinables en el tipo redactado de forma poco taxativa*".

Al respecto, esta Agencia desea señalar que se ha detallado ampliamente cuáles han sido los hechos constitutivos de la infracción y cómo se incardinan en el tipo redactado.

Alegaba ENDESA en sus alegaciones al acuerdo de inicio del presente procedimiento sancionador que: "*el artículo 5.1.f) del RGPD establece un principio general que no tiene concreción específica mediante actos positivos o limitativos claros que el sujeto obligado pueda conocer y cumplir. Al contrario, utiliza conceptos jurídicos indetermina-*

dos de forma encadenada ("seguridad adecuada", "medidas apropiadas"), que no permiten conocer de forma transparente el alcance de las obligaciones o prohibiciones."

En el presente caso, tal y como se detalla en el Fundamento de Derecho IV, el 24 de agosto de 2021 ENDESA detectó en la red social Facebook un anuncio donde se vende usuario de la aplicación ******HERRAMIENTA.1*** con acceso a información de clientes. Y el 10 de septiembre de 2021 ENDESA obtuvo la comprobación de la veracidad del anuncio y la identificación de las credenciales del usuario de la aplicación que estaban siendo usadas por el anunciante para vender accesos. Es decir, que ya para septiembre de 2021 se había verificado que la confidencialidad de las bases de datos titularidad de ENDESA se había visto comprometida.

Posteriormente, el 19 de octubre de 2021 ******EMPRESA.1*** detectó que un usuario de ******EMPRESA.9*** había intentado realizar un alta fraudulenta, razón por la cual el 27 de octubre de 2021 envió una carta certificada a ******EMPRESA.9*** en la que se le comunicaba el cierre definitivo de la campaña de venta de contrato de suministro de ENDESA con efectos 19 de octubre, después de haber sido suspendida cautelarmente tal campaña ese mismo día.

El 20 de octubre de 2021, ******EMPRESA.1*** envió una comunicación a ENDESA indicando las operaciones afectadas por la práctica fraudulenta de ******EMPRESA.9***, identificándose 137 contrataciones realizadas y otras 7 operaciones pendientes de validación por parte de ENDESA que no habían llegado a darse de alta. También se identificaron y se bloquearon, para que no se tramitara su contratación, otras 172 órdenes que estaban pendientes de validar por el back office de ******EMPRESA.9***.

Es decir, que desde septiembre de 2021 ENDESA ya conocía la existencia de una quiebra de seguridad y desde octubre de 2021 que la confidencialidad e integridad de los datos de 137 interesados se habían visto comprometidas y que había otros 179 posibles interesados cuyos datos era más que probable que pudieran haber sido comprometidos.

Por su parte, el 27 de octubre de 2021 se envió un correo electrónico a ENDESA en el que se remitía adjunto un e-mail del gerente de ******EMPRESA.9*** comunicando a ******EMPRESA.1*** las denuncias presentadas ante la Policía de ***PAÍS.1 el 19 de octubre de 2021 contra 23 agentes comerciales", ***(…)***.

El 27 de octubre de 2021 ******EMPRESA.1*** recibió un email del gerente de ******EMPRESA.9***, que ese mismo día ******EMPRESA.1*** reenvió a ENDESA***,*** con el detalle de las averiguaciones realizadas sobre la práctica fraudulenta llevaba a cabo por algunos de sus agentes y su *modus operandi*.

Con el detalle de este *modus operandi* quedaba acreditado que se habían visto afectadas la integridad y confidencialidad de los datos personales de al menos aquellos clientes a los que se les hubiera dado de alta de forma fraudulenta, toda vez que para poder proceder al alta era necesario acceder a sus datos y modificarlos por unos falsos.

También en este mail con fecha 27 de octubre de 2021 ******EMPRESA.1*** identificó cinco de los usuarios de ******HERRAMIENTA.1*** comprometidos en la violación de la seguridad

de los datos personales (utilizados por ***EMPRESA.9**) y se adjuntaron capturas de pantalla con anuncios de Facebook en los que se ofrecía el alquiler y/o venta de credenciales de acceso a la aplicación ***HERRAMIENTA.1**.

El 17 de enero de 2022 se publicaron nuevos anuncios en Facebook por parte del usuario ***B.B.B.***, en los que existió afectación a bases de datos de clientes de energía de ENDESA. Por tanto, como mínimo durante el mes de enero de 2022 la confidencialidad de los datos obrantes en la base de datos titularidad de ENDESA continuaba sin ser debidamente garantizada.

El 7 de febrero de 2022 ENDESA envió un burofax a FACEBOOK SPAIN S.L. en el que indicaba que había usuarios publicando información que podía ser constitutiva de delito y pedía su eliminación, de lo que se infiere que aún continuaban publicados los anuncios que vendían las credenciales para acceder a ***HERRAMIENTA.1**, viéndose aún comprometida la confidencialidad de los datos obrantes en dicho sistema.

El día 8 de febrero de 2022, tras las investigaciones oportunas, ENDESA tuvo conocimiento de la existencia de ciertas coincidencias entre los datos que aparecían en las bases de datos publicadas y los que podían estar incluidos en el sistema comercial de ENDESA, ***HERRAMIENTA.2**.

ENDESA llevó a cabo una nueva valoración del incidente y con fecha 9 de febrero de 2022 comprobó la veracidad de los últimos anuncios y la identidad de los dos anunciantes, ambos extrabajadores de proveedores de ENDESA con acceso a ***PLATAFORMA.1 (***HERRAMIENTA.1)**. Se detectaron un total de nueve usuarios comprometidos entre septiembre de 2021 y enero de 2022, que estaban siendo usados por los anunciantes de Facebook para vender accesos *a* ***PLATAFORMA.1 (***HERRAMIENTA.1**). Además, se comprobó que seis de ellos tenían acceso a ***HERRAMIENTA.2**. Se comprobó también la validez de las credenciales, en todos los casos asignadas a proveedores de ENDESA para realizar trabajos de captación y atención al cliente.

Es decir, se comprobó que la confidencialidad de los datos obrantes en ***HERRAMIENTA.1** y ***HERRAMIENTA.2** no había sido suficientemente garantizada toda vez que estuvieron a disposición de terceros no autorizados, lo cual permitió que además la integridad de los datos se viera también en riesgo al posibilitar la realización de numerosas altas fraudulentas.

También, ENDESA ha señalado que el hecho de que dos o más personas pudieran acceder a la vez con un mismo usuario a ***HERRAMIENTA.1**, opción multisesión habilitada cuando se produjo la violación de la seguridad de los datos personales, y que, en relación con los usuarios comprometidos y con el período en que este incidente se desarrolló, no se mantuviera un registro (logs) del uso de las herramientas ***HERRAMIENTA.1** o ***HERRAMIENTA.2**, le impide conocer el número de registros de los aplicativos que pudieron ser realmente accedidos, al menos desde que tuvo conocimiento en agosto de 2021 de la publicación del anuncio en Facebook.

Los potenciales afectados por la violación de la seguridad de los datos personales en cuestión, respecto a la herramienta ***HERRAMIENTA.1**, fueron 30,6 millones de puntos de suministros y 8,6 millones de puntos de suministro de gas de usuarios no

clientes de ENDESA, así como datos de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas de ENDESA.

Tampoco, respecto a la herramienta ******HERRAMIENTA.2***, se garantizó la confidencialidad de los datos personales de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas de ENDESA.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA no garantizó debidamente la confidencialidad e integridad de los datos personales de su titularidad.

En cuanto a la exigencia de ENDESA de que esta Agencia concrete cuáles serían las medidas específicas que Endesa no ha cumplido, el propio enfoque del RGPD impide dar tal detalle.

La responsabilidad proactiva que predica el RGPD implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento generalizado de las obligaciones en materia de protección de datos. Comprende el establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que le permita demostrar su cumplimiento.

Pivota sobre la gestión del riesgo. Tal y como se establece en el Informe 0064/2020 del Gabinete Jurídico de la AEPD se muestra la metamorfosis de un sistema que ha pasado de ser reactivo a convertirse en proactivo, puesto que "*en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la LOPDGDD: "la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan".*

Requiere de una actitud consciente, comprometida, activa y diligente. La consciencia supone el conocimiento de su organización por parte del responsable del tratamiento y de cómo se ve afectada por la protección de datos y de los riesgos inherentes a los tratamientos de datos personales; el compromiso involucra la voluntad de cumplir y el hacerse verdaderamente responsable de la implantación de las políticas de protección de datos en la organización; la actitud activa está relacionada con la proactividad, la eficacia, la eficiencia y la operatividad; y la diligencia es el cuidado, el celo y la dedicación puesta en el cumplimiento.

Quien mejor conoce su actividad es quien realiza los tratamientos de datos personales en cuestión (en este caso, ENDESA) y quien debe detallar y demostrar las medidas adoptadas, de acuerdo con lo establecido, en particular, en el artículo 5.2 del RGPD. Las deficiencias observadas en las medidas adoptadas por Endesa ya han sido puestas de manifiesto por esta Agencia a lo largo de la presente resolución.

Por todo lo expuesto, se desestima la presente alegación.

Segunda.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 33 del RGPD

La Propuesta de Resolución, a la hora de mantener la propuesta de sanción por presunta infracción del artículo 33 del RGPD, se centra principalmente en el argumento, a juicio de ENDESA erróneo, de que Endesa no calificó correctamente el incidente al considerar que no era notificable tras los dos primeros análisis realizados.

La AEPD sostiene que "*simplemente basta con que exista una probabilidad (la que sea) de que exista un riesgo (el que sea)*" para que, de conformidad con el artículo 33 del RGPD, un responsable del tratamiento deba notificar la existencia de una brecha de seguridad a la AEPD.

Sorprende a ENDESA que esta sea la interpretación de la AEPD en este procedimiento cuando esta misma Agencia, junto con la primera Guía de Gestión de Notificación de Brechas de Seguridad, publicó una herramienta, la cual pretendía ayudar a responsables del tratamiento en su evaluación del riesgo, en la que, en función de varios factores (volumen de datos afectados, tipología de datos e impacto de la violación), otorgaba un nivel de riesgo (del 2 al 100) y, en función del mismo, otorgaba un resultado sobre la necesidad o no de notificar la violación de seguridad a la AEPD (y a los interesados afectados). En este sentido, la herramienta únicamente arrojaba como resultado la necesidad de notificar la brecha a la AEPD en aquellos casos en los que el nivel de riesgo era: (i) desde el punto de vista cuantitativo, mayor que 20; o (ii) desde el punto de vista cualitativo, elevado en función de los factores analizados.

Es decir, según el análisis de dicha herramienta no bastaba simplemente con que, tal y como ahora indica la AEPD, "*exista una probabilidad (la que sea) de que exista un riesgo (el que sea)*" para que la violación de la seguridad fuese notificable a la AEPD, sino que dicho riesgo debería ser suficientemente apreciable y probable (en el ejemplo anterior, mayor que 20).

Alega ENDESA que en un sentido similar se pronuncia la actual Guía para la notificación de brechas de datos personales de la AEPD, la cual indica literalmente que: "*No es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas*".

Señala ENDESA estas dos últimas palabras, "*improbable*" y "*riesgo*", ya que resulta relevante traer a colación las notas al pie unidas a las mismas en la ya mencionada Guía de la AEPD. En este sentido, ambas notas al pie asociadas a las palabras anteriores

en la Guía, hacen referencia a las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679 publicadas por el Grupo de Trabajo del Artículo 29 (actual CEPD), en las cuales se indica que:

i "*Cuando la violación se refiera a datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la militancia en un sindicato, o que incluyan datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas, se considerará probable que tales daños y perjuicios se produzcan*"; y
ii *"…inmediatamente después de tener conocimiento de una violación, es de vital importancia que el responsable del tratamiento no trate solo de contener el incidente, sino que también evalúe el riesgo que podría derivarse del mismo".*

Alega ENDESA que, tal y como se puede observar de la primera mención, si en aquellos casos en los que la violación de la seguridad tiene impacto en categorías especiales de datos, se considerara probable que se produzcan daños y perjuicios sobre los interesados, "*a sensu contrario*" debe interpretarse que, en el resto de casos (en los que categorías especiales de datos no se ven afectadas – tal y como ocurre en el marco de este expediente) esto no será así por defecto, por lo que la probabilidad de que la violación constituya un riesgo para los interesados deberá calcularse y valorarse. De no ser así, las Directrices del Grupo de Trabajo del Artículo 29 no habrían hecho esta distinción.

Indica ENDESA que, en el caso que nos ocupa, determinó, en sus dos primeros análisis de riesgos del incidente, que no era probable que éste entrañase un riesgo para los derechos y las libertades de las personas físicas afectadas, entre otros aspectos porque ninguna categoría especial de datos se había visto afectada.

Explica ENDESA que, volviendo a la nota al pie número (ii) arriba indicada, el Grupo de Trabajo del Artículo 29 indica que es responsabilidad del responsable del tratamiento, además de contener el incidente, evaluar el riesgo que para los interesados afectados supone la violación de seguridad. Es decir, el responsable del tratamiento (en este caso, Endesa), con anterioridad a la realización de la notificación de la violación de la seguridad a la AEPD, deberá evaluar el riesgo que ésta supone para los derechos y libertades de los interesados afectados y, en función de esa evaluación y del riesgo, realizar o no dicha notificación. Por lo tanto, atentaría directamente contra las directrices del Grupo de Trabajo del Artículo 29, y contra la literalidad del artículo 33.1 del RGPD, lo que indica la AEPD en su Propuesta de Resolución; es decir, que la notificación a la autoridad de control debe realizarse siempre que "*exista una probabilidad (la que sea) de que exista un riesgo (el que sea)*".

A mayor abundamiento y en este sentido, ENDESA trae a colación las Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales emitidas por el CEPD y a las que la propia AEPD hace referencia en su Propuesta de Resolución para justificar su conclusión. En dichas Directrices, en varios de sus ejemplos (más concretamente en los casos números 9, 13 y 15) en los que el Comité llega a la conclusión de que **no** sería necesario realizar una notificación ante la autoridad de control, se indica que, aunque existe riesgo, este es bajo. Es decir, el propio Comité no comparte la interpretación realizada por la AEPD en la Propuesta de Re-

solución en virtud de la cual la determinación de cualquier riesgo, "*el que sea*", llevaría a la conclusión de que es necesario notificar la violación de la seguridad a la autoridad de control.

Más específicamente, uno de los ejemplos indica: "*En el caso concreto que se describe, el riesgo es bajo, ya que no estaban implicadas categorías especiales de datos personales …*" (caso Nº 13) y en otro de ellos se indica que "*era poco probable que esta violación de la seguridad de los datos entrañara un riesgo para los derechos y libertades de los interesados, por lo que no era necesaria ninguna notificación a la AC o a los interesados afectados*" (caso Nº 15). Alega ENDESA que, como se puede observar, al contrario de lo que indica la AEPD en su Propuesta de Resolución, ni cualquier riesgo ("*el que sea*"), ni cualquier probabilidad ("*la que sea*"), convierte, a ojos del CEPD, una violación de la seguridad en notificable de conformidad con el artículo 33 del RGPD.

Es decir, de conformidad con las Directrices 1/2021, en aquellos supuestos en los que se determine que el riesgo es bajo (por ejemplo, por no afectar a categorías especiales de datos) o que la probabilidad de que la violación entrañe un riesgo es remota ("*poco probable*") tampoco sería necesaria una notificación a la autoridad de control. Este es específicamente el caso que nos ocupa, en el que Endesa, tras la realización de los correspondientes análisis de riesgo y probabilidad, determinó, en dos ocasiones, que tanto el riesgo para los derechos y libertades de los interesados afectados era bajo, como la probabilidad de que dicho riesgo se materializase era remota.

Y que, cuando las circunstancias del caso cambiaron, Endesa volvió a realizar un tercer análisis cuyo resultado arrojó que en ese momento sí era necesario realizar una notificación de la violación de seguridad a la AEPD. Convienen destacar que, si la intención de Endesa, desde el primer momento, hubiese sido ocultar este incidente a la AEPD, no se hubiera llevado a cabo la notificación de la violación una vez consideró que la misma era notificable. Y no lo hizo hasta entonces puesto que estaba convencida, tras la realización de los análisis oportunos, que, hasta dicho momento: (i) el riesgo para los derechos y libertades de los interesados afectados era bajo; y (ii) la probabilidad de que dicho riesgo se materializase era remota.

Por lo tanto, alega ENDESA que no es cierto, como indica la Propuesta de Resolución, que no notificase el incidente en el primer momento en el que tuvo conocimiento de los anuncios publicados en Facebook puesto que se encontraba realizando un "*examen detallado de la situación*". Al contrario, Endesa realizó dicho examen de la situación nada más tuvo conocimiento de la misma, pero determinó, siguiendo las directrices de la AEPD y del CEPD al efecto, que no se alcanzaba el umbral de notificación previsto en el artículo 33 del RGPD.

Sin perjuicio de lo anterior, sorprende a ENDESA que la AEPD, en su Propuesta de Resolución, más allá de indicar que no está de acuerdo con la valoración de la no necesidad de notificación de la violación realizada por Endesa en sus dos primeros informes [puesto que, al contrario de lo indicado en sus propias guías y en las directrices emitidas por el CEPD, la AEPD entiende en este caso que la notificación a la autoridad de control debe realizarse siempre que "*exista una probabilidad (la que sea) de que exista un riesgo (el que sea)*"], no fundamente la concurrencia de dolo en la actuación de Endesa. Es decir, dado que los dos primeros informes realizados por Endesa analizando el incidente se redactaron (en opinión de ENDESA) basándose en una interpre-

tación razonable de la normativa de protección de datos aplicable y de las directrices interpretativas, lo cual acredita (a su juicio) una debida diligencia, entiende Endesa que la imposición de una sanción por incumplimiento del artículo 33 del RGPD (máxime cuando se propone la imposición de una sanción tan cuantiosa) debe venir precedida de una fundamentación jurídica rigurosa y completa sobre la concurrencia de dolo en la actuación de Endesa, lo que no se da en la Propuesta de Resolución.

Al respecto, esta Agencia reconoce que la redacción de la frase de la propuesta de resolución, controvertida por ENDESA, de que "*Simplemente, basta con que exista una probabilidad (la que sea) de que exista un riesgo (el que sea). Tampoco hace falta que ese riesgo se hubiera materializado para que tal incidente sea notificable, basta con que sea probable*", quizás no fue la más acertada, o más bien, podría requerir un mayor desarrollo en su explicación.

Por supuesto que no todas las violaciones de la seguridad de los datos personales deben ser notificadas a la autoridad de control correspondiente. Pero es cierto que el artículo 33 del RGPD contiene una suerte de norma general según la cual todas las violaciones de la seguridad de los datos personales deben ser notificadas a la autoridad de control, a no ser que *"…sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"*.

De lo estipulado en el RGPD y de todo lo explicado en la Guía para la notificación de brechas de datos personales de la AEPD (tanto en su primera versión como en su versión actual), así como en las citadas Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales, se desprende que (tal como afirma ENDESA) "es responsabilidad del responsable del tratamiento, además de contener el incidente, evaluar el riesgo que para los interesados afectados supone la violación de seguridad. Es decir, el responsable del tratamiento (en este caso, Endesa), con anterioridad a la realización de la notificación de la violación de la seguridad a la AEPD, deberá evaluar el riesgo que esta supone para los derechos y libertades de los interesados afectados y, en función de esa evaluación y del riesgo, realizar o no dicha notificación." Pero esto no excluye que la Agencia pueda valorar posteriormente la adecuación al RGPD de las decisiones tomadas por el responsable del tratamiento relativas a la protección de datos de carácter general.

De toda la documentación obrante en el presente procedimiento sancionador, esta Agencia ha concluido que ENDESA no ha calificado correctamente la violación de la seguridad de los datos personales como notificable.

Cita ENDESA la primera Guía de Gestión de Notificación de Brechas de Seguridad, la cual contaba con una herramienta para ayudar a evaluar el riesgo de los incidentes y la necesidad de notificarlos a la AEPD e interesados.

En primer lugar, esta Agencia desea señalar que las conclusiones a las que pudiera arribar el responsable del tratamiento al utilizar dicha Guía y la herramienta en cuestión, no es más que una guía, precisamente, una ayuda a la toma de decisiones, pero la decisión sobre si debe notificarse una violación de seguridad de los datos personales a la AEPD corresponde única y exclusivamente al responsable del tratamiento y su utilización en ningún caso representa el pronunciamiento de esta Agencia sobre la aplicación del artículo 33 del RGPD sobre un incidente concreto.

En segundo lugar, la herramienta en cuestión indicaba que debía notificarse un incidente a la AEPD cuando el nivel de riesgo y su probabilidad era tan bajo que pudiera ser descartado. Para ello, evaluaba una serie de factores y asignaba una puntuación al riesgo (la cual debía ser mayor que 20 para considerarse notificable) y también analizaba distintos factores (si coincidía más de uno, debía notificarse).

Tal y como consta en los hechos probados del presente procedimiento, el 13 de septiembre de 2021, según consta en el Documento número 10 que acompaña el escrito de ENDESA de 26 de julio de 2022, se realiza la primera valoración de la violación de la seguridad de los datos personales, donde se recoge la información obtenida hasta ese momento en un documento firmado el 14 de septiembre de 2021.

En dicho documento se indica que los principales datos que contiene ******PLATAFORMA.1*** son: nombre, apellidos y dirección del cliente, NIF, Número CUPS, productos contratados, y que el número estimado de registros afectados estaría entre 100 y 1.000.

En base a los datos que constan en tal documento, ENDESA realiza una valoración del riesgo siguiendo la herramienta proporcionada por esta Agencia, en la que asigna al incidente la siguiente puntuación:

- Volumen: entre 100 y 1.000 registros (2). [No en color destacado.]
- Datos no sensibles (x1) [No en color destacado.]
- Impacto: Externo (6). [En color destacado]

Y se le asigna un riesgo de 3 x (1 x 6): 12

Por tanto, por ser un valor inferior a 20 y por no coincidir más de un factor destacado (en otro color), ENDESA consideró que el incidente no era notificable.

No obstante, la propia ENDESA ha indicado en ese mismo documento que los datos afectados por la violación de la seguridad de los datos personales comprendían el nombre, apellidos, domicilio, entre otros, junto con su NIF. Datos que identifican a los interesados de manera inequívoca.

Sobre este extremo cabe señalar que, los considerandos 51 y 75 del RGPD distinguen un grupo de datos personales que por su naturaleza son particularmente "*sensibles"* por el importante riesgo que puede entrañar su tratamiento para los derechos y libertades fundamentales. Su denominador común es el riesgo que comporta para los derechos y las libertades fundamentales, pues su tratamiento puede llegar a provocar daños y perjuicios físicos, materiales o inmateriales.

Se incluyen en este grupo o categoría los datos especialmente protegidos que regula el artículo 9 del RGPD -considerando 51 del RGPD- y, además, otros muchos que no se citan en ese precepto. El considerando 75 menciona con detalle los datos personales cuyo tratamiento puede entrañar un riesgo de gravedad y probabilidad variables para los derechos y libertades de las personas físicas como consecuencia de que pueden provocar daños y perjuicios físicos, materiales o inmateriales. Entre ellos se refiere a aquellos cuyo 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;"

El identificador numérico del DNI junto con el carácter de verificación correspondiente al número de identificación fiscal identifica a una persona física de modo indubitado. Esta cualidad lo convierte en un dato particularmente sensible pues, en la medida en que su tratamiento no vaya acompañado de las medidas técnicas y organizativas necesarias para garantizar que quien se identifica con él es realmente su titular, un tercero puede suplantar la identidad de una persona física con total facilidad, o, con otras palabras, puede provocar un fraude de identidad, con los riesgos que ello comporta para la privacidad, el honor y el patrimonio del suplantado.

La vulneración del principio de confidencialidad del que se responsabiliza a ENDESA ha tenido por objeto, entre otros datos, el NIF de los interesados, que permite su identificación unívoca. Razón por la cual esta Agencia ha considerado en anteriores procedimientos sancionadores (a modo de ejemplo, el PS/00012/2022) que el NIF es un dato personal que se considera asimilable a aquéllos de categorías especiales, merecedores de una especial protección, por el mayor riesgo que entrañan para los derechos y libertades de los interesados. Todo ello sin olvidar que junto con el NIF se vieron también afectados por la violación de la seguridad los datos personales de nombre, apellidos, domicilio y cuentas bancarias, entre otros, de los afectados, de lo que se infiere al menos un riesgo de usurpación de identidad o fraude.

Por tanto, esa primera valoración del incidente no habría estado bien realizada, toda vez que la puntuación del riesgo debió ser mayor, debiendo asignarse a la tipología de los datos afectados un valor doble por ser datos sensibles (el valor numérico habría sido 24, superando el umbral de los 20 necesarios para considerar el incidente como notificable. Además, se habría tratado de factores de los destacados, por lo que cualitativamente, también habría superado el umbral necesario para ser notificable. Por lo que esta Agencia se reitera en considerar que ENDESA debió notificar a esta Agencia la violación de la seguridad de los datos personales mucho antes de lo que lo hizo.

Cita ENDESA la actual Guía de la AEPD para la notificación de brechas de datos personales, que indica que la excepción a esta obligación de notificación a la autoridad de control se da cuando el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Y respecto de las palabras “improbable” y “riesgo” trae a colación la referencia que se realiza a las Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales, para concluir que cuando las violaciones de la seguridad de los datos personales no tienen impacto en categorías especiales de datos, “a sensu contrario”, no sería necesario notificarlas por defecto.

Al respecto, esta Agencia desea remarcar que aunque la violación de la seguridad de los datos personales no hubiera afectado a categorías especiales de datos, ello no exime de forma automática del deber de notificar el incidente a la autoridad de control correspondiente, sino que el responsable del tratamiento debe, en todo caso, evaluar los

riesgos para los derechos y libertades de los interesados así como la probabilidad de que ocurran, determinando el posible impacto del incidente en cuestión.

En cualquier caso, tal y como se ha detallado anteriormente, en el presente supuesto, tanto por el volumen de los datos personales comprometidos como por la categoría de dichos datos (en especial, al haberse visto comprometida la confidencialidad de los nombres, apellidos, domicilios, DNI y hasta números de cuentas bancarias, con los consiguientes riesgos que ello podría suponer para los derechos y libertades de los afectados) esta Agencia se reitera en que el riesgo era mayor de lo valorado por ENDESA y que debió realizarse la notificación del incidente con anterioridad a lo que se hizo.

Cita ENDESA también algunos ejemplos (números 9, 13 y 15, en concreto) de las citadas Directrices 1/2021, para concluir que en dichos ejemplos se considera no necesario notificar a la autoridad de control la violación de la seguridad de los datos personales. No obstante, tales ejemplos citados no serían extrapolables al presente caso.

El caso número 9 refiere a un supuesto de transmisión accidental de datos a un tercero de confianza y las diferencias con el presente supuesto son más que evidentes: en el ejemplo de las Directrices se trata de un error involuntario, a diferencia de lo que ocurre en el presente caso (que hubo una acción intencionada); el incidente afectaba solo a la confidencialidad de los datos, mientras que en el presente caso se afectó la confidencialidad y la integridad de los datos; en el ejemplo solo se afectaba mientras que en el presente caso los afectados por el incidente se contaron por millones; y quien tuvo acceso a los datos estaba sujeto a un deber de secreto profesional (lo cual no ocurrió en el presente caso tampoco).

El caso número 13 de las citadas Directrices refiere a un error de correo postal, lo cual tampoco ha acontecido en el presente caso (que se trató de un acceso a los sistemas informáticos de ENDESA). Y en el ejemplo no se habían visto afectadas categorías especiales de datos (lo cual puede entenderse sí ha ocurrido en el presente caso, como se ha detallado anteriormente).

El caso número 15 de las citadas Directrices refiere a datos personales enviados por correo por error, lo cual tampoco ha acontecido en el presente caso. Si bien se trata en ambos casos de datos especialmente protegidos, lo cierto es que en el ejemplo el riesgo para los derechos y libertades de los afectados se consideraba relativamente bajo, a diferencia de lo que ocurre en el presente caso. Además, la cantidad de datos vulnerados y el número de interesados era muy bajo (a diferencia de lo que ocurrió en el presente caso).

Por último, esta Agencia considera que el ejemplo de las citadas Directrices que podría considerarse más similar a lo acontecido en la violación de la seguridad de los datos personales objeto del presente procedimiento sancionador es posiblemente el caso número 8, referido a una exfiltración de datos por un empleado, toda vez que fueron empleados de empresas que trabajaban con ENDESA quienes pusieron a la venta los accesos a los sistemas en cuestión. Si bien se observan algunas diferencias (en el ejemplo se considera que normalmente solo se ve comprometida la confidencialidad y que no se vieron comprometidas categorías especiales de datos personales), en el mismo ejemplo las Directrices hacen referencia a que *“no se excluye un uso indebido*

adicional y más grave de los datos robados, en función de la finalidad del tratamiento establecido por el antiguo empleado." Y concluye*: "En resumen, dado que la violación en cuestión no supondrá un riesgo elevado para los derechos y libertades de las personas físicas, bastará con una notificación a la AC. Sin embargo, la información a los interesados podría ser beneficiosa también para el responsable del tratamiento, ya que podría ser mejor que supieran por la empresa acerca de la fuga de datos en lugar de por el antiguo empleado que intenta ponerse en contacto con ellos*". Es decir, aun con las diferencias señaladas, en este supuesto las mismas Directrices consideran que la violación de la seguridad de los datos personales debía ser notificada a la autoridad de control.

Por último, señala ENDESA que no tuvo intención de ocultar el incidente a la AEPD y que no se ha fundamentado debidamente la concurrencia de dolo en la actuación de ENDESA al respecto.

Sobre esta cuestión, esta Agencia desea señalar que no ha considerado en ningún momento que ENDESA hubiera tenido intención de ocultar la violación de la seguridad de los datos personales ni que hubiera existido dolo en su actuación. Sino que ha considerado que a la hora de valorar el riesgo para los derechos y libertades de los afectados por el incidente, no ha sido todo lo diligente que debiera haber sido, razón por la que la valoración no ha sido la debida y no ha realizado la notificación a que refiere el artículo 33 del RGPD cuando hubiera debido hacerla, por lo que se considera que ENDESA ha infringido dicho artículo 33 del RGPD.

Por todo lo expuesto, se desestima la presente alegación.

Tercera.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 34 del RGPD

Interesa a Endesa clarificar que, al contrario de lo que indica la Propuesta de Resolución, ésta no ha "olvidado" que la obligación del artículo 34 del RGPD no se "activa" cuando se haya producido un daño sino cuando se determina que la violación de la seguridad puede entrañar un alto riesgo para los derechos y libertades de los interesados.

De hecho, alega que es esto lo que se analiza, por parte de Endesa, en las tres ocasiones en las que realiza el correspondiente análisis de riesgos que ya han sido presentados ante la AEPD. En ningún caso por parte de Endesa se está esperando, como parece dar a entender la AEPD, a que se materialice un daño, sino que se realiza el correspondiente análisis de conformidad con el RGPD y las Guías publicadas sobre la materia y se determina que el riesgo que la violación puede suponer para los interesados no es alto.

Y que es a posteriori, y no como parte del análisis ya realizado en su momento por Endesa, cuando se puede apreciar que dicho análisis era correcto y que realmente la violación no supuso un alto riesgo para los derechos y libertades de los interesados afectados. No trata por tanto Endesa de justificar la no notificación a los interesados bajo la pretendida excusa de que estos no sufrieron daños (el análisis sobre el riesgo se realizó mucho antes de conocer si los interesados sufrirían daños y Endesa seguiría - y sigue - defendiendo, independientemente del resultado dañoso o no dañoso, el rigor con

el que se realizó dicho análisis y el resultado del mismo), sino más bien constatar que el resultado del análisis realizado por Endesa (el incidente no suponía un alto riesgo para los derechos y libertades de los interesados), resultó ser más acorde a la realidad de las consecuencias que el realizado por la AEPD.

Sin perjuicio de lo anterior y de que, ENDESA está en desacuerdo con el resultado arrojado por el análisis de riesgos realizado por la AEPD (la violación entraña un alto riesgo para los derechos y libertades de los interesados) y, por tanto, con el requerimiento emitido por la AEPD sobre la necesidad de notificar la brecha a los interesados afectados (más aun cuando a la fecha de recepción de dicho requerimiento Endesa ya había tomado medidas ulteriores para garantizar que ya no existiese la probabilidad de que se concretizase el riesgo que había apreciado la AEPD), Endesa, con la finalidad de mostrar su máxima colaboración con esta Agencia y en un ejercicio de transparencia a todas luces innecesario desde el punto de vista normativo (a su juicio), decidió atender el requerimiento de la AEPD y facilitar la información requerida a los interesados afectados.

Aporta ENDESA, como **Documento número 2**, una declaración de ***DEPARTAMENTO.7 en la que se detallan las actuaciones llevadas a cabo de manera proactiva por parte de Endesa para atender de manera personalizada a los interesados que se hubieran podido ver afectados por el incidente, así como unos ejemplos de dichas tareas.

Respecto de la forma a través de la cual Endesa realizó la notificación a los interesados, la AEPD, en la Propuesta de Resolución, indica que no entra a valorar la conveniencia o no de utilizar un modelo por capas. Asume ENDESA, por tanto, que, como no podría ser de otro modo puesto que esta posibilidad se contempla en la infografía de la AEPD sobre cómo realizar las correspondientes notificaciones de brechas de datos personales a los interesados, no puede reprochársele a Endesa que no facilitase a los interesados toda la información requerida por el artículo 34 del RGPD[1].

Alega Endesa que siguió este modelo de información por capas para lograr una comunicación más efectiva con los interesados afectados atendiendo a las características de la violación de la seguridad (puesto que no todos los interesados podrían sufrir las mismas consecuencias ni se vieron afectados de la misma manera, las posibles medidas de mitigación del riesgo serían distintas en función del caso concreto, por lo que era más efectivo que dichas medidas se comunicasen a los interesados de manera personalizada a través de ***DEPARTAMENTO.4).

Teniendo lo anterior en cuenta, sorprende a ENDESA la aseveración realizada por la AEPD en su Propuesta de Resolución, puesto que contradice: (i) el hecho de que la AEPD no entre a valorar la conveniencia o no de utilizar un modelo por capas (sin valoración no puede haber reproche); y (ii) la propia infografía de la AEPD sobre cómo realizar notificaciones de brechas de datos personales a los interesados.

Por último, la Propuesta de Resolución reitera que la información facilitada a los interesados en la notificación realizada por Endesa no es veraz.

[1] *Asimismo, en la comunicación enviada a los afectados ENDESA no ha incluido una descripción de las posibles consecuencias que la violación de la seguridad de los datos personales podría causarles*" – Página 144 de la Propuesta de Resolución

En primer lugar, porque, según la Propuesta de Resolución, la notificación indica que la confidencialidad y la integridad de los datos personales de los interesados no se ha visto comprometida. Olvida la AEPD que esta notificación se realizó a finales del mes de marzo de 2022, cuando Endesa: (i) ya había procedido a deshabilitar los usuarios comprometidos; (ii) ya había desplegado la autenticación multifactor en las plataformas ******HERRAMIENTA.2 y ***HERRAMIENTA.1***; y (iii) ya se encontraba en contacto con la mayoría de los interesados afectados, prestándoles asistencia personalizada para, tal y como se indica en la notificación, "*evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades*" de los clientes de Endesa.

Es por esta razón que Endesa indica que la confidencialidad y la integridad de los datos no se ha visto comprometida (la intención de Endesa era indicar que, dado que había implementado medidas oportunas para evitar el riesgo, en ese momento la brecha de confidencialidad y la integridad de los datos ya se había subsanado).

En segundo lugar, indica la Propuesta de Resolución que "*tampoco es cierto que con las medidas adoptadas se evitara producir una afectación de alto riesgo a los derechos y libertades de los afectados*", puesto que los datos comprometidos podían ser utilizados para otras finalidades. Endesa no puede más que mostrar su desacuerdo con esta aseveración puesto que, tal y como ha quedado demostrado a posteriori, las medidas implementadas por Endesa fueron totalmente efectivas para prevenir cualquier tipo de daño en los interesados. De no haber sido así, Endesa, o incluso la propia AEPD, hubiese recibido alguna reclamación por estos motivos (cuando no ha sido así).

Alega ENDESA que es por esta razón, y por el hecho de que, a finales de marzo de 2022 (cuando se realizó la notificación) Endesa: (i) ya se encontraba en contacto con la mayoría de los interesados afectados, prestándoles asistencia personalizada y atajando cualquier consecuencia que la violación hubiese podido acarrear; (ii) ya había bloqueado cualquier acceso a las plataformas ******HERRAMIENTA.1 y ***HERRAMIENTA.2*** por parte de los usuarios comprometidos y había implementado medidas de autenticación multifactor; y (iii) ya conocía que las intenciones de las personas que habían hecho uso de los usuarios comprometidos no eran, como indica la AEPD, la suplantación de identidad o la obtención de más datos a través de ingeniería social, que Endesa determinó (y así informó a los interesados) que las medidas adoptadas evitaban cualquier riesgo futuro.

De hecho, indica ENDESA que la propia plataforma ******HERRAMIENTA.1***, por la forma en la que está y estaba configurada con anterioridad a la violación de la seguridad de los datos, impide la realización de descargas masivas de datos personales (las consultas se realizan a nivel individualizado, es decir, para acceder a los datos de una persona en particular, es necesario introducir primero un código de punto de suministro), por lo que el riesgo identificado en la Propuesta de Resolución relativo a la posibilidad de que los datos podrían ser utilizados para otras finalidades (p.ej. obtención de más datos a través de ingeniería social) era sumamente bajo y, por tanto, despreciable de cara a la realización de la notificación a los interesados.

Considera ENDESA que haber informado de lo contrario, cuando a través de otros canales los equipos de Endesa ya se encontraban prestando una atención personalizada a los interesados y atajando cualquier consecuencia que estos pudieran haber sufrido,

hubiese llevado a que estos recibiesen mensajes contradictorios que, lejos de resultar informativos y útiles, hubiesen creado una falsa sensación de peligro que, a finales de marzo de 2022, ya no existía (tal y como ha quedado plenamente comprobado a posteriori, a su juicio).

La AEPD considera, a juicio de ENDESA de manera errónea y totalmente desproporcionada, que la aseveración incluida en la comunicación a los afectados relativa a que la confidencialidad y la integridad de los datos no se había visto comprometida, debe ser sancionada con 800.000 euros cuando, dicho sea de paso, la modificación de la redacción en el sentido propuesto por la AEPD no hubiese cambiado en nada el fin que se pretende con esta notificación (que no es otro que los interesados puedan tomar medidas para evitar el riesgo), puesto que el riesgo, como ya se ha expuesto anteriormente, ya se encontraba totalmente mitigado y/o se estaba atajando por parte de los equipos especializados de Endesa en el momento de realizar dicha notificación.

Adicionalmente, y tal y como ocurría en relación a la sanción propuesta por la presunta vulneración del artículo 33 del RGPD, la AEPD, en su Propuesta de Resolución, vuelve a justificar la imposición de esta sanción (por presunto incumplimiento del artículo 34 del RGPD) en aspectos puramente subjetivos, sin motivar, de manera rigurosa, a su juicio, por qué considera que la actuación de Endesa (la cual, a su entender, se realizó con la máxima diligencia, haciendo una interpretación razonable de la normativa y las directrices aplicables) es merecedora de un reproche tan desproporcionado.

Al respecto, esta Agencia se reitera en que el análisis realizado por ENDESA cuando determinó que la violación de la seguridad de los datos personales no debía ser comunicada a los afectados no fue adecuado, razón por la que la Directora de esta Agencia ordenó a ENDESA que realizara la comunicación a que hace referencia el artículo 34 del RGPD.

En cuanto a la afirmación de ENDESA de que no se constató un riesgo elevado para los derechos y libertades de las personas, esta Agencia se reitera en que no todos los riesgos tienen que ver con contrataciones fraudulentas de productos de ENDESA, sino que los riesgos podrían ser de otra índole, toda vez que los afectados podrían ser, por ejemplo, víctimas de phishing o de ingeniería social, de otro ciberataque o de cambio de compañía de suministros, ser víctimas de suplantación de identidad y fraude, de todo lo cual no tendría conocimiento ENDESA. El hecho de que esos datos se hubieran visto vulnerados hace que sus titulares hubieran perdido el control sobre los mismos y que pudieran utilizarse de manera ílicita, no sólo en ese momento sino en el futuro.

En cuanto al Documento número 2 aportado por ENDESA con las alegaciones a la propuesta de resolución del presente procedimiento, las actuaciones de la empresa a que se hace referencia son únicamente respecto de las contrataciones fraudulentas llevadas a cabo por ******EMPRESA.1***. Al respecto, esta Agencia se reitera en que el alcance de la violación de la seguridad de los datos personales excedió de lo que pudo comunicar ******EMPRESA.1***, ya que se vieron comprometidos más usuarios de los que comunicaron estos proveedores y los datos obrantes en ******HERRAMIENTA.1 y ***HERRAMIENTA.2*** quedaron expuestos a más personas, no únicamente a aquellos que trabajaban en estas empresas.

En cuanto a la forma por la cual ENDESA comunicó el incidente a los interesados (información por capas), esta Agencia no ha realizado reproche alguno dado que no es una cuestión de forma lo que se considera infringido por ENDESA, sino que esta Agencia entiende que el contenido de dicha comunicación no cumple con lo exigido en el artículo 34 del RGPD.

En especial, en lo referido a las posibles consecuencias del incidente, si el fin perseguido por ENDESA era que los afectados se pusieran en contacto con el DPD para poder explicar las consecuencias en cada caso concreto, debió quedar ello meridianamente claro. Pretender que con la frase "*Puedes consultar nuestra política de privacidad en www.endesa.com/es/proteccion-datos-endesa, donde encontrarás la información relativa al tratamiento de tus datos personales. Si lo prefieres, puedes contactar directamente con nuestro Delegado de Protección de Datos enviando una comunicación a ***EMAIL.1 para conocer el detalle de las medidas adoptadas u obtener más información"* deba interpretarse que lo que ENDESA desea es que los afectados se pongan en contacto con el DPD para conocer las posibles consecuencias para su persona que el incidente pudiera tener, es un argumento que esta Agencia no comparte en absoluto y que considera imposible de defender.

También desea esta Agencia señalar que el hecho de considerar que con su actuación ENDESA ha infringido el artículo 34 del RGPD no se contradice en ningún momento con la posibilidad de utilizar un modelo por capas para proporcionar la información exigida por dicho artículo ni contradice la propia infografía de la AEPD. Se insiste en que no se considera infringido el artículo 34 del RGPD por un defecto de forma sino que se considera que el contenido de tal comunicación no ha cumplido con lo exigido por la normativa.

En cuanto a que la información proporcionada en tal comunicación era veraz porque cuando se realizó la comunicación en marzo de 2022 ya se habían adoptado medidas que habían subsanado la violación de la seguridad de los datos personales comprometidos, esta Agencia no comparte tal interpretación. Aun cuando se considerase que ello era cierto y se hubieran mitigado los riesgos para los derechos y libertades de los afectados, no es menos cierto que la confidencialidad e integridad de los datos personales sí que se había visto comprometida y así debió constar en la comunicación dirigida a los interesados.

Tampoco comparte esta Agencia la opinión de ENDESA de que los datos comprometidos no pudieran ser utilizados para otras finalidades, tal y como se ha explicado anteriormente. En este sentido, esta Agencia se reitera en que ENDESA (y esta Agencia) no habría tenido conocimiento de los posibles incidentes que hubieran podido derivarse del incidente en cuestión, ya que los riesgos no son únicamente la posible contratación fraudulenta de productos de ENDESA.

El hecho de que la plataforma ******HERRAMIENTA.1*** no pudiera realizar descargas masivas de datos personales, no es óbice para considerar que los datos obtenidos hubieran podido ser utilizados para otras finalidades, en especial, teniendo en cuenta que la propia ENDESA era incapaz de conocer cuántos registros habían sido obtenidos durante los meses que duró el incidente. Por tanto, esta Agencia de ninguna manera considera dicho riesgo como "despreciable" de cara a la comunicación del incidente a los interesados.

Tampoco está de acuerdo esta Agencia con la afirmación de que lo contrario habría llevado a recibir mensajes contradictorios y a crear una falsa sensación de peligro. Más bien al contrario, esta Agencia considera digno de reproche que con el mensaje de ENDESA se dio una falsa sensación de ausencia de riesgos, lo cual considera no era real, por los motivos anteriormente explicados.

En cuanto a que el importe de la multa por la infracción del artículo 34 del RGPD (800.000 euros) no es proporcionada porque el riesgo estaba totalmente mitigado por ENDESA, esta Agencia se reitera en que ello no era así, ya que ENDESA se centra única y exclusivamente en los riesgos de una contratación fraudulenta de productos de ENDESA y no en otros riesgos. El riesgo para los derechos y libertades de los interesados sigue existiendo porque éstos han perdido el control de sus datos.

Por último, esta Agencia desea señalar que de ninguna manera se justifica la imposición de dicha sanción en aspectos puramente subjetivos ni sin motivar por qué ENDESA no ha actuado diligentemente. Al contrario, se ha detallado los motivos por los que ENDESA debió realizar la comunicación exigida por el artículo 34 del RGPD, la cual no fue realizada debidamente por ENDESA, infringiendo lo dispuesto por la normativa aplicable.

Por lo demás, esta Agencia se reitera en lo contestado al respecto en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento sancionador.

Por todo lo expuesto, se desestima la presente alegación.

Cuarta.- De la improcedencia de la sanción impuesta por presunta infracción del artículo 44 del RGPD

Alega ENDESA que, en lo que respecta a la sanción impuesta por supuesta vulneración del artículo 44 del RGPD, existen diversos vicios proce***PLATAFORMA.1 y de fondo que, de mantenerse en la resolución que se dicte, serían causa de nulidad absoluta de la misma.

4.1 Indica ENDESA que, en el ámbito procesal, la Agencia ha comenzado con una imputación directa en el Acuerdo de Inicio del presente procedimiento, sin fundamento alguno y sin soporte fáctico de ningún tipo. El Acuerdo de Inicio incluye una sanción de, nada más y nada menos, que dos millones de euros (2.000.000€), por no cumplir las obligaciones establecidas en el RGPD para las transferencias internacionales de datos. El Acuerdo agravaba esta infracción, además, por una supuesta negligencia grave, dado que "*han transcurrido más de cuatro años desde que resulta aplicable el RGPD, no obstante lo cual ENDESA no ha adecuado las transferencias internacionales de sus datos personales a lo exigido* (…)".

A ENDESA le resulta seriamente desconcertante este enfoque del Acuerdo de Inicio, y la forma en que se ha continuado manteniendo esta sanción en la Propuesta de Resolución, puesto que:

a) La Agencia parece referirse al estado de cumplimiento de Endesa en materia de transferencias internacionales a fecha del inicio del procedimiento (cuando hace refe-

rencia a los más de cuatro años desde la obligatoriedad de cumplimiento del RGPD), en lugar de referirse a la fecha de los hechos objeto del procedimiento.

Al respecto, esta Agencia desea señalar que, en este caso, Endesa no dio cumplimiento a lo dispuesto Decisión de Ejecución 2021/914 a pesar de la prórroga concedida en la mima y continuó realizando transferencias internacionales a ***EMPRESA.15** sin evaluar si la normativa interna de ***PAÍS.2 permitía garantizar el nivel de protección elevado que confiere el RGPD a los interesados, lo que denota una mayor intensidad en la falta de diligencia, por cuanto tras la STJUE de 16/07/2020 Endesa era consciente de las limitaciones que podían suponer para los derechos y libertades de las personas la realización de transferencias internacionales a un tercer país cuya normativa interna podía no garantizar un nivel de protección adecuado, circunstancia que se agrava con la persistencia temporal del incumplimiento, razones que permiten aplicar la agravante de culpabilidad.

Por lo que se desestima la presente alegación.

b) La Agencia, a pesar de haber conocido la existencia de prestadores de servicio fuera de la Unión Europea durante la exhaustiva labor de investigación previa que llevó a cabo, en ningún momento solicitó a Endesa justificación o información alguna sobre los mecanismos aplicados por Endesa para realizar esas transferencias internacionales de datos. Sin embargo, incluye una sanción por este motivo por un importe absolutamente inédito.

Con respecto a esta falta de indagación previa, la Propuesta de Resolución señala que las actuaciones previas no son obligatorias, según el artículo 67 de la LOPD-gdd. Coincide ENDESA en esta afirmación, pero lo que también es cierto, y entiende no ofrece dudas, es que no se puede imponer una sanción sin haber realizado una mínima investigación del hecho supuestamente imputado, o sin tener el más mínimo indicio de la existencia de un hecho constitutivo de infracción o, al menos, sin haber realizado una mera consulta sobre la existencia del hecho por el que se quiere sancionar. La imputación de un hecho inexistente y no comprobado, junto con la enorme cuantía de la multa aparejada a tal hecho inexistente, es lo que resulta realmente sorprendente.

Al respecto, esta Agencia desea señalar que, según determina el artículo 67.1 de la LOPDGDD: "*Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación …*" Por tanto, la realización de estas actuaciones de investigación no resulta preceptiva.

No obstante, no es cierto que no se realizara ninguna actuación tendente a comprobar si existían garantías que ampararan las transferencias internaciones y, en su caso, determinar la posible existencia de infracción del artículo 44 del RGPD. Así, se pudo constar que ni en los contratos con sus proveedores aportados por Endesa ni en las Condiciones Generales de Contratación que tiene publicadas en su página web: https://globalprocurement.enel.com/es/documentos/condiciones-generales-contratacion se hacía referencia a la existencia de garantías adecuadas, por lo que cuando se acordó el inicio del procedimiento sancionador si existían indicios de una posible infracción.

Por lo que se desestima la presente alegación.

c) Alega ENDESA que, considerando que la violación de seguridad fue notificada el 10 de febrero de 2022, no es hasta el 26 de junio de 2023, durante la fase probatoria del expediente -esto es, más de dieciséis meses después y solo porque Endesa ha puesto de manifiesto la incorrección de la imputación-, cuando la AEPD solicita, por primera vez, información al respecto de las transferencias internacionales, siendo facilitada por Endesa puntualmente, para acreditar la regularidad de los mecanismos empleados. Señala ENDESA, además, que la Agencia no sólo solicitó información sobre la forma en que se llevaban a cabo las transferencias en el momento de los hechos, sino en la actualidad. Por tanto, ENDESA tiene la impresión de que se pretenden buscar argumentos para mantener una imputación inicialmente realizada sin soporte fáctico alguno, reorientándola hacia otro supuesto que nada tiene que ver con los hechos objeto del procedimiento. Y, además, que la información solicitada se refiere a requisitos que no solo no existen ni existían en ninguna norma imperativa, sino que, como se argumentará más adelante, no existían de forma claramente identificada en las fechas en que ocurrieron los hechos (de hecho, incluso a fecha actual considera ENDESA tremendamente dudoso que se pueda defender que una Evaluación de una Transferencia Internacional sea más o menos correcta utilizando una u otra metodología).

Al respecto, esta Agencia desea señalar que la propuesta de resolución no modifica la imputación, que sigue siendo la infracción del artículo 44 RGPD por la falta de garantías para la realización de las correspondientes transferencias internacionales. Las cláusulas contractuales suscritas entre las partes pueden no tener carácter vinculante para las autoridades de ***PAÍS.2 y por tanto pueden no ser suficientes para garantizar una protección adecuada, por ello la cláusula 14 de la Decisión de Ejecución contempla la necesidad de garantizar, a través de una adecuada evaluación de la legislación del país de que se trate, un nivel de protección equivalente al garantizado dentro de la Unión por el RGPD. La falta de evaluación sobre los aspectos contemplados en esta cláusula conlleva que no pueda considerarse aportada la garantía que la misma pretende ofrecer y, por tanto, que no se garantice que la transferencia esté sujeta a garantías adecuadas en el sentido del artículo 46.1.c) del RGPD.

Así se recoge en el considerando (19) de la Decisión de Ejecución: "*La transferencia y el tratamiento de datos personales en virtud de cláusulas contractuales tipo no deben producirse si el Derecho y las prácticas del tercer país de destino impiden que el importador de datos cumpla dichas cláusulas (…). Las partes deben garantizar que, en el momento de someterse a las cláusulas contractuales tipo, no tienen motivos para creer que el Derecho y las prácticas aplicables al importador de datos no se ajustan a estos requisitos*", lo que se garantiza a través de la evaluación a que se refiere la letra b) de la cláusula 14.

Como también se infiere de la SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 16 de julio de 2020.

> *"102 El órgano jurisdiccional remitente desea asimismo saber qué elementos deben tomarse en consideración para determinar la adecuación del nivel de protección en el contexto de una transferencia de datos personales a un país tercero sobre la base de las cláusulas tipo de protección de datos adoptadas en virtud del artículo 46, apartado 2, letra c), del RGPD.*

103 A este respecto, si bien esa disposición no enumera los diferentes elementos que han de tenerse en cuenta para evaluar la adecuación del nivel de protección que debe respetarse en el marco de una transferencia de esas características, el artículo 46, apartado 1, del referido Reglamento precisa que los interesados deben gozar de garantías adecuadas y contar con derechos exigibles y acciones legales efectivas.

104 La evaluación requerida a tal efecto en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales transferidos, los elementos pertinentes del sistema jurídico de dicho país. En lo que a este último aspecto se refiere, los elementos que deben tomarse en consideración en el contexto del artículo 46 del antedicho Reglamento se corresponden con los mencionados, de modo no exhaustivo, en el artículo 45, apartado 2, de este.

105 Por tanto, procede responder a las cuestiones prejudiciales segunda, tercera y sexta que el artículo 46, apartados 1 y 2, letra c), del RGPD debe interpretarse en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45, apartado 2, del referido Reglamento".

En definitiva, la decisión de Ejecución 2021/914 de la Comisión de 4 de junio 2021 recoge la necesidad de realizar una evaluación de los elementos pertinentes del sistema jurídico del país en su cláusula 14, por lo que no puede afirmarse que en ausencia de una evaluación adecuada del derecho del país de destino se haya adoptado la garantía que la decisión de Ejecución contempla.

Por lo que se desestima la presente alegación.

d) En la Propuesta de Resolución la Agencia sigue imponiendo una sanción, ahora ya acotada a la supuesta insuficiencia del mecanismo de Evaluación de Impacto de la Transferencia (conocida como "TIA", las siglas en inglés de "*Transfer Impact Assessment*"), con la misma cifra anteriormente impuesta en el Acuerdo de Inicio por la su-

puesta ausencia absoluta de cobertura legal de las transferencias. Y, alega ENDESA que, a pesar de la información facilitada, impone una multa en una cantidad que es, probablemente, la más alta impuesta en toda la Unión Europea por insuficiencia de la TIA en transferencias internacionales (aunque es, también posiblemente, la única sanción impuesta en toda la Unión Europea por este motivo). Es decir, a pesar de que se modifica la imputación (ya no es la ausencia de mecanismos, sino la insuficiencia de los mismos), el importe de la sanción no se ve modificado.

Al respecto, esta Agencia se reitera en que no existe ninguna modificación en la imputación. No obstante, el importe de la sanción se ha modificado, tal y como se explicará más adelante.

e) Por otra parte, alega ENDESA, también en relación con la proporcionalidad, que el hecho de que la Agencia considere que el mecanismo de transferencia empleado no está suficientemente ejecutado (insuficiencia de la TIA) debería hacer decaer la causa modificativa de la responsabilidad consistente en apreciar una negligencia grave por no aplicar mecanismos adecuados para la transferencia. En este sentido, la Agencia aplicaba esa agravación porque señalaba que, habiendo transcurrido cuatro años desde la obligatoriedad del RGPD, no se habían adecuado las transferencias a la nueva normativa. Al apreciar ahora que el mecanismo empleado sí existe, aunque no se considera del todo correcto, claramente se pone de manifiesto que no existió negligencia de ningún tipo. La agravante desaparecería y, sin embargo, la cuantía de la sanción se mantiene.

Al respecto, esta Agencia se reitera en la falta de diligencia observada en la actuación de ENDESA que no dio cumplimiento a lo dispuesto Decisión de Ejecución 2021/914 a pasar de la prórroga concedida en la misma y continuó realizando transferencias internacionales a ******EMPRESA.15***. Si bien se constata que la transferencia realizada a ***PAÍS.1 finalizó antes de que se cumpliera el plazo previsto en la decisión de ejecución, por lo que procede por este motivo una aminoración de la sanción.

f) Además de ello, la Propuesta de Resolución señala que Endesa "*ha realizado transferencias internacionales a ***PAÍS.1 y ***PAÍS.2, y continúa realizando transferencias internacionales a ***PAÍS.2 (…)*". Sin perjuicio de que tal hecho no ha negado ENDESA en ningún momento, y de que tales transferencias se realizan con estricto cumplimiento de la normativa (según manifiesta), como se ha señalado en fase de prueba, el análisis de las transferencias internacionales realizadas por Endesa, tanto en las fechas de los hechos objeto del procedimiento sancionador como, especialmente, en la fecha actual, entiende ENDESA no pueden ser objeto de análisis específico en el marco del presente procedimiento sancionador. La Agencia estaría obrando una acumulación de diversos procedimientos sancionadores sin cumplir las normas establecidas en el ordenamiento jurídico para el desempeño de la potestad sancionadora de la administración.

En particular, alega que sin abrir un proceso específico sobre unos hechos concretos (los hechos inicialmente imputados, inexistencia de mecanismos que regularan las transferencias, eran inexistentes) y, adicionalmente, abriendo una especie de "pieza separada" de investigación sobre el particular en medio de la fase probatoria del expediente sancionador iniciado en relación con una violación de seguridad de datos personales, situando a Endesa en una posición de desprotección procesal y vulnerando su

derecho constitucional a la defensa, en su vertiente de acceso a la imputación desde el momento en que se produce y dándole la posibilidad de alegar sobre los hechos imputados (los hechos inicialmente contenidos en el Acuerdo de Inicio eran, a su juicio, inexistentes, por lo que el nuevo enfoque adoptado en la Propuesta de Resolución nunca pudo ser objeto de alegaciones por parte de Endesa).

Al respecto, esta Agencia desea señalar que consta en el acuerdo de inicio que ni en los contratos aportados con sus proveedores ni en las Condiciones Generales de Contratación que tiene publicadas en su página web: https://globalprocurement.enel.com/es/documentos/condiciones-generales-contratacion se hacía referencia a la existencia de las mismas. Por tanto, no se ha conculcado el derecho a la defensa. ENDESA ha podido formular alegaciones y aportar cuanto a su derecho ha considerado conveniente tanto al acuerdo de inicio como a la propuesta de resolución.

Por lo que se desestima la presente alegación.

g) Alega ENDESA que se impone una sanción por un requisito formal que no aparece recogido en el RGPD, ni en la LOPD-gdd, ni en ninguna otra norma de carácter imperativo del ordenamiento jurídico de la Unión Europea ("UE"). En concreto, el citado mecanismo de Evaluación de Impacto de la Transferencia que, en realidad, no es más que un mecanismo o metodología de análisis que se deriva de la Sentencia del Tribunal de Justicia de la Unión Europea ("TJUE") en el asunto Schrems II, pero que ni siquiera se establece en esa sentencia de forma detallada, sino que se desarrolla de forma progresiva a partir del año 2020 en diversas guías interpretativas de distintos organismos, tales como el CEPD, que todavía en junio de 2021 publicaba sus Recomendaciones 1/2021 sobre esta materia. Indica ENDESA que las guías del CEPD no constituyen derecho imperativo, sino que se configuran como guías interpretativas de la normativa que debe ser considerada como mejores prácticas o fórmulas de adecuación. Sin perjuicio de lo cual, indica Endesa que cumplió debidamente sus obligaciones de diligencia debida y responsabilidad proactiva, atendiendo a los requerimientos de la citada Sentencia y de las Recomendaciones del CEPD, llegando al extremo de aplicar las fórmulas de cumplimiento más rigurosas existentes entre los expertos en la materia. Fórmulas que, sin embargo, la Agencia considera que no son suficientes.

Sin duda, en su opinión, la sanción de 2.000.000€ por insuficiencia de la TIA, de mantenerse, será comentada entre los expertos en privacidad de toda la UE y del resto del mundo como un hito, una novedad y un primer caso de sanción por este motivo, y será criticada tanto por lo estricto de su interpretación de la Sentencia Schrems II como por el importe de la sanción impuesta.

Al respecto, esta Agencia desea señalar que el cumplimiento de la cláusula 14 de la Decisión de Ejecución no es un requisito formal sino un requisito necesario para que las transferencias internacionales se realicen con las debidas garantías para la protección de los derechos fundamentales de los interesados. No obstante, en cualquier caso, el importe de la sanción se ha minorado.

4.2. Adicionalmente a todo lo anterior, y ya en el ámbito material, niega ENDESA rotundamente haber incumplido con las obligaciones establecidas por el RGPD en relación con las transferencias internacionales, por los siguientes motivos:

a) En primer lugar porque, a diferencia de lo que señalaba la Agencia en el Acuerdo de Inicio, Endesa disponía de los mecanismos legalmente exigidos para poder realizar transferencias internacionales de datos fuera de la UE. En concreto, había firmado las cláusulas contractuales tipo de la UE válidas en el momento en que se utilizaron, es decir, el modelo aprobado por las decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE, que fueron perfectamente válidas hasta el 27 de diciembre de 2022, nada más y nada menos.

La Propuesta de Resolución desarrolla ampliamente los requisitos exigidos por la "Decisión de Ejecución (UE) 2021/914 de la Comisión Europea, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para las transferencias de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo" (en adelante, la "Decisión"). Alega ENDESA que nada tiene que ver el contenido de dicha Decisión con el objeto del presente procedimiento, puesto que esa Decisión aprobaba unos modelos de cláusulas contractuales tipo que pudieron convivir con las anteriores, perfectamente válidas estas hasta el 27 de diciembre de 2022.

Al respecto, cabe señalar que esta Agencia ha tenido en cuenta que los contratos celebrados antes del 27 de septiembre de 2021 con arreglo a la Decisión 2001/497/CE o a la Decisión 2020/87/UE podían mantenerse hasta el 27 de diciembre de 2022. Pero, a partir de esa fecha, ENDESA no ha cumplido con el requisito exigido en la cláusula 14 de la citada Decisión de Ejecución, razón por la que esta Agencia considera que ENDESA ha infringido el artículo 44 del RGPD, por lo que se desestima la presente alegación.

b) En segundo lugar, alega ENDESA que los mecanismos de refuerzo de las Cláusulas Contractuales Tipo fueron protocolos de análisis que se derivaban de la Sentencia del TJUE en el caso Schrems II en fecha 16 de julio de 2020. Pero la concreción de estos protocolos no fue ni fácil, ni rápida, ni unívoca, ni se ha incorporado a ningún tipo de norma con rango imperativo en la Unión Europea.

Indica ENDESA que el CEPD, tras publicar un primer documento titulado "*Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18*", se demora hasta el 18 de junio de 2021 para publicar su documento "*Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE*" (las "Recomendaciones"). Las Recomendaciones son incluso posteriores a la Decisión de la Comisión Europea.

Entrando al detalle, explica ENDESA que la Decisión se basa en la necesidad de que las partes firmantes (exportador e importador de datos) garanticen haber realizado una serie de análisis que, tal como cita la Agencia en su Propuesta de Resolución, se incorporan a las nuevas cláusulas contractuales tipo (que no son las que Endesa tenía en la fecha de ocurrencia de los hechos) por medio de declaraciones de las partes. Por su parte, las Recomendaciones establecen un esquema y una metodología de evaluación y análisis que puede permitir llegar a la conclusión de que la transferencia en concreto no supone un riesgo para los derechos y libertades de los interesados afectados, teniendo en cuenta todos los elementos relevantes, tales como la legisla-

ción del estado de destino, el tipo de datos transferidos o el perfil del destinatario, entre otros.

Alega ENDESA que ha aportado documentación suficiente al expediente para acreditar, en primer lugar, que disponía de un mecanismo legalmente válido para la transferencia (las cláusulas contractuales tipo de la Comisión todavía válidas en aquel momento) y, en segundo lugar, que había extremado la diligencia realizando una Evaluación de Impacto de la Transferencia, teniendo en cuenta ya los elementos citados en la sentencia Schrems II.

Entiende ENDESA que la Propuesta de Resolución no justifica la procedencia de la sanción que impone en este ámbito. No solo porque Endesa (a su juicio) sí ha acreditado haber cumplido fielmente con las obligaciones legales y con las mejores prácticas en la materia, tanto para el caso de ***PAÍS.1 como para el caso de ***PAÍS.2 (a pesar de la diferencia que parece ver la AEPD, en ambos casos se ha llevado a cabo una Evaluación de Impacto de la Transferencia y existían cláusulas contractuales tipo). Sino porque, entiende ENDESA que, si la AEPD considera que las transferencias de datos a ***PAÍS.1 y a ***PAÍS.2 incumplen el RGPD, debe señalar los motivos exactos por los que tiene tal consideración.

Y, si se trata de afirmar que el criterio de Endesa es equivocado y la legislación de ambos países no cumple con un nivel de seguridad suficiente, deberá señalar en qué aspectos la Agencia entiende que aquellos ordenamientos jurídicos incurren en tales deficiencias. Esto es especialmente relevante en el caso de estos dos países, ***PAÍS.1 y ***PAÍS.2, para cuyas transferencias la AEPD había autorizado expresamente dicha operación de tratamiento a Endesa en el marco del sistema jurídico anterior al RGPD. En opinión de ENDESA, resulta muy difícil de entender y justificar cómo, en este caso, una transferencia de datos expresamente autorizada por la Agencia, podría dejar de ser correcta cuando la legislación del país de destino sigue siendo la misma (o, incluso, puede haber mejorado con los años) y Endesa ha añadido, además, los análisis y métodos exigidos por la nueva legislación europea al respecto.

Al respecto, esta Agencia desea señalar que la cláusula 14 de la citada Decisión de Ejecución sí contiene un pronunciamiento preciso sobre la necesidad de tener en cuenta, para aportar la garantía, si el derecho y las prácticas del país de destino respetan los derechos y libertades de los interesados, y en particular indica que se deberán tener en cuenta los siguientes aspectos:

> *i) las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;*
>
> *ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables;*

iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

Sin embargo, la documentación aportada por ENDESA no evalúa el derecho y las prácticas de ***PAÍS.2 en relación con la exigencia de comunicar datos personales a las autoridades del país.

Entiende ENDESA que no es nada diferente al ejercicio realizado por el TJUE en la sentencia Schrems II, en el que fue desgranando uno por uno los motivos, casos, situaciones y ejemplos concretos por los que el Tribunal Europeo consideraba que el ordenamiento jurídico de los Estados Unidos no cumplía con las garantías suficientes que deben ser exigidas desde el punto de vista de la UE en cuanto a la seguridad de los datos. Aquel prolijo desglose detallado y fundamentado permitió al TJUE declarar la invalidez del acuerdo del *Privacy Shield*. Sin embargo, alega ENDESA que la Agencia, en el presente caso, determina que ha incumplido el RGPD porque, a pesar de que existe un mecanismo de transferencia válido (cláusulas contractuales tipo) y una evaluación de impacto de la privacidad, la transferencia de datos supone un riesgo para los derechos y libertades de los individuos. La inconcreción de esta imputación no puede ser sino motivo de nulidad absoluta (en opinión de ENDESA), como consecuencia de la falta de tipicidad de la actuación de Endesa.

Al respecto, esta Agencia desea señalar que no ha realizado ningún pronunciamiento sobre si el derecho de ***PAÍS.2 ofrece un nivel adecuado de protección o no, cuestión que ha de ser valorada y documentada por ENDESA para que pueda considerarse aportada la garantía contenida en la cláusula 14 de la Decisión de Adecuación y poder basar la transferencia en las cláusulas contractuales tipo contenidas en la Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021.

Por todo lo expuesto, se desestima la presente alegación.

c) Alega ENDESA que el nivel de inseguridad jurídica generado por la Sentencia Schrems II en cuanto a la forma de realizar transferencias internacionales de datos ha venido siendo una constante desde su publicación, hasta el punto de que, ni siquiera en la actualidad, existe un consenso absoluto sobre la forma de realizar los análisis necesarios previos a la realización de una transferencia de datos hacia fuera de la UE, más allá de las normas de “soft law” como las citadas Recomendaciones del CEPD. La grandísima mayoría de las empresas europeas a fecha actual, septiembre de 2023, todavía no saben qué tienen que cumplir ni cómo, y las que más o menos han hecho intentos de adaptarse a lo que se supone que exige la Sentencia Schrems II no pasan de realizar trabajos tentativos no validados por norma alguna. Obviamente, esta situación afecta al elemento de la culpabilidad como esencia del derecho administrativo sancionador.

En ese entorno, entiende ENDESA que imponer una sanción de 2.000.000€ por la supuesta insuficiencia de la TIA se presenta como una multa absolutamente improcedente, además de desproporcionada y extravagante. Afirma ENDESA que la inseguridad jurídica derivada de la indefinición del marco normativo no puede perjudicar a los operadores económicos, especialmente cuando demuestran haber desplegado toda la dili-

gencia debida para atender a unos requerimientos extremadamente complejos desde el punto de vista jurídico más especializado en una materia como es la normativa de protección de datos personales. Y, en paralelo, sin que la Agencia señale un solo punto en que la legislación del país de destino, así como la transferencia concreta, pueden suponer un riesgo para los derechos de los interesados, habiendo autorizado previamente exactamente la misma transferencia, como se ha dicho.

Al respecto, esta Agencia desea señalar que, sobre la culpabilidad de ENDESA, ya se ha hecho referencia a que la Decisión de Ejecución 2021/914 dispuso que los contratos celebrados antes del 27 de septiembre de 2021 basados en las Decisiones anteriores ofrecían garantías adecuadas hasta el 27 de diciembre de 2022. Por lo que Endesa conocía que a partir de dicha fecha su contrato debía incorporar las nuevas cláusulas contractuales que requieren evaluar si la normativa interna de ***PAÍS.2 garantiza la continuidad del nivel de protección.

Por lo que se desestima la presente alegación.

Quinta.- Sobre la graduación de la sanción impuesta a Endesa y la falta de proporcionalidad relativa de la Propuesta de Resolución

En la Propuesta de Resolución, la AEPD, en respuesta a la alegación realizada por Endesa de falta de proporcionalidad relativa de las sanciones propuestas a Endesa en comparación a las propuestas en otros expedientes (a juicio de ENDESA mucho más graves), expone ciertas razones que ENDESA entiende son del todo insuficientes para desestimar la alegación realizada por Endesa.

Y alega que, aunque la AEPD indique que cada caso es distinto y que debe analizarse según sus propias circunstancias, existen una serie de hechos objetivos y comparables (puesto que se recogen en la propia resolución sancionadora de la AEPD) que no dejan lugar a duda (en su opinión) en el sentido indicado por Endesa en sus alegaciones; es decir, que las sanciones propuestas en el marco de este expediente son del todo desproporcionadas.

En este sentido, detalla, por ejemplo:

a. En relación a la resolución de la AEPD relativa al procedimiento E/05937/2021, la cual finalizó con la imposición de una sanción de apercibimiento incluso cuando la notificación de la violación de seguridad de los datos a la AEPD se notificó, de conformidad con lo indicado por la AEPD en su resolución, "*en un plazo superior a las 72 horas desde que se tuvo conocimiento de que se había producido*", la AEPD indica, en la Propuesta de Resolución, que no se consideró infringido el artículo 33 del RGPD puesto que "*la responsable de tratamiento indicó debidamente los motivos de la dilación en la notificación a la autoridad de control*".

Explica ENDESA que el motivo para tal demora en el procedimiento E/05937/2021 fue que la notificación se retrasó "*debido a las investigaciones llevadas a cabo para esclarecer si hubo acceso de datos y/o actividad fraudulenta, lo que requirió múltiples análisis por parte de los equipos de seguridad".* A ENDESA le resulta sorprendente que, en este caso, al contrario de lo que indica la AEPD en la Propuesta de Resolución, la AEPD no considerase que "*la notificación de la brecha no debe realizarse después de*

que el responsable del tratamiento haya realizado un examen detallado de la situación sino cuando el responsable detecta que la brecha se ha producido, pudiendo realizase este análisis en paralelo con la notificación".

En este punto entiende ENDESA que se puede observar cómo, la AEPD, trata dos circunstancias, a su juicio idénticas (retraso en la notificación de la brecha), de distinta manera, demostrando una clara desproporcionalidad (en su opinión).

Al respecto, esta Agencia se reitera en que los hechos objeto de sendos expedientes no son comparables, tal y como se detalló en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento.

Por su parte, la propia ENDESA en la página 24 de sus alegaciones a la propuesta de resolución del presente procedimiento ha indicado que "no es cierto, como indica la Propuesta de Resolución, que Endesa no notificase el incidente en el primer momento en el que tuvo conocimiento de los anuncios publicados en Facebook puesto que se encontraba realizando un "*examen detallado de la situación*". Al contrario, Endesa realizó dicho examen de la situación nada más tuvo conocimiento de la misma, pero determinó, siguiendo las directrices de la AEPD y del CEPD al efecto, que no se alcanzaba el umbral de notificación previsto en el artículo 33 del RGPD".

Los motivos de la dilación de ENDESA en la notificación a la autoridad de control obedecieron a que no calificó debidamente el incidente como notificable, razón por la que esta Agencia considera que infringió el artículo 33 del RGPD.

Por lo que se desestima la presente alegación.

b. En relación a la resolución de la AEPD relativa al procedimiento PS/00118/2020, la cual finalizó con la imposición de una sanción de apercibimiento incluso cuando: (i) la notificación de la violación de seguridad de los datos a la AEPD se realizó dos meses después de que la entidad investigada tuviese constancia de la misma; (ii) la entidad investigada en este supuesto no aportó a la AEPD el análisis de riesgos de los tratamientos de los que es responsable (mientras que Endesa sí lo hizo); y (iii) la entidad investigada declaró que "*la máquina afectada por los incidentes de seguridad estaba técnicamente obsoleta*", por lo que no contaba con medidas de seguridad adecuadas al riesgo que conllevaba el tratamiento, la AEPD indica, en la Propuesta de Resolución, que "*el grado de reprochabilidad de la actuación del responsable de tratamiento permitía sustituir la imposición de una multa por un apercibimiento*".

A ENDESA le resulta sorprendente como, en un caso en el que el responsable del tratamiento: (i) notifica una violación de seguridad de forma tardía (con 2 meses de retraso) sin razón alguna aparente (en su opinión), cuando en el caso que nos ocupa Endesa ha justificado cómo llevo a cabo, hasta en tres ocasiones, análisis de riesgos de la violación determinando, en el último de ellos, que era probable que ésta supusiese un riesgo para los derechos y libertades de los interesados); y (ii) no cuenta, en su opinión, con las mínimas medidas de seguridad exigibles (realización de análisis de riesgos y mantenimiento de sistemas actualizados), cuando Endesa realizó el correspondiente análisis de riesgos que facilitó a la AEPD y contaba con medidas de seguridad que, en opinión de ENDESA, era adecuadas al riesgo, la AEPD entiende que su con-

ducta no es merecedora de reproche, mientras que, en el presente caso, no solo entiende lo contrario, sino que propone imponer las mayores sanciones hasta la fecha.

Al respecto, esta Agencia se reitera en las diferencias señaladas en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento: entre otras, el incidente duró solo tres días y afectó a 75.000 interesados máximo, frente al incidente de ENDESA que duró meses y afectó a millones de interesados, y se consideró que el grado de reprochabilidad de la actuación del responsable de tratamiento permitía sustituir la imposición de una multa por un apercibimiento, lo cual no ocurre en el presente procedimiento sancionador contra ENDESA. Además, esta Agencia se reitera en que las medidas adoptadas por ENDESA con anterioridad al incidente no eran las apropiadas en función del riesgo.

El considerando 148 del RGPD permite sustituir la imposición de una multa por un apercibimiento, en atención a "*la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante*."

En el presente caso, esta Agencia ha valorado tales circunstancias para cada una de las infracciones (todo lo cual se detalla en los Fundamentos de Derecho VI, IX, XII, XV, XVIII, respectivamente) y ha considerado que lo que corresponde en las presentes infracciones es no sustituir la sanción de multa por apercibimiento.

Por lo que se desestima la presente alegación.

c. En relación a la resolución de la AEPD relativa al procedimiento PS/00254/2019, la cual finalizó con la imposición de una sanción de apercibimiento incluso cuando la AEPD consideró que, de las investigaciones llevadas a cabo, se apreciaba una falta de diligencia del responsable en la implementación de medidas de seguridad relevantes, indicando incluso que "*la ausencia de consideración del riesgo que puede suponer el acceso no autorizado por terceros a datos de suscriptores de información relacionada con un partido político, y su posterior difusión pública, agrava el reproche culpabilístico y sancionador de la conducta*".

De nuevo sorprende a ENDESA cómo la AEPD, en un caso en el que (a su juicio) la propia AEPD claramente indica que el responsable del tratamiento no tuvo en consideración el riesgo que podía suponer el acceso no autorizado a datos de suscriptores de información relacionada con un partido político, y su posterior difusión pública y que, por ello, esto "*agrava el reproche culpabilístico y sancionador de la conducta*", indica, en la Propuesta de Resolución, que "*las circunstancias de la brecha difieren de la actuación tan gravemente negligente de ENDESA*".

Entiende la AEPD que la actuación de Endesa, la cual en el marco de este procedimiento y, entre otros: (i) había analizado el riesgo que suponía para los interesados el tratamiento comprometido; (ii) había implementado medidas de seguridad adecuadas (en su opinión) al riesgo de conformidad con los estándares de la industrias; (iii) ha realizado hasta 3 análisis de riesgos en relación al impacto que el incidente puede te-

ner sobre los derechos y libertades de los interesados afectados; (iv) ha implementado, tras la brecha, medidas de seguridad para tratar de evitar que una violación de la seguridad vuelva a ocurrir y ha atendido a los interesados afectados de manera que el posible riesgo identificado no haya llegado a materializar; y (v) ha contestado a 5 requerimientos de información emitidos por parte de esta AEPD, merece un reproche mayor (insiste, el mayor reproche hasta la fecha en cuanto a violaciones de seguridad se refiere) que una entidad que ni siquiera había tenido en consideración el riesgo que podía suponer el acceso a categorías especiales de datos.

Al respecto, esta Agencia se reitera en que las medidas de seguridad adoptadas por ENDESA antes del incidente no eran apropiadas en función del riesgo, que si bien realizó tres informes de la brecha no calificó correctamente el incidente como notificable, que en el mejor de los casos lo que ha mitigado es únicamente el riesgo de una contratación fraudulenta de productos de ENDESA, y que contestar los requerimientos de información de esta Agencia es una obligación legal establecida por la normativa aplicable cuya infracción puede ser objeto de un procedimiento sancionador específico.

En cuanto al párrafo de la resolución del PS/00254/2019 citado por ENDESA, éste hacía referencia únicamente a que la entidad no había considerado que los datos de contacto para el envío de una newsletter relativa a un partido político pudieran ser considerados categorías de datos especialmente protegidos, ya no por los datos expuestos en sí sino por su posible combinación con otras fuentes.

En cualquier caso, no es menos cierto que en tal resolución se consideró apropiado sustituir la sanción de multa por un apercibimiento en atención a, entre otros, la diligencia llevada a cabo por la entidad en lo referente a la comunicación sin dilación de la violación de seguridad a esta Agencia Española de Protección de Datos, lo cual no ha acontecido en el presente caso.

Por lo que se desestima la presente alegación.

Teniendo en cuenta todo lo anterior, considera ENDESA que es patente la disparidad de criterios que la AEPD aplica a la hora de analizar las medidas de seguridad implementadas por las entidades investigadas por la AEPD, así como las consecuencias que, en materia de sanciones administrativas, se derivan de las presuntas infracciones contenidas en Propuesta de Resolución y, por tanto, se reitera en la falta de proporcionalidad relativa (y absoluta) de la Propuesta de Resolución.

Al respecto, esta Agencia se reitera en todo lo anteriormente expuesto, por lo que se desestima la presente alegación.

Por último, ENDESA reitera, tal y como hizo en el marco de las alegaciones al Acuerdo de Inicio, su desacuerdo con la aplicación de las circunstancias que la AEPD considera agravantes de la conducta de Endesa. Sin perjuicio de que ENDESA considera que su actuación en el marco de este expediente ha sido plenamente diligente y, por tanto, no debería ser objeto de reproche alguno (y menos de un reproche tan desproporcionado como el propuesto en la Propuesta de Resolución), para el supuesto de que la AEPD siga entendiendo que esto no es así, ENDESA entiende que:

(i) No debería apreciarse, como circunstancia agravante, una "*grave falta de diligencia*" por parte de Endesa. Como se ha expuesto en las alegaciones anteriores, considera ENDESA que todas las actuaciones de Endesa en el marco de este expediente se realizaron: (a) siguiendo una interpretación razonable de la normativa de protección de datos aplicable y las directrices interpretativas publicadas por la propia AEPD y el CEPD; y (b) con la máxima diligencia posible en un momento de máxima preocupación en la compañía por lo ocurrido.

En este sentido, dado que ha quedado acreditado, de conformidad con lo indicado en las alegaciones anteriores, alega ENDESA que:

(a) el informe elaborado por ******EMPRESA.1*** es totalmente parcial, y subjetivo, y sobre el mismo se proyecta una fundada sospecha de haber sido elaborado interesadamente con mucha posterioridad a la ocurrencia de los hechos por lo que no debería ser tenido en cuenta en el marco de este expediente;

(b) Endesa no se dirigió a Facebook Irlanda conscientemente dado que no quería aceptar la jurisdicción irlandesa a efectos de una posible reclamación judicial o administrativa posterior (no a efectos de protección de datos) y hacerlo no tenía ninguna utilidad práctica de cara a la protección de los derechos y libertades de los interesados afectados (las credenciales de ******HERRAMIENTA.2 y ***HERRAMIENTA.1*** comprometidas, excepto una, ya habían sido deshabilitadas);

(c) Endesa tenía implementadas (en su opinión), en sus sistemas, medidas de seguridad adecuadas al riesgo (tal y como se desprende de los análisis de riesgos facilitados a la AEPD, del informe forense presentado ante la AEPD y del hecho de que, durante años, no se produjo ningún incidente similar);

(d) Endesa desplegó, una vez tuvo conocimiento del incidente y con la mayor diligencia posible, medidas adecuadas (en su opinión) para deshabilitar las cuentas comprometidas en el menor tiempo posible (nunca transcurrieron, tal y como indica la Propuesta de Resolución, varios meses entre que Endesa tuvo conocimiento del compromiso de cuentas y su deshabilitación);

(e) Endesa, a la hora de realizar los primeros análisis sobre la necesidad de notificación de la violación de la seguridad a la AEPD realizó una interpretación razonable (en su opinión) y fundada en la normativa y las directrices publicadas sobre la materia y procedió a notificar la violación a la AEPD en el plazo de 24 horas desde que tuvo constancia de que la misma podría suponer un riesgo (real) para los derechos y libertades de los interesados. Resulta, a todas luces, insostenible para ENDESA mantener que "todo incidente" debe comunicarse a la AEPD;

(f) Endesa, a la hora de realizar la notificación del incidente a los interesados afectados, siguió (en su opinión) lo indicado en las directrices e infografías de la AEPD, informando a los interesados de aquellos aspectos que, dado el tiempo transcurrido desde que se produjo la violación, era más útiles para éstos; y

(g) Endesa ha cumplido y cumple (en su opinión), de manera completamente escrupulosa, con la obligación de implementación de garantías adecuadas para la realización de transferencias internacionales,

ENDESA considera que la aplicación de la agravante de grave falta de diligencia por parte de la AEPD es totalmente improcedente y desproporcionada, y no responde a la realidad de las actuaciones llevadas a cabo por Endesa.

Al respecto, esta Agencia se reitera en lo contestado a las alegaciones al acuerdo de inicio y a la propuesta de resolución del presente procedimiento sancionador:

(a) La determinación de la comisión de infracciones por parte de ENDESA, así como la negligencia grave por su parte, ha quedado acreditada a lo largo del presente procedimiento no con el informe de ******EMPRESA.1***, sino con toda la documentación obrante en el expediente, y ningún contenido del citado informe se cita en los Fundamentos de Derecho para fundamentar ni las infracciones ni la graduación del importe de las sanciones, más allá de las respuestas a las alegaciones presentadas por ENDESA al respecto;

(b) ENDESA tardó más de un mes en deshabilitar las credenciales y aunque quedara solo una credencial sin deshabilitar, con ella era suficiente para acceder a los datos personales obrantes en los sistemas de ENDESA. Por lo demás, esta Agencia se reitera en que solo es competente para valorar si ENDESA cumplió con la normativa de protección de datos personales y no para valorar cuestiones vinculadas a la propiedad intelectual u otros ámbitos. En este sentido, en el presente caso, se había publicado una serie de anuncios ofreciendo acceso a los sistemas de ENDESA, que permitía el acceso a datos personales titularidad de ENDESA, que trataba en su calidad de responsable de tratamiento. Y como tal, debió adoptar una serie de medidas, entre otras, que tales anuncios fueran retirados. Si para ello era necesario acudir a Facebook Irlanda, pues eso es lo que se debió hacer. Por último, ENDESA tampoco tenía la certeza de que los usuarios comprometidos eran únicamente aquéllos de los que tenía conocimiento, por lo que resultaba necesario el auxilio de Facebook para retirar los anuncios en cuestión;

(c) Esta Agencia se reitera en que ENDESA no contaba, antes del incidente, con las medidas de seguridad apropiadas en función del riesgo (y el informe forense no señala nada al respecto, sino que analiza las medidas implementadas a la fecha del informe). El hecho de que no se hubiera producido ningún incidente similar del cual ENDESA tuviera conocimiento, no implica de ninguna manera de que las medidas de seguridad fueran las apropiadas sino simplemente eso, que ENDESA no tuvo constancia de ningún incidente similar. Tampoco adoptó durante el incidente de seguridad medidas adecuadas para mitigar de una manera efectiva el riesgo y ello sin perjuicio de que adoptara una serie de medidas, tales como, el reseteo de las contraseñas de los usuarios, el seguimiento de las publicaciones en Facebook, intentar dar de baja los citados anuncios, deshabilitar la posibilidad de mantener sesiones simultáneas y ampliar la trazabilidad de los accesos a ******HERRAMIENTA.1***;

(d) ENDESA tuvo conocimiento el 24 de agosto de 2021 que había anuncios publicados en Facebook vendiendo credenciales de acceso a sus sistemas y en su primer informe de la violación de la seguridad de los datos personales, de 14 de septiembre de 2021, ya se había comprobado la validez de los accesos. En cualquier caso, el 27 de octubre de 2021, ENDESA recibió un correo electrónico de ******EMPRESA.1*** indicando que había cinco usuarios comprometidos y no fue hasta el 29 de noviembre de 2021 que se deshabilitaron. Es decir, las cuentas no se deshabilitaron hasta transcurrido más de un mes.

(e) Esta Agencia de ninguna manera sostiene que deba notificarse a la autoridad de control "todo incidente". Pero en el presente caso, esta Agencia considera que ENDESA no ha realizado una interpretación adecuada sobre si la violación de la seguridad de los datos personales era notificable por implicar un riesgo para los derechos y las libertades de las personas físicas, tal y como se detalla ampliamente en los Fundamentos de Derecho de la presente resolución.

(f) ENDESA no ha proporcionado debidamente a los interesados la información requerida por el artículo 34 del RGPD, tal y como se detalla ampliamente en los Fundamentos de Derecho de la presente resolución.

(g) Endesa ha cumplido y cumple (en su opinión), de manera completamente escrupulosa, con la obligación de implementación de garantías adecuadas para la realización de transferencias internacionales, ENDESA no ha cumplido debidamente con las obligaciones establecidas por el artículo 44 y siguientes del RGPD, tal y como se detalla ampliamente en los Fundamentos de Derecho de la presente resolución.

ENDESA considera que la aplicación de la agravante de grave falta de diligencia por parte de la AEPD es totalmente improcedente y desproporcionada, y no responde a la realidad de las actuaciones llevadas a cabo por Endesa.

Al respecto, esta Agencia se reitera en todo lo detallado en la respuesta a las alegaciones al acuerdo de inicio y propuesta de resolución del presente procedimiento.

Y por todo lo expuesto, considera que la actuación de ENDESA ha sido gravemente negligente, por lo que desestima la presente alegación.

(ii) Alega ENDESA que no debería apreciarse, como circunstancia agravante, la "*vinculación de la actividad del infractor con la realización de tratamientos de datos personales*". Como ya indicó en las alegaciones al Acuerdo de Inicio, la actividad de comercialización de energía eléctrica supone, por supuesto, que Endesa esté habituada "*al tratamiento de datos personales*", pero que ello suponga una agravación cuando la mayoría de empresas a nivel mundial tratan datos de clientes y terceros y realizan una actividad que conlleva estar en permanente contacto con ellos resulta difícil de percibir, puesto que, de ser este el caso, se estaría aplicando esta circunstancia agravante (que debería ser excepcional) a la gran mayoría de los casos analizados por la AEPD, desvirtuando completamente la naturaleza de dicha agravante (como así está sucediendo fruto de la aplicación, a juicio de ENDESA desmesurada, que la AEPD está llevando a cabo de esta circunstancia agravante).

Al respecto, esta Agencia se reitera en que el legislador español ha incluido en la LOPDGDD tal circunstancia a la hora de graduar la imposición de una sanción, y que ello es lo que hace esta Agencia, tomar en consideración tal circunstancia.

Y que no es lo mismo a efectos de decidir sobre la imposición de una multa administrativa la consideración de una infracción producida por una persona física o una empresa pequeña no habituada al tratamiento de datos personales, que la de una gran empresa como ENDESA, acostumbrada al tratamiento de datos personales de millones de clientes y no clientes, con una larga trayectoria a sus espaldas al respecto. Por supuesto que se considera que la infracción es más grave a los efectos de imponer una multa si el responsable del tratamiento se encuentra entre los segundos, como es el caso de ENDESA. Y así lo ha señalado la Audiencia Nacional en su SAN 65/2017, de siete de febrero de dos mil diecisiete, al recoger la doctrina del Tribunal Supremo, "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 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 exquisito cuidado por ajustarse a las prevenciones legales al respecto".

Adicionalmente, y en aras de la brevedad, se reitera ENDESA en lo ya indicado en su escrito de alegaciones al Acuerdo de Inicio respecto de la falta de aplicación, en la Propuesta de Resolución, de atenuantes respecto de la conducta de Endesa, como son: (i) las medidas tomadas por Endesa para paliar los daños y perjuicio sufridos por los interesados (como se ha acreditado, Endesa, con anterioridad al inicio de este expediente, ya había adoptado las medidas de protección técnicas y organizativas apropiadas, en su opinión, para garantizar que no se materializara riesgo alguno para los derechos y libertades de los interesados afectados y les había proporcionado asistencia individual y personalizada al efecto); (ii) la cooperación con la autoridad de control (Endesa ha contestado, en tiempo y forma, hasta 6 requerimientos emitidos por la AEPD); y (iii) la falta de beneficios obtenidos (Endesa ha sido la clara perjudicada por la violación de la seguridad, puesto que ha visto como terceros extraños a la organización accedían a sus sistemas y a los datos en ellos contenidos con una finalidad ilegítima).

Al respecto, esta Agencia se reitera en que (i) haber revisado las contrataciones realizadas por ******EMPRESA.9*** para evitar nuevas altas fraudulentas, no puede ser considerado una atenuante, cuando es una obligación impuesta por la normativa y que haber adoptado a posteriori las medidas apropiadas al riesgo, ya se ha valorado como una atenuante de la supuesta infracción del artículo 32 del RGPD; (ii) contestar cada uno de los requerimientos de información enviados por esta Agencia, no se considera atenuante dado que se trata de una obligación contemplada en la normativa aplicable cuya infracción es susceptible de un procedimiento sancionador ulterior (artículo 52 del RGPD y artículo 72.1.ñ) de la LOPDGDD); y (iii) no puede considerarse la falta de beneficios obtenidos por parte de ENDESA como una atenuante, de acuerdo con la Sentencia de la Audiencia Nacional, de 05/05/2021, rec. 1437/2020, que indica: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto*

para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante".

Por lo demás, esta Agencia se remite a lo ya indicado en la respuesta a las alegaciones al acuerdo de inicio del presente procedimiento sancionador.

Por todo lo expuesto, se desestima la presente alegación.

IV
Integridad y confidencialidad

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."*

En el presente caso, ENDESA tenía suscrito desde el día 01 de junio de 2020 un contrato con ******EMPRESA.1*** para comercializar los productos y servicios de ENDESA a través de diferentes acciones comerciales. A tal fin, el 28 de julio de 2021 ENDESA emitió una autorización a ******EMPRESA.1*** para la subcontratación a favor de ******EMPRESA.9*** para que se encargara de la captación mediante televenta de clientes en favor de ENDESA y se estableció como fecha de inicio de los trabajos subcontratados el 1 de agosto de 2021.

El 24 de agosto de 2021 ENDESA detectó en la red social Facebook un anuncio donde se vende usuario de la aplicación ******HERRAMIENTA.1*** con acceso a información de clientes. Y el 10 de septiembre de 2021 ENDESA obtuvo la comprobación de la veracidad del anuncio y la identificación de las credenciales del usuario de la aplicación que estaban siendo usadas por el anunciante para vender accesos. Es decir, que ya para septiembre de 2021 se había verificado que la confidencialidad de las bases de datos titularidad de ENDESA se había visto comprometida.

Posteriormente, el 19 de octubre de 2021 ******EMPRESA.1*** detectó que un usuario de ******EMPRESA.9*** había intentado realizar un alta fraudulenta, razón por la cual el 27 de octubre de 2021 envió una carta certificada a ******EMPRESA.9*** en la que se le comunicaba el cierre definitivo de la campaña de venta de contrato de suministro de ENDESA con efectos 19 de octubre, después de haber sido suspendida cautelarmente tal campaña ese mismo día.

El 20 de octubre de 2021, ******EMPRESA.1*** envió una comunicación a ENDESA indicando las operaciones afectadas por la práctica fraudulenta de ******EMPRESA.9***, identificándose 137 contrataciones realizadas y otras 7 operaciones pendientes de validación por parte de ENDESA que no habían llegado a darse de alta. ***(…).*** También

se identificaron y se bloquearon, para que no se tramitara su contratación, otras 172 órdenes que estaban pendientes de validar por el back office de ******EMPRESA.9***.

Es decir, que desde septiembre de 2021 ENDESA ya conocía la existencia de una violación de la seguridad de los datos personales y desde octubre de 2021 que la confidencialidad e integridad de los datos de 137 interesados se habían visto comprometidas y que había otros 179 posibles interesados cuyos datos era más que probable que pudieran haber sido comprometidos.

Por su parte, el 27 de octubre de 2021 se envió un correo electrónico a ENDESA en el que se remitía adjunto un e-mail del gerente de ******EMPRESA.9*** comunicando a ******EMPRESA.1*** las denuncias presentadas ante la Policía de ***PAÍS.1 el 19 de octubre de 2021 contra 23 agentes comerciales a los que se les "ha dado acceso a nuestra base de datos para que realice ventas, usando de manera ilegal las bases de datos y la información presentada en ellas para obtener provechos de otra finalidad", ***(…)***

El 27 de octubre de 2021 ******EMPRESA.1*** recibió un email del gerente de ******EMPRESA.9***, que ese mismo día ******EMPRESA.1*** reenvió a ENDESA**,** con el detalle de las averiguaciones realizadas sobre la práctica fraudulenta llevaba a cabo por algunos de sus agentes y su *modus operandi* ya que algunos de los comerciales habían decidido colaborar tras ver la denuncia presentada contra ellos ante la Policía. En este e-mail se detallaban las tres formas de operar, según la gerencia de ******EMPRESA.9***, de los comerciales:

1. Contactaban con el cliente y explicaban el producto, de estar de acuerdo y ser consciente con la contratación procedían con el cierre. Sin embargo, el cliente ponía la objeción indicando que no podían responder el SMS por diferentes motivos (bloqueado para SMS, no tenía móvil, no tenía batería, próximo a viajar, etc.). Lo que hacía el comercial era conseguir un número de otro cliente que era de ENDESA y pedían a este último que respondiera el SMS.

1. Por medio de internet los comerciales contrataban el programa de ******PLATAFORMA.1 (***HERRAMIENTA.1)***. Como se puede apreciar en las imágenes 4.1, 4.2, 4.3 y 4.4 adjuntas en el Documento 2 que acompaña al presente escrito, diferentes personas "comercializaban" accesos al programa de ******PLATAFORMA.1*** de Endesa. Lo que hacían los comerciales es utilizar esta herramienta para poder extraer datos de clientes de Endesa, por lo que las grabaciones las hacían con otras personas.

3. Otro caso fueron clientes que por algún momento no quisieron pasar textos por ser muy largos, se cansaron de recibir varias llamadas. Lo que hicieron en este caso es una simulación de ventas con otras personas y el mensaje también fue respondido por otros."

Con el detalle de este *modus operandi* queda acreditado que se habían visto afectadas la integridad y confidencialidad de los datos personales de al menos aquellos clientes a los que se les hubiera dado de alta de forma fraudulenta, toda vez

que para poder proceder al alta era necesario acceder a sus datos y modificarlos por unos falsos.

También en este mail con fecha 27 de octubre de 2021 ******EMPRESA.1*** identificó cinco de los usuarios de ******HERRAMIENTA.1*** comprometidos en la violación de la seguridad de los datos personales (utilizados por ******EMPRESA.9***) y se adjuntaron capturas de pantalla con anuncios de Facebook en los que se ofrecía el alquiler y/o venta de credenciales de acceso a la aplicación ******HERRAMIENTA.1***.

A raíz de esta situación, ENDESA verificó que a partir del 1 de julio de 2021 el volumen de ventas de ENDESA experimentó un aumento inusual no justificado (concretamente, las ventas se incrementaron en más del 500%) lo cual podía ser representativo de las actuaciones irregulares del personal contratado por ******EMPRESA.9***.

El 17 de enero de 2022 se publicaron nuevos anuncios en Facebook por parte del usuario ***B.B.B.***, en los que existió afectación a bases de datos de clientes de energía de ENDESA. Por tanto, como mínimo durante el mes de enero de 2022 la confidencialidad de los datos obrantes en la base de datos titularidad de ENDESA continuaba sin ser debidamente garantizada.

El 7 de febrero de 2022 ENDESA envió un burofax a FACEBOOK SPAIN S.L. en el que indicaba que había usuarios publicando información que podía ser constitutiva de delito y pedía su eliminación, de lo que se infiere que aún continuaban publicados los anuncios que vendían las credenciales para acceder a ******HERRAMIENTA.1***, viéndose aún comprometida la confidencialidad de los datos obrantes en dicho sistema.

El día 8 de febrero de 2022, tras las investigaciones oportunas, ENDESA tuvo conocimiento de la existencia de ciertas coincidencias entre los datos que aparecían en las bases de datos publicadas y los que podían estar incluidos en el sistema comercial de ENDESA, ******HERRAMIENTA.2***.

ENDESA llevó a cabo una nueva valoración del incidente y con fecha 9 de febrero de 2022 comprobó la veracidad de los últimos anuncios y la identidad de los dos anunciantes, ambos extrabajadores de proveedores de ENDESA con acceso a ******PLATAFORMA.1 (***HERRAMIENTA.1)***. Se detectaron un total de nueve usuarios comprometidos entre septiembre de 2021 y enero de 2022, que estaban siendo usados por los anunciantes de Facebook para vender accesos *a* ******PLATAFORMA.1 (***HERRAMIENTA.1***). Además, se comprobó que seis de ellos tenían acceso a ******HERRAMIENTA.2***. Se comprobó también la validez de las credenciales, en todos los casos asignadas a proveedores de ENDESA para realizar trabajos de captación y atención al cliente.

Es decir, se comprobó que la confidencialidad de los datos obrantes en ******HERRAMIENTA.1*** y ******HERRAMIENTA.2*** no había sido suficientemente garantizada toda vez que estuvieron a disposición de terceros no autorizados, lo cual permitió que además la integridad de los datos se viera también en riesgo al posibilitar la realización de numerosas altas fraudulentas.

En fecha 27 de junio de 2022 desde la AEPD se le solicita a ENDESA justificación del número de afectados por la violación de la seguridad de los datos personales y, a continuación, se incluye el análisis aportado en fecha 26 de julio de 2022:

> *"En el análisis que se llevó a cabo para la correcta identificación de los clientes cuyos datos aparentemente habían sido sustraídos sin autorización de la herramienta* ******HERRAMIENTA.1*** *y, por tanto, podían eventualmente haber sido tratados sin su consentimiento, se realizaron las siguientes actuaciones:*
>
> *(i) En primer lugar, una vez el proveedor* ******EMPRESA.1*** *puso en conocimiento de ENDESA la práctica irregular cometida por personal de* ******EMPRESA.9*** *y se realizaron las comprobaciones oportunas, se verificó que dicha práctica no se extendía a otros proveedores.*
>
> *(i) En segundo lugar, una vez identificado el posible origen de las contrataciones supuestamente irregulares, se procedió a acotar el alcance temporal de sus actuaciones, verificándose que a partir del 1 de julio de 2021 el volumen de ventas de ENDESA experimentó un aumento inusual no justificado (concretamente, las ventas se incrementaron en más del 500%) lo cual podía ser representativo de las actuaciones irregulares del personal contratado por* ******EMPRESA.9****. Con fecha 15 de octubre de 2021 se cesó la actividad de dicho subcontratista – como consecuencia de la rescisión del contrato con* ******EMPRESA.9*** *–, limitando, por tanto, el perímetro temporal del análisis de las contrataciones al período comprendido entre el 1 de julio y 15 de octubre de 2015* (se considera una errata este año y se interpreta 2021)*.*
>
> *(i) Finalmente, se llevó a cabo un control de calidad y auditoría de las contrataciones llevadas a cabo por* ******EMPRESA.9*** *en el perímetro temporal fijado. En dicho análisis, se descartaron aquellos casos en los que los propios clientes en cuyo nombre se había efectuado una contratación en la que intervino* ******EMPRESA.9*** *– en el período de tiempo delimitado –, se habían puesto en contacto con ENDESA para realizar acciones propias de sus contratos (por ejemplo, consultas comerciales), lo cual era indicativo de que los propios clientes eran conocedores de sus contratos y no manifestaron objeción alguna.*
>
> *El número de potenciales afectados por el incidente resultante fue: 760 clientes.*

Es decir, ENDESA reconoce que se vio afectada la confidencialidad e integridad de los datos personales de 760 clientes, pero sólo respecto de las contrataciones en las que intervino ******EMPRESA.9*** entre el 1 de julio y 15 de octubre de 2021, en las que los propios clientes eran supuestamente conocedores de sus contratos y no manifestaron objeciones al respecto.

No obstante, ENDESA ha señalado que el hecho de que dos o más personas pudieran acceder a la vez con un mismo usuario a ******HERRAMIENTA.1***, opción multisesión habilitada cuando se produjo la violación de la seguridad de los datos personales, y que, en relación con los usuarios comprometidos y con el período en que este incidente se

desarrolló, no se mantuviera un registro (logs) del uso de las herramientas ******HERRAMIENTA.1*** o ******HERRAMIENTA.2***, le impide conocer el número de registros de los aplicativos que pudieron ser realmente accedidos, al menos desde que tuvo conocimiento en agosto de 2021 de la publicación del anuncio en Facebook.

En este sentido, la propia ENDESA ha reconocido que el volumen aproximado de puntos de suministro que potencialmente se puede consultar desde la herramienta ******HERRAMIENTA.1*** es de 30,6 millones de puntos de suministro y de 8,6 millones de puntos de suministro de gas, de los que se podía conocer datos técnicos – como potencia, tensión, consumos estimados. Y que en caso de clientes con contrato en vigor, el volumen aproximado que un usuario podía consultar era de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas, de los que se podía consultar nombre y apellidos del titular del punto de suministro, número de Documento Nacional de Identidad, número de contrato, CUPS, importe de facturación anual, indicador de deuda, información sobre precios, datos técnicos referentes al punto de suministro, datos de consumo y gráfica de utilización.

En relación con la herramienta ******HERRAMIENTA.2,*** ENDESA ha reconocido que *"los usuarios identificados comprometidos podían acceder a los datos relativos a clientes con un contrato en vigor con ENDESA, siendo el volumen aproximado durante el periodo comprendido entre el 1 de julio de 2021 y el 15 de octubre de 2021, de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas. En cuanto a la tipología de datos que podía visualizar,* principalmente son: nombre y apellidos del titular del punto de suministro, dirección postal, número de Documento Nacional de Identidad, CUPS, teléfono, correo electrónico, productos contratados, facturas, número de cuenta bancaria, calidad del crédito, deudas con la compañía".

Es decir, que los potenciales afectados por la violación de la seguridad de los datos personales en cuestión, respecto a la herramienta ******HERRAMIENTA.1***, fueron 30,6 millones de puntos de suministros y 8,6 millones de puntos de suministro de gas de usuarios no clientes de ENDESA, así como datos de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas de ENDESA.

Tampoco, respecto a la herramienta ******HERRAMIENTA.2***, se garantizó la confidencialidad de los datos personales de 4,8 millones de clientes de electricidad y de 1,2 millones de clientes de gas de ENDESA.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA no garantizó debidamente la confidencialidad e integridad de los datos personales de su titularidad.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a ENDESA, por vulneración del artículo 5.1.f) del RGPD.

V

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

Se considera que ENDESA no garantizó debidamente la confidencialidad e integridad de los datos personales de su titularidad.

Los hechos conocidos son constitutivos de una infracción, imputable a ENDESA**,** tipificada en el artículo 83.5 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72.1.a) de la LOPDGDD, que califica de muy grave la siguiente conducta:

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

VI

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

Esta infracción puede ser sancionada con multa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no haber garantizado debidamente, al menos entre el 1 de julio de 2021 y el 15 de octubre de 2021, la integridad de los datos de, como mínimo, 760 interesados que resultaron víctima de contrataciones fraudulentas y por no haber garantizado la confidencialidad de los datos de 30,6 millones de puntos de suministros de electricidad y 8,6 millones de puntos de suministros de gas de no clientes de ENDESA, así como no haber garantizado la confidencialidad de los datos de identificación, domicilio, teléfono, correo electrónico, número de cuenta bancaria, entre otros, de 4,8 millones de clientes de electricidad y 1,8 millones de clientes de gas de ENDESA entre los meses de agosto 2021 a febrero de 2022.

- Negligencia en la infracción (apartado b): Si bien en el mes de agosto de 2021 ENDESA ya tenía conocimiento de que había publicado un anuncio veraz

vendiendo la posibilidad de acceder a su base de datos, ENDESA tardó más de un mes en resetear o eliminar los usuarios comprometidos comunicados por ***EMPRESA.1 y tardó meses en eliminar el usuario comprometido ***USUARIO.1** (ni siquiera realizó un reseteo preventivo inmediato de todos los usuarios ni se crearon nuevos usuarios a fin de evitar tener que utilizar un mismo usuario con varias sesiones iniciadas), lo que permitió que durante meses se pudiera acceder a los datos personales obrantes en los sistemas de ENDESA y se dieran de alta usuarios de forma fraudulenta. También ha sido gravemente negligente a la hora de solicitar a Facebook que se eliminaran los anuncios en cuestión, toda vez que no se dirigió a FACEBOOK IRELAND LIMITED, tal y como se le indicó que era el cauce correcto. Todo ello permitió que la confidencialidad de los datos se viera comprometida, como mínimo hasta el mes de febrero de 2022, y además se permitió a su vez que la integridad de tales datos se viera comprometida también entre el 1 de julio de 2021 y el 15 de octubre de 2021, como mínimo.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA fue gravemente negligente a la hora de garantizar la confidencialidad e integridad de los datos de su titularidad.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite imponer una sanción de multa administrativa de 2.500.000 € (dos millones quinientos mil euros).

VII

Seguridad del tratamiento

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, ENDESA emitió una autorización a ******EMPRESA.1*** para la subcontratación a favor de ******EMPRESA.9*** en la que se estableció como fecha de inicio de los trabajos subcontratados el 1 de agosto de 2021.

El 24 de agosto de 2021 ENDESA detectó en la red social Facebook un anuncio donde se vendía usuario de la aplicación ******HERRAMIENTA.1*** con acceso a información de clientes.

El 8 de septiembre de 2021 ENDESA realizó una segunda valoración del incidente donde proponía ***(…).***

El 10 de septiembre de 2021 ENDESA obtuvo la comprobación de la veracidad del anuncio y la identificación de las credenciales del usuario de la aplicación que estaban siendo usadas por el anunciante para vender accesos.

El 13 de septiembre de 2021 ENDESA convocó al Comité de Brechas de Seguridad y se decidió adoptar las siguientes medidas:

- ***(…)***

También en este Comité se propuso adoptar las siguientes medidas:

- ***(…)***

Por tanto, para el mes de septiembre de 2021 ENDESA ya era conocedora de que se había producido una violación de la seguridad de los datos personales en sus sistemas y que era posible acceder a los datos personales de sus clientes y era

consciente de que las medidas de seguridad que había implantado no eran apropiadas y debían ser mejoradas, ya para esas fechas.

En cualquier caso, esta Agencia considera que las medidas adoptadas por ENDESA con anterioridad al incidente en cuestión no pueden ser consideradas apropiadas en los términos del artículo 32 del RGPD, teniendo en cuenta entre otras circunstancias el volumen elevado de datos que trata, la cantidad de afectados por el tratamiento y la participación de encargados, toda vez que el estado de la técnica permitía de sobra haber tenido implantadas unas medidas adecuadas para, como mínimo, impedir que un mismo usuario pudiera tener varias sesiones iniciadas a la vez, implementar un inicio de sesión multifactor que dificultara los accesos indebidos, mantener un registro de logs amplio para obtener el detalle de la actividad realizada por sus usuarios, entre otras, y que el coste de implementar tales medidas era perfectamente asumible por ENDESA, una empresa que tuvo un volumen de ventas de ***CANTIDAD.1 euros y un resultado de ejercicio de ***CANTIDAD.3 euros, en especial teniendo en cuenta el alto riesgo para los derechos y libertades de los millones de interesados de los que ENDESA trata datos personales.

Con posterioridad, el 19 de octubre de 2021 ******EMPRESA.1*** detectó que un usuario de ******EMPRESA.9*** había intentado realizar un alta fraudulenta. Ante la sospecha de que esto pudiera haberse realizado por parte de otros agentes de ******EMPRESA.9***, ******EMPRESA.1*** inició un proceso de auditoría interna y comunicó a la persona Responsable de su cuenta en ENDESA lo sucedido telefónicamente, enviando también un e-mail con las primeras averiguaciones realizadas y las primeras medidas tomadas al respecto. Este mismo día se llevó a cabo el cierre total de todos los usuarios de ******EMPRESA.9*** y el acceso a cualquier herramienta de la campaña de ENDESA y se inició una auditoría interna para valorar el volumen de clientes afectados por contrataciones fraudulentas.

******EMPRESA.1*** rescindió el contrato con ******EMPRESA.9*** con fecha efectiva el día 19 de octubre de 2021, día en que tuvo conocimiento de la práctica fraudulenta llevada a cabo por ******EMPRESA.9***.

No obstante, indica ENDESA que, una vez identificado el posible origen de las contrataciones supuestamente irregulares, se procedió a acotar el alcance temporal de sus actuaciones, verificándose que a partir del 1 de julio de 2021 el volumen de ventas de ENDESA experimentó un aumento inusual no justificado (concretamente, las ventas se incrementaron en más del 500%) lo cual podía ser representativo de las actuaciones irregulares del personal contratado por ******EMPRESA.9***. Y que con fecha 15 de octubre de 2021 se cesó la actividad de dicho subcontratista – como consecuencia de la rescisión del contrato con ******EMPRESA.9*** –, limitando, por tanto, el perímetro temporal del análisis de las contrataciones al período comprendido entre el 1 de julio y 15 de octubre de 2021.

Pese a lo manifestado por ENDESA, ha quedado acreditado en el presente procedimiento que la actividad de ******EMPRESA.9*** cesó el 19 de octubre de 2021.

Como puede observarse, entre el 24 de agosto de 2021 (fecha en que ENDESA detecta que se publicó un anuncio en la red social Facebook vendiendo usuario de la aplicación ******HERRAMIENTA.1*** con acceso a información de clientes) y el 19 de

octubre de 2021 (fecha en que ***EMPRESA.1** detecta y comunica a ENDESA que un usuario de ***EMPRESA.9** había intentado realizar un alta fraudulenta) había transcurrido casi dos meses. Como se indicó anteriormente, en el mes de septiembre ENDESA ya era consciente de que sus medidas de seguridad no eran las apropiadas y debían ser mejoradas, pese a lo cual más de un mes más tarde se detectó un nuevo incidente de seguridad.

El 20 de octubre de 2021, ***EMPRESA.1**, tras la auditoría realizada, envió una comunicación a ENDESA indicando las operaciones afectadas por la práctica fraudulenta de ***EMPRESA.9**, identificándose 137 contrataciones realizadas y otras 7 operaciones pendientes de validación por parte de ENDESA que no habían llegado a darse de alta. También se identificaron y se bloquearon, para que no se tramitara su contratación, otras 172 órdenes que estaban pendientes de validar por el back office de ***EMPRESA.9**. Además, en esta comunicación se indicaban las medidas que se pretendían seguir llevando a cabo en los próximos días para detectar cualquier otra irregularidad adicional.

Por otra parte, en esta comunicación realizada a ENDESA se remitía adjunto un e-mail del gerente de ***EMPRESA.9** comunicando a ***EMPRESA.1** las denuncias presentadas ante la Policía de ***PAÍS.1, contra sus comerciales implicados en esta práctica fraudulenta, ***(…)***.

El 27 de octubre de 2021 ***EMPRESA.1** recibió un email del gerente de ***EMPRESA.9** detallando las averiguaciones realizadas sobre la práctica fraudulenta llevaba a cabo por algunos de sus agentes y su *modus operandi* ya que algunos de los comerciales habían decidido colaborar tras ver la denuncia presentada contra ellos ante la Policía. En este e-mail se detallaban las tres formas de operar, según la gerencia de ***EMPRESA.9**, de los comerciales. En este mail con fecha 27 de octubre de 2021 se identificaban también cinco de los usuarios de ***HERRAMIENTA.1** comprometidos en la violación de la seguridad de los datos personales y se adjuntaban capturas de pantalla con anuncios de Facebook en los que se ofrece el alquiler y/o venta de credenciales de acceso a la aplicación ***HERRAMIENTA.1**.

El 27 de octubre de 2021, ***EMPRESA.1** remitió un correo electrónico a ENDESA detallando estas prácticas fraudulentas realizadas por algunos agentes de ***EMPRESA.9** y adjuntando capturas de pantalla con anuncios de Facebook en los que se ofrecía el alquiler y/o venta de credenciales de acceso a la aplicación ***HERRAMIENTA.1** y se adjuntaban los usuarios utilizados. A continuación, se reproduce el contenido del correo:

> *"Por medio de internet los asesores han contratado el* ***PLATAFORMA.1 (***HERRAMIENTA.1*)*. Lo que han hecho los comerciales es **(…)**. Adjunto los usuarios de ***PLATAFORMA.1* (***HERRAMIENTA.1*) *que han usado. Cabe mencionar que nosotros en su momento pedimos esta herramienta por lo que nos negaste indicando que estaba prohibido."*

Como se indicó anteriormente, pese a haber sido conocedora en el mes de septiembre de que las medidas de seguridad que tenía implantadas no eran apropiadas a fin de garantizar la confidencialidad de los datos personales titularidad de ENDESA, no se

resetearon ni se eliminaron de forma inmediata, ni de ******HERRAMIENTA.1*** ni de ******HERRAMIENTA.2***, los usuarios que se sabía comprometidos, se tardaron meses, lo que propició que durante todo ese tiempo se pudiera acceder indebidamente a los datos personales titularidad de ENDESA y facilitó que se realizara un gran número de altas fraudulenta. Tampoco se realizó un reseteo preventivo de todos los usuarios de los sistemas, ante una posible amenaza (que luego resultó ser cierta), ni se crearon nuevos usuarios que permitieran no utilizar varias sesiones para un único usuario.

Durante el mes de enero de 2022, ENDESA identificó nuevos anuncios publicados por el usuario ***B.B.B.***, donde se ofrecía la venta de bases de datos de clientes de energía de distintas empresas del sector.

Es decir, que cuatro meses más tarde de que ENDESA detectara que se había publicado un anuncio ofreciendo usuario de ******HERRAMIENTA.1*** y que se había comprobado era veraz, y tres meses después de que ******EMPRESA.1*** detectara y comunicara que se había producido un uso indebido de los usuarios de ******HERRAMIENTA.1*** por parte de trabajadores de la empresa ******EMPRESA.9***, ENDESA identificó nuevos anuncios donde se ofertan usuarios para acceder a los datos personales obrantes en sus sistemas.

Ello implica que cinco meses después de que ENDESA detectara un anuncio en Facebook vendiendo usuario para acceder a ******HERRAMIENTA.1***, todavía había anuncios de ese estilo publicados, lo cual evidencia que las medidas implantadas para entonces tampoco eran las apropiadas para impedir que un incidente de seguridad como aquel siguiera produciéndose.

El 7 de febrero de 2022 ENDESA envió un burofax a FACEBOOK SPAIN solicitando la eliminación de una serie de anuncios "*relacionadas con la venta de credenciales de acceso a plataformas de gestión con datos de carácter personal*".

Con fecha 8 de febrero de 2022, dicha comunicación de ENDESA fue respondida mediante correo electrónico en el que se indicaba que FACEBOOK SPAIN no era la entidad competente para resolver la cuestión, sino FACEBOOK IRELAND LIMITED, y se solicitaba que se dirigiera la comunicación a dicha entidad. Pese a esta comunicación, no ha quedado acreditado en el presente expediente que ENDESA hubiera dirigido comunicación alguna en este sentido a FACEBOOK IRELAND LIMITED, tal y como solicita FACEBOOK SPAIN, lo cual también evidencia una falta de diligencia notable a la hora de implementar una de las primeras medidas decididas allá por el mes de septiembre de 2021, como ser la retirada de los anuncios en cuestión.

El día 8 de febrero de 2022, tras las investigaciones oportunas, ENDESA tuvo conocimiento de la existencia de ciertas coincidencias entre los datos que aparecían en las bases de datos publicadas y los que podían estar incluidos en el sistema comercial de ENDESA, ******HERRAMIENTA.2***.

ENDESA llevó a cabo una nueva valoración del incidente y con fecha 9 de febrero de 2022 comprobó la veracidad de los anuncios y la identidad de los dos anunciantes, ambos extrabajadores de proveedores de ENDESA con acceso a ******PLATAFORMA.1 (***HERRAMIENTA.1)***. Se detectaron un total de nueve usuarios comprometidos entre

septiembre de 2021 y enero de 2022, que estaban siendo usados por los anunciantes de Facebook para vender accesos *a* ******PLATAFORMA.1 (***HERRAMIENTA.1***). Además, se comprobó que seis de ellos tenían acceso a ******HERRAMIENTA.2***. Se comprobó también la validez de las credenciales, en todos los casos asignadas a proveedores de ENDESA para realizar trabajos de captación y atención al cliente.

Es decir, que pese a que ya en septiembre de 2021 ENDESA era conocedora de que se había producido un incidente de seguridad que había puesto en riesgo los datos personales de su titularidad, su falta de diligencia a la hora de adoptar las medidas de seguridad apropiadas y necesarias para que no pudiera vulnerarse la confidencialidad de dichos datos permitió que hasta el mes de enero de 2022 se hubieran comprometido un total de nueve usuarios que estaban siendo utilizados para vender accesos a ******HERRAMIENTA.1*** a través de Facebook desde los meses de agosto 2021 a febrero 2022, como mínimo.

Respecto a los usuarios comprometidos identificados por ******EMPRESA.1*** en su correo electrónico enviado a ENDESA el 27 de octubre de 2021:

- El usuario ******USUARIO.13,*** asignado a ******EMPRESA.12,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 3 de septiembre de 2021, nuevamente reseteado el 29 de noviembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Pero recién fue eliminado del sistema ******HERRAMIENTA.2*** el 12 de enero de 2022, siendo su último acceso al sistema el 26 de noviembre de 2021.

  Es decir, que ******EMPRESA.1*** avisó a ENDESA que este usuario estaba comprometido el 27 de octubre de 2021, pero ENDESA ya había reseteado el usuario en ******HERRAMIENTA.1*** el 3 de septiembre, casi dos meses antes (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA ya conociera que ese usuario estaba comprometido, de hecho, dos días antes desde ******EMPRESA.16*** se había indicado que uno de los usuarios que publicaba los anuncios de Facebook había sido una agente de esta empresa).

  En cualquier caso, si el usuario en cuestión fue utilizado para realizar contrataciones fraudulentas en octubre de 2021, esta Agencia considera que de poco había servido el reseteo de la contraseña en septiembre de 2021 y el riesgo para los derechos y libertades de los afectados permanecía intacto. Y, con posterioridad a la comunicación por parte de ******EMPRESA.1***, el usuario fue reseteado más de un mes más tarde.

  También llama la atención de esta Agencia que el usuario se hubiera reseteado en ******HERRAMIENTA.1*** el 3 de septiembre de 2021, pero recién el 12 de enero de 2022 fue eliminado de la plataforma ******HERRAMIENTA.2***, siendo su último acceso a la misma el 26 de noviembre de 2021. Es decir, que aun sabiendo que el usuario se había visto comprometido en ******HERRAMIENTA.1***, el usuario accedió libremente a ******HERRAMIENTA.2*** durante un mes más.

- El usuario ******USUARIO.15,*** asignado a ******EMPRESA.12,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 21 de septiembre de 2021,

nuevamente reseteado el 29 de noviembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Pero recién fue eliminado del sistema ******HERRAMIENTA.2***** el 12 de enero de 2022, siendo su último acceso al sistema el 25 de noviembre de 2021.

Es decir, que ******EMPRESA.1***** avisó a ENDESA que este usuario estaba comprometido el 27 de octubre de 2021, pero ENDESA ya había reseteado el usuario en ******HERRAMIENTA.1***** el 21 de septiembre, más de un mes antes (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA ya conociera que ese usuario estaba comprometido, de hecho, ese mismo día se había indicado a ENDESA que uno de los usuarios que publicaba los anuncios de Facebook había sido un agente de ******EMPRESA.15******).

En cualquier caso, si el usuario en cuestión fue utilizado para realizar contrataciones fraudulentas en octubre de 2021, esta Agencia considera que de poco había servido el reseteo de la contraseña en septiembre de 2021 y el riesgo para los derechos y libertades de los afectados permanecía intacto. Y, con posterioridad a la comunicación por parte de ******EMPRESA.1******, el usuario fue reseteado más de un mes más tarde.

También llama la atención de esta Agencia que el usuario se hubiera reseteado en ******HERRAMIENTA.1***** el 21 de septiembre de 2021, pero recién el 12 de enero de 2022 fue eliminado de la plataforma ******HERRAMIENTA.2******, siendo su último acceso a la misma el 25 de noviembre de 2021. Es decir, que aun sabiendo que el usuario se había visto comprometido en ******HERRAMIENTA.1******, el usuario accedió libremente a ******HERRAMIENTA.2****** durante un mes más.

- El usuario ******USUARIO.14,****** asignado ***a ***EMPRESA.15,**** fue reseteado o deshabilitado en ******HERRAMIENTA.1***** el 29 de noviembre de 2021 y eliminado de los sistemas el 4 de marzo de 2022 (aunque esto fue porque caducó el usuario sin más). Y recién fue eliminado del sistema ******HERRAMIENTA.2****** el 16 de marzo de 2022, siendo su último acceso al sistema el 18 de febrero de 2022.

  Es decir, que este usuario fue reseteado o deshabilitado en ******HERRAMIENTA.1****** más de un mes después de que ENDESA tuviera conocimiento por parte de ******EMPRESA.1****** de que este usuario se había visto comprometido. Y aun sabiendo que el usuario se había visto comprometido en ******HERRAMIENTA.1******, el usuario accedió libremente a ******HERRAMIENTA.2****** durante casi tres meses más.

  - El usuario ******USUARIO.9,**** asignado a ******EMPRESA.6****** fue reseteado o deshabilitado en ******HERRAMIENTA.1****** el 21 de noviembre de 2021 y el 15 de febrero de 2022 y eliminado de los sistemas el 24 de agosto de 2022.

  Es decir, que recién se reseteó este usuario más de un mes después de que ******EMPRESA.1****** le hubiera comunicado a ENDESA que se había visto comprometido.

- El usuario ******USUARIO.16***, asignado a ******EMPRESA.5*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 29 de noviembre de 2021 y eliminado de sus sistemas el 24 de agosto de 2022. Y se eliminó del sistema ******HERRAMIENTA.2*** el 17 de febrero de 2022, siendo su último acceso al sistema el 3 de diciembre de 2021.

  Es decir, que recién se reseteó este usuario más de un mes después de que ******EMPRESA.1*** le hubiera comunicado a ENDESA que se había visto comprometido.

Respecto al resto de usuarios, se desconoce la fecha en que ENDESA supo que tales usuarios se habían visto comprometidos, pero se puede señalar lo siguiente:

- El usuario ******USUARIO.10,*** asignado ***a ***EMPRESA.15,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 10 de septiembre de 2021 y eliminado de los sistemas el 24 de agosto de 2022. Y fue eliminado del sistema ******HERRAMIENTA.2*** el 10 de septiembre de 2021, siendo su último acceso al sistema el 9 de septiembre de 2021.

  Es decir, ENDESA reseteó el usuario en ******HERRAMIENTA.1 y ***HERRAMIENTA.2*** el 10 de septiembre de 2021 (los motivos por los cuales se realizó esta acción se desconocen por parte de esta Agencia, pero puede que ENDESA tuviera conocimiento de que ese usuario estaba comprometido, ya que ese mismo día ENDESA envió un correo electrónico haciendo referencia a un empleado activo en ******EMPRESA.15***, cuyo usuario se iba a dar de baja con carácter inmediato).

- El usuario ******USUARIO.2 (***USUARIO.2)***, asignado a ******EMPRESA.8,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** y eliminado de sus sistemas el 19 de noviembre de 2021.

- El usuario ******USUARIO.1,*** asignado a ******EMPRESA.13,*** fue reseteado o deshabilitado en ******HERRAMIENTA.1*** el 15 de febrero de 2022 y eliminado de los sistemas el 24 de agosto de 2022. Es decir, no fue reseteado antes del envío del primer burofax a Facebook el 8 de febrero de 2022, tal y como afirma ENDESA en sus alegaciones al acuerdo de inicio.

Todo lo expuesto evidencia que, pese a que en octubre de 2021 ya se había identificado a cinco de los usuarios comprometidos por la violación de la seguridad de los datos personales en cuestión, la falta de diligencia de ENDESA a la hora de impedir el acceso a sus aplicaciones por parte de los usuarios comprometidos permitió que durante más de un mes se hubieran podido producir aún más accesos indebidos a datos personales de los que hasta entonces habían tenido lugar.

Tampoco se habían implementado las medidas de seguridad propuestas desde el inicio de la violación de la seguridad de los datos personales y supuestamente adecuadas para mitigar las consecuencias de la violación de la seguridad de los datos, puesto que no es cierto que se hubieran bloqueados los accesos de los usuarios comprometidos a las herramientas de ENDESA de forma diligente, deshabilitando sus credencia-

les, ni que esto tuviera lugar antes de que se hubiera enviado el primer burofax a Facebook.

Por su parte, en cuanto al análisis de riesgos realizado sobre la actividad del tratamiento que ha sufrido la violación de la seguridad de los datos personales con anterioridad a la incidencia acaecida, ENDESA aporta junto a su escrito de fecha 26 de julio de 2022 dos documentos, ambos generados por la herramienta "******HERRAMIENTA.1***" utilizada por el Grupo Enel para llevar a cabo la evaluación del riesgo de privacidad, sobre las herramientas ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***. En ninguno de estos documentos se observa que se hubiera contemplado siquiera la posibilidad de que un empleado de un proveedor o una empresa subcontratista de éste hiciera un uso indebido de los datos personales obrantes en los sistemas de información de ENDESA.

Asimismo, el 15 de septiembre de 2022 desde la SGID se comprueba que siguen publicados en Facebook anuncios identificados por ENDESA donde se ofrece la venta de credenciales de acceso a *****HERRAMIENTA.1** y bases de datos. Esto evidencia que más de un año después de que se detectara un anuncio vendiendo usuario para el acceso a ******HERRAMIENTA.1***, ENDESA no había sido lo suficientemente diligente para conseguir que tales publicaciones desaparezcan de la red social en cuestión, lo cual era una de las primeras medidas decididas por la empresa un año antes.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA no fue lo suficientemente diligente a la hora de implantar medidas de seguridad apropiadas para impedir que se produjeran incidentes de seguridad como el que tuvo lugar en el presente caso.

Por tanto, se considera que los hechos conocidos son ser constitutivos de una infracción, imputable a ENDESA, por vulneración del artículo 32 del RGPD.

VIII

Tipificación y calificación de la infracción del artículo 32 del RGPD

En el presente caso, se considera que ENDESA no aplicó las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de que una violación de la seguridad de los datos personales como la que tuvo lugar se produjera.

Los hechos conocidos son constitutivos de una infracción, imputable a ENDESA**,** tipificada en el artículo 83.4 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los dos años, conforme al artículo 73.f) de la LOPDGDD, que califica de grave la siguiente conducta:

> *"f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".*

IX

Sanción por la infracción del artículo 32 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 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no tener implantadas las medidas de seguridad apropiadas al riesgo de que se produjera una violación de la seguridad de los datos personales como la que ha tenido lugar en el presente caso, que permitió que la integridad de los datos de al menos 760 interesados se viera comprometida entre el 1 de julio de 2021 y el 15 de octubre de 2021 y permitió que la confidencialidad de los datos de 30,6 millones de puntos de suministros de electricidad y 8,6 millones de puntos de suministros de gas de no clientes de ENDESA y la confidencialidad de los datos de identificación, domicilio, teléfono, correo electrónico, número de cuenta bancaria, entre otros, de 4,8 millones de clientes de electricidad y 1,8 millones de clientes de gas de ENDESA entre los meses de agosto 2021 a febrero de 2022, se viera en riesgo.

  En este sentido, cabe destacar que la propia ENDESA reconoce que dos o más personas podían, acceder a la vez con un mismo usuario a ******HERRAMIENTA.1***, opción multisesión habilitada, y que no se mantenía un registro (logs) del uso de las herramientas ******HERRAMIENTA.1*** o ******HERRAMIENTA.2***, lo que denota la falta de medidas de seguridad adecuadas para detectar y evitar accesos no autorizados.

  En cuanto a las consecuencias posibles de la falta de tales medidas de la seguridad de los datos personales, la principal es la pérdida de control sobre sus datos, con el consiguiente riesgo de ser víctima de phishing, de otro ciberataque y de contratación de suministros no solicitados, con el estrés y

costes adicionales que tales situaciones podrían suponerles toda vez que hasta podría exigírseles una deuda por esos servicios no pedidos.

- Negligencia en la infracción (apartado b): Respecto de la supuesta infracción del artículo 32 del RGPD, la conducta gravemente negligente de ENDESA se aprecia en todo su comportamiento antes y después de producido el incidente, toda vez que ni siquiera se había previsto siquiera la posibilidad de que se hiciera un uso indebido de los usuarios de ******HERRAMIENTA.1*** y ******HERRAMIENTA.2***, por lo que no se había implementado unas medidas adecuadas para asegurar una autenticación de usuarios con las debidas garantías, impidiendo que se produjesen accesos indebidos a los sistemas y posibilitando que se rastree debidamente la actividad de estos usuarios en esos sistemas.

Tampoco se resetearon ni se eliminaron de forma inmediata ni efectiva, ni de ******HERRAMIENTA.1*** ni de ******HERRAMIENTA.2***, los usuarios que se sabía comprometidos, pues se tardó más de un mes, lo que propició que durante todo ese tiempo se pudiera acceder indebidamente a los datos personales titularidad de ENDESA y facilitó que se realizara un gran número de altas fraudulenta. Tampoco se realizó un reseteo preventivo de todos los usuarios de los sistemas, ante una posible amenaza (que luego resultó ser cierta).

Pese a que ya en septiembre de 2021 ENDESA era conocedora de que se había producido un incidente de seguridad que había puesto en riesgo los datos personales de su titularidad, su falta de diligencia a la hora de adoptar las medidas de seguridad apropiadas y necesarias para que no pudiera vulnerarse la confidencialidad de dichos datos permitió que hasta el mes de enero de 2022 (según ha reconocido ENDESA) se hubieran comprometido un total de nueve usuarios que estaban siendo utilizados para vender accesos a ******HERRAMIENTA.1*** a través de Facebook desde los meses de agosto 2021 a febrero 2022, como mínimo.

A mayor abundamiento, con fecha 27 de octubre de 2021 ENDESA ya tenía identificados cinco de los usuarios de ******HERRAMIENTA.1*** comprometidos en la violación de la seguridad de los datos personales, que se resetearon más de un mes más tarde de tal comunicación. Todo lo cual evidencia que, pese a que en octubre de 2021 ya se había identificado a cinco de los usuarios comprometidos por la violación de la seguridad de los datos personales de seguridad en cuestión, la falta de diligencia de ENDESA a la hora de impedir el acceso a sus aplicaciones por parte de los usuarios comprometidos permitió que durante meses se hubieran podido producir aún más accesos indebidos a datos personales de los que hasta entonces habían tenido lugar.

Por su parte, el 8 de febrero de 2022 FACEBOOK SPAIN contesta a ENDESA indicando que no era la entidad competente para eliminar los anuncios publicados, sino que lo era FACEBOOK IRELAND LIMITED, y se solicitaba que se dirigiera la comunicación a dicha entidad. Pese a ello, no ha quedado acreditado en el presente expediente que ENDESA hubiera dirigido comunicación alguna en este sentido a FACEBOOK IRELAND LIMITED, tal y como solicita FACEBOOK SPAIN, a pesar de haber sido acordado en la reunión del 13 de septiembre de 2021 y en agosto 2021 solicitar la baja de los

anuncios, debido al riesgo que entrañaban, lo cual también evidencia una falta de diligencia notable a la hora de implementar una de las primeras medidas acordadas en el mes de septiembre de 2021, como es la retirada de los anuncios en cuestión.

A mayor abundamiento, el 15 de septiembre de 2022 desde la SGID se comprueba que siguen publicados en Facebook anuncios identificados por ENDESA donde se ofrece la venta de credenciales de acceso a ******HERRAMIENTA.1*** y bases de datos. Esto evidencia que más de un año después de que se detectara un anuncio vendiendo usuario para el acceso a ******HERRAMIENTA.1***, ENDESA no había sido lo suficientemente diligente para solicitar que tales publicaciones desaparecieran de la red social en cuestión, lo cual era una de las primeras medidas decididas por la empresa un año antes.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA fue gravemente negligente a la hora de implantar medidas de seguridad apropiadas para impedir que se produjeran incidentes de seguridad como el que tuvo lugar en el presente caso y su actuación con posterioridad al incidente en cuestión también lo fue.

Como atenuante:

- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción (apartado k): al tener conocimiento de la publicación de anuncios en Facebook vendiendo usuarios para acceder al ******HERRAMIENTA.1***, ENDESA adoptó una serie de medidas, tales como el reseteo de las contraseñas de los usuarios, el seguimiento de las publicaciones dicha red social, intentar dar de baja los citados anuncios, deshabilitar la posibilidad de mantener sesiones simultáneas y ampliar la trazabilidad de los accesos a ******HERRAMIENTA.1***, entre otras.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite imponer una sanción de multa administrativa de 1.500.000 € (un millón quinientos mil euros).

X

Notificación a la autoridad de control

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
(…)."

En el presente caso, consta que ENDESA el 24 de agosto de 2021 ya había detectado que se había publicado en la red social Facebook un anuncio vendiendo usuario para acceder a ******HERRAMIENTA.1***. Y que para el 10 de septiembre de 2021 ENDESA ya había comprobado la veracidad de tal anuncio, al punto que el 13 de septiembre de 2021 se reunió en Comité para decidir y proponer sobre la adopción de las medidas de seguridad correspondientes.

Con posterioridad, el 19 de octubre de 2021 su proveedor ******EMPRESA.1*** le informó a ENDESA de que había detectado posibles altas fraudulentas por parte de su subcontratista ******EMPRESA.9*** e incluso el 27 de octubre de 2021 ENDESA recibió un correo electrónico de ******EMPRESA.1*** en el que se informaba que se había detectado 5 usuarios de ******HERRAMIENTA.1*** comprometidos y se explicaba la forma en que tales altas fraudulentas podían haber tenido lugar.

Meses más tarde, en enero de 2022 ENDESA identificó nuevos anuncios publicados en la red social Facebook ofertando usuarios para el acceso a ******HERRAMIENTA.1***. Y el 4 de febrero de 2022 solicitó a FACEBOOK SPAIN que retirara los citados anuncios, al poder ser constitutivos de delito.

Pese a todo lo expuesto, ENDESA no ha informado a esta Agencia de la existencia de una posible violación de la seguridad de los datos personales hasta el 10 de febrero de 2022, que fue cuando comprobó que se habían visto comprometidos los datos de la herramienta ******HERRAMIENTA.2***, sin que resultaran acreditados los motivos que justifiquen tal dilación.

No obstante, meses antes ya sabía que se había visto comprometida la seguridad de los datos obrantes en la herramienta ******HERRAMIENTA.1***, lo cual permitió que se realizara un gran número de altas fraudulentas, todo ello sin que hubiera efectuado notificación alguna a esta Agencia.

Tal y como se indicó en la respuesta a las alegaciones al acuerdo de inicio y propuesta de resolución del presente procedimiento sancionador, en el presente caso, esta Agencia considera que ENDESA no calificó correctamente el incidente al considerarlo que no era notificable y se reitera en que el incidente en cuestión era notificable desde que ENDESA tuvo conocimiento el 10 de septiembre de 2021 de la veracidad del anuncio de agosto de 2021, además conoció a través de ******EMPRESA.1*** que se habían visto comprometidos cinco usuarios de ******HERRAMIENTA.1*** y que se había producido un uso indebido de los datos personales obrantes en sus sistemas, lo cual

tuvo lugar el 27 de octubre de 2021. Con independencia de que se hubieran reseteado o eliminado los usuarios (lo cual ya se analizó sobradamente que no se hizo de forma inmediata ni diligentemente), la realidad es que el incidente ya había tenido lugar, se había perdido la confidencialidad de los datos personales tratados por ENDESA y existía un riesgo probable para los derechos y libertades de las personas físicas, toda vez que ENDESA había perdido el control de los accesos a esos datos, con independencia de que se hubiera producido (o no) accesos indebidos, además, a ******HERRAMIENTA.2***. Por tanto, esta Agencia se reitera en que en el presente caso ENDESA debió notificar la violación de la seguridad de los datos personales en el plazo máximo de 72 horas desde que conoció la veracidad de los anuncios en septiembre de 2021 o al menos desde que tuvo conocimiento por parte de ******EMPRESA.1*** de que tal incidente se había producido, en octubre de 2021.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a ENDESA, por vulneración del artículo 33 del RGPD.

XI

Tipificación y calificación de la infracción del artículo 33 del RGPD

En el presente caso, se considera que ENDESA no notificó en plazo a la autoridad de control que se había producido una violación de la seguridad de los datos personales.

Los hechos conocidos son constitutivos de una infracción, imputable a ENDESA**,** tipificada en el artículo 83.4 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe al año, conforme al artículo 74.m) de la LOPDGDD, que califica de leve la siguiente conducta:

> *"m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679".*

XII

Sanción por la infracción del artículo 33 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 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no haber comunicado a la autoridad de protección de datos que se había producido una violación de la seguridad de los datos personales en el plazo de 72 horas, de la cual tuvo indicios ya en agosto de 2021 y fue comprobada en septiembre de 2021, es decir que recién se comunicó cinco meses más tarde, sin que pueda apreciarse la existencia de motivos legítimos que justifiquen dicha dilación.

- Negligencia en la infracción (apartado b): ENDESA el 24 de agosto de 2021 ya había detectado que se había publicado en la red social Facebook un anuncio vendiendo usuario para acceder a ******HERRAMIENTA.1***. Y el 10 de septiembre de 2021 ENDESA ya había comprobado la veracidad de tal anuncio, al punto que el 13 de septiembre de 2021 se reunió en Comité para decidir y proponer sobre la adopción de las medidas de seguridad correspondientes.

Con posterioridad, el 19 de octubre de 2021 su proveedor ******EMPRESA.1*** le informa a ENDESA de que había detectado posibles altas fraudulentas por parte de su subcontratista ******EMPRESA.9*** e incluso el 27 de octubre de 2021 ENDESA recibe un correo electrónico de ******EMPRESA.1*** en el que se informaba que se había detectado 5 usuarios de ******HERRAMIENTA.1*** comprometidos y se explicaba la forma en que tales altas fraudulentas podían haber tenido lugar.

Meses más tarde, en enero de 2022 ENDESA identifica nuevos anuncios publicados en la red social Facebook ofertando usuarios para el acceso a ******HERRAMIENTA.1***. Y el 4 de febrero de 2022 solicita a FACEBOOK SPAIN que retire los citados anuncios, al poder ser constitutivos de delito.

Pese a todo lo expuesto, ENDESA no ha informado a esta Agencia de la existencia de una posible violación de la seguridad de los datos personales hasta el 10 de febrero de 2022, sin que los motivos alegados por Endesa puedan justificar esta dilación.

Todo lo expuesto demuestra, como se ha indicado anteriormente, que ENDESA fue gravemente negligente a la hora de notificar a la autoridad de control correspondiente de la existencia de una violación de la seguridad de los datos personales.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 33 del RGPD, permite imponer una sanción de multa administrativa 800.000 € (ochocientos mil euros).

XIII

Comunicación al interesado

El artículo 34 "*Comunicación de una violación de la seguridad de los datos personales al interesado*" del RGPD establece:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:
a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3".

En el presente caso, la violación de la seguridad de los datos personales entrañaba un alto riesgo para los derechos y libertades de las personas físicas y no se han dado ninguna de las circunstancias enumeradas en el apartado 3 del artículo 34 del RGPD que eximiera a ENDESA del deber de comunicar a los interesados que esta violación de la seguridad de los datos personales se había producido.

De hecho, en la notificación del incidente en cuestión a esta Agencia, de fecha 10 de febrero de 2022, ENDESA había indicado que no comunicaría la violación de la seguridad de los datos personales a los afectados por entender que no había un alto riesgo para sus derechos y libertades razón por la cual esta Agencia emitió una orden (notificada a ENDESA el 8 de marzo de 2022) para que sí realizara la comunicación a los afectados en los términos del artículo 34 del RGPD.

El contenido del modelo de carta remitida por ENDESA era el siguiente:

> *"31 de Marzo de 2022*
> *Estimado cliente,*
> *Nos ponemos en contacto contigo para informarte que hemos detectado un posible acceso indebido a determinados sistemas comerciales de Endesa Energía y que desde el mismo momento que hemos sido conocedores de este hecho, hemos adoptado las oportunas medidas de seguridad, técnicas y organizativas, para evitar que se pudiera producir una afectación de alto riesgo a los derechos y libertades de nuestros clientes, con lo que la confidencialidad y la integridad de tus datos personales no se ha visto comprometida.*
>
> *Puedes consultar nuestra política de privacidad en www.endesa.com/es/proteccion-datos-endesa, donde encontrarás la información relativa al tratamiento de tus datos personales. Si lo prefieres, puedes contactar directamente con nuestro Delegado de Protección de Datos enviando una comunicación a ***EMAIL.1 para conocer el detalle de las medidas adoptadas u obtener más información.*
>
> *Aprovechamos para agradecerte la confianza depositada en Endesa.*
>
> *Un cordial saludo,*
> *Endesa Energía".*

Como puede apreciarse, en la comunicación enviada a los afectados se dice que "*la confidencialidad y la integridad de tus datos personales no se ha visto comprometida".* No obstante, esa información proporcionada no es cierta.

En la notificación de ENDESA de la violación de la seguridad de los datos personales a esta Agencia, de fecha 10 de febrero de 2022, se indica que como consecuencia del incidente se ha visto afectada la confidencialidad y la integridad del tratamiento. Y durante el desarrollo de las actuaciones de investigación se ha constatado que las credenciales de usuarios de aplicaciones de ENDESA comprometidos en la violación de la seguridad de los datos personales fueron utilizadas por comerciales de otra empresa (******EMPRESA.9***), que no tenían acceso a las bases de datos de ENDESA, para extraer datos de clientes de ENDESA que se utilizaron para realizar contrataciones fraudulentas.

Asimismo, en la comunicación enviada a los afectados ENDESA no ha incluido una descripción de las posibles consecuencias que la violación de la seguridad de los datos personales podría causarles y llega hasta a negar que se pueda producir un alto riesgo para los derechos y libertades de las personas afectadas. Ni tampoco se hace referencia específica en la comunicación a la posibilidad de solicitar información adicional a través de otro medio sobre estas posibles consecuencias.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a ENDESA, por vulneración del artículo 34 del RGPD.

XIV

Tipificación y calificación de la infracción del artículo 34 del RGPD

En el presente caso, se considera que ENDESA no cumplió con la obligación de informar debidamente a los afectados que se había producido una violación de la seguridad de los datos personales.

Los hechos conocidos son constitutivos de una infracción, imputable a ENDESA**,** tipificada en el artículo 83.4 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe al año, conforme al artículo 74.ñ) de la LOPDGDD, que califica de leve la siguiente conducta:

> *"ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica".*

XV

Sanción por la infracción del artículo 34 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 del RGPD.
Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no haber proporcionado debidamente, al menos, a los 760 afectados por las altas fraudulentas la información a la que estaba obligada respecto a la violación de la seguridad de los datos personales en cuestión.

- Negligencia en la infracción (apartado b): primeramente ENDESA fue negligente a la hora de identificar la necesidad de que la comunicación a los afectados por la violación de la seguridad de los datos personales, en los términos del artículo 34 del RGPD debía ser enviada. Y una vez esta Agencia ordena a ENDESA que remita la citada comunicación a los afectados, ENDESA fue gravemente negligente a la hora de proporcionar la información exigida por el citado artículo 34 del RGPD de forma veraz y completa.

Como atenuante:

- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción (apartado k): se facilitó el contacto del Delegado de Protección de Datos para obtener más información.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 34 del RGPD, permite imponer una sanción de multa administrativa de 800.000 € (ochocientos mil euros).

XVI

Transferencias de datos a terceros países u organizaciones internacionales

El artículo 44 "*Principio general de las transferencias"* del RGPD establece:

"Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales

desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

En este sentido, el artículo 45 "*Transferencias basadas en una decisión de adecuación*" del RGPD dispone que:

> *"1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica. (…)"*

Mientras que el artículo 46 "*Transferencias mediante garantías adecuadas*" del RGPD dice que:

> *"1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.*
>
> *2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:*
> *a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;*
> *b) normas corporativas vinculantes de conformidad con el artículo 47;*
> *c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;*
> *d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;*
> *e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o*
> *f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.*
> *(…)"*

En el presente caso, ENDESA en su respuesta de fecha 11 de noviembre de 2022 identifica para cada uno de los usuarios comprometidos en la violación de la seguridad de los datos personales en cuestión el proveedor de servicios de ENDESA con el que habían suscrito contrato:

Usuario	Proveedor que tenía asignado el usuario
***USUARIO.1	***EMPRESA.13 (en adelante, ***EMPRESA.13)
***USUARIO.7	***EMPRESA.14 (en adelante, ***EMPRESA.14)
USUARIO.2 (USUARIO.2)	***EMPRESA.8. (en adelante, ***EMPRESA.8)
***USUARIO.8	***EMPRESA.15
***USUARIO.3	***EMPRESA.12 (***EMPRESA.12.)
***USUARIO.4	***EMPRESA.15(en adelante, ***EMPRESA.15)
***USUARIO.5	***EMPRESA.12 (***EMPRESA.12.)
***USUARIO.6	***EMPRESA.17 (en adelante, ***EMPRESA.17)
***USUARIO.9	Este usuario es el mismo que el ***USUARIO.7

Es decir, que ENDESA trabajaba con prestadores ubicados en países dentro y fuera de la Unión Europea. En concreto, los prestadores ***EMPRESA.15** y ***EMPRESA.12.** están ubicados fuera de la Unión Europa, en ***PAÍS.2 y ***PAÍS.1, respectivamente. También consta en el presente procedimiento que ENDESA había autorizado a ***EMPRESA.1** a subcontratar con ***EMPRESA.9**, empresa ubicada en ***PAÍS.1. Por lo que ENDESA estaba realizando transferencias internacionales de los datos personales de su titularidad a estos países.

No obstante, el artículo 45 del RGPD permite la realización de transferencias internacionales de datos personales, sin necesidad de autorización específica, cuando la Comisión hubiera decidido que el tercer país en cuestión garantiza un nivel de protección adecuado. Para el resto de casos, el artículo 46 del RGPD permite la realización de estas transferencias siempre y cuando se ofrezcan garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Hasta el momento, ni ***PAÍS.1 ni ***PAÍS.2 han sido declarados como destinatarios de nivel adecuado por la Comisión Europea, razón por la cual las transferencias de datos personales hacia estos países deben cumplir con garantías adecuadas de las del artículo 46 del RGPD.

En este caso, ENDESA ha realizado transferencias internacionales a ***PAÍS.1 y ***PAÍS.2, y continúa realizando transferencias a ***PAÍS.2, países respecto de los cuales la Comisión no ha declarado que garanticen un nivel de protección adecuado, en los términos que fija el artículo 45 del RGPD.

El considerando (108) del RGPD sobre las transferencias en ausencia de una decisión de adecuación declara que "*el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control (…)".*

El artículo 46 del RGPD trata de las «transferencias sujetas a garantías adecuadas» y dispone en su apartado 1 que, a falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Añade el artículo 46, apartado 2, del RGPD que las «garantías adecuadas» podrán ser aportadas, sin necesidad de autorización expresa de una autoridad de control, entre otras, por cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2. (artículo 46, apartado 2, letra c).

Este artículo debe interpretarse en el sentido de lo declarado por el Tribunal de justicia de la Unión Europea (TJUE), en su sentencia, de 16 de julio de 2020, dictada en el asunto C-311/18 (Schrems II):

"*105 Por tanto, procede responder a las cuestiones prejudiciales segunda, tercera y sexta que el artículo 46, apartados 1 y 2, letra c), del RGPD debe interpretarse en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45, apartado 2, del referido Reglamento*."

En este sentido, la Comisión Europea ha adoptado la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Estas cláusulas contractuales tipo adoptadas por la Comisión Europea constituyen un método para proporcionar «garantías adecuadas» en ausencia de una decisión de adecuación con arreglo al artículo 46, apartado 2, letra c), del RGPD, estableciendo nuevas cláusulas contractuales tipo que pueden ser utilizadas tanto por el responsable como por el encargado a fin de ofrecer garantías adecuadas en el sentido del artículo 46, 1 del RGPD, quedando derogadas las anteriores decisiones de 2001 y 2010, a partir del 27 de septiembre de 2021. Ahora bien a tenor de su cláusula 4.4 se considera que los contratos celebrados antes del 27 de septiembre de 2021 con arreglo a la Decisión 2001/497/CE o la Decisión 2010/87/UE ofrecen garantías adecuadas en el sentido del artículo 46, apartado 1, del RGPD hasta el 27 de diciembre de 2022, siempre que las operaciones de tratamiento que sean objeto del

contrato permanezcan inalteradas y que las cláusulas contractuales tipo garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas.

Sobre este particular ha de recordarse que ENDESA ha aportado:

- Sobre ******EMPRESA.15***:
  - Resolución de la Directora de la AEPD, de 1 de diciembre de 2015, por la que se autoriza la realización de transferencias internacionales de datos personales de ENDESA a ******EMPRESA.15***, ubicada en ***PAÍS.2.
  - Contrato de 11 de noviembre de 2021 por el que se sustituye dicha autorización y se da cumplimiento a lo dispuesto por la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
  - Evaluación de Impacto de Protección de Datos de ***PAÍS.2 como país importador de datos personales.
  - Evaluación de impacto sobre el derecho y las prácticas de ***PAÍS.2 aplicables al tratamiento de los datos personales realizados por el proveedor ******EMPRESA.15***.

- Sobre ******EMPRESA.12*** (...)
  - Contrato entre ENDESA y ******EMPRESA.12.***
  - ***(…)*** se da cumplimiento a lo dispuesto por la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
  - Resolución de contrato entre ENDESA y ******EMPRESA.16***, de fecha 15 de noviembre de 2022.
  - Evaluación de Impacto de Protección de Datos de ***PAÍS.1 como país importador de datos personales.

- Sobre ******EMPRESA.9.*** (...)
  - Contrato entre ENDESA, y ******EMPRESA.9.***, de fecha 22 de julio de 2020.
  - Burofax de 27 de octubre de 2022, de ******EMPRESA.1*** a ******EMPRESA.9***., por el que se resuelve el contrato entre ellos.
  - Comprobante de baja de ******EMPRESA.9.*** como proveedor de ENDESA, con fecha 2 de noviembre de 2021.

De lo anterior cabe concluir que los contratos con ******EMPRESA.12*** y ******EMPRESA.9.*** se rescindieron antes del 27 de diciembre de 2022.

Sentado lo anterior conviene resaltar, respecto de la transferencia internacional realizada a ***PAÍS.2 en virtud del contrato suscrito entre ENDESA y ******EMPRESA.15***, que la cláusula 14 de la decisión se refiere al «Derecho y prácticas del país que afectan al cumplimiento de las cláusulas». Esta cláusula contiene cuatro módulos

relativos a la transferencia de responsable a responsable; transferencia de responsable a encargado; transferencia de encargado a encargado; y transferencia de encargado a responsable, a los que resultan de aplicación las disposiciones que contiene. Así establece lo siguiente:

"*MÓDULO UNO: transferencia de responsable a responsable*

MÓDULO DOS: transferencia de responsable a encargado

MÓDULO TRES: transferencia de encargado a encargado

MÓDULO CUATRO: transferencia de encargado a responsable (solo si el encargado de la UE combina los datos personales recibidos del responsable del tercer país con los datos personales recopilados por el encargado en la UE)

a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:

i)las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;

ii) el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables (12);

iii) las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la

información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.

d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a). [Módulo tres: El exportador de datos notificará al responsable.]

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres:, si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).”

De este modo, la citada cláusula 14 establece una obligación para el exportador e importador de elaborar una evaluación que tenga en cuenta todas las cuestiones que la propia cláusula determina.

Por su parte, el TJUE ha explicado en su sentencia Schrems II:

“132 Dado que, como se desprende del apartado 125 de la presente sentencia, es inherente al carácter contractual de las cláusulas tipo de protección de datos que estas no pueden vincular a las autoridades públicas de países terceros, pero que los artículos 44 y 46, apartados 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta, exigen que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea comprometido, puede resultar necesario completar las garantías recogidas en esas cláusulas tipo de protección datos. A ese respecto, el considerando 109 del referido Reglamento dispone que «la posibilidad de que [los] responsable[s] […] del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión […] no debe obstar a que los responsables […] añadan otras cláusulas o garantías adicionales» y precisa, en particular, que «se debe alentar a los responsables […] a ofrecer garantías adicionales […] que complementen las cláusulas tipo de protección de datos».

133 Resulta, por tanto, evidente que las cláusulas tipo de protección de datos adoptadas por la Comisión en virtud del artículo 46, apartado 2, letra c), del mismo Reglamento tienen únicamente como finalidad proporcionar a los responsables o encargados del tratamiento establecidos en la Unión garantías contractuales que se apliquen de manera uniforme en todos los países terceros y, por tanto, independientemente del nivel de protección garantizado en cada uno de ellos. En la medida en que esas cláusulas tipo de protección de datos no pueden proporcionar, debido a su naturaleza, garantías que vayan más allá de una obligación contractual de velar por que se respete el nivel de protección exigido por el Derecho de la Unión, tales cláusulas pueden necesitar, en función de cuál sea la situación de un país tercero determinado, la adopción de medidas adicionales por parte del responsable del tratamiento con el fin de garantizar el respeto de ese nivel de protección.

134 A este respecto, tal como ha señalado el Abogado General en el punto 126 de sus conclusiones, el mecanismo contractual previsto en el artículo 46, apartado 2, letra c), del RGPD se basa en la responsabilización del responsable o del encargado del tratamiento establecidos en la Unión, así como, con carácter subsidiario, de la autoridad de control competente. Corresponde, por tanto, ante todo, a ese responsable o encargado del tratamiento comprobar, caso por caso y, si es preciso, en colaboración con el destinatario de la transferencia, si el Derecho del tercer país de destino garantiza una protección adecuada, a la luz del Derecho de la Unión, de los datos personales transferidos sobre la base de cláusulas tipo de protección de datos, proporcionado, cuando sea necesario, garantías adicionales a las ofrecidas por dichas cláusulas."

En este orden de ideas han de tenerse también en cuenta las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020, en las que al interpretar la citada sentencia del TSJUE declaran que "*el Tribunal deja abierta la posibilidad de que los exportadores apliquen medidas complementarias que palíen estas lagunas de protección, a fin de que esta alcance el nivel exigido por el Derecho de la Unión. El Tribunal no especifica qué medidas podrían ser. Sin embargo, el Tribunal subraya que los exportadores tendrán que determinarlas caso por caso. Tal extremo concuerda con el principio de responsabilidad proactiva del artículo 5, apartado 2, del RGPD, que exige que los responsables del tratamiento sean responsables y capaces de demostrar el cumplimiento de los principios del RGPD relativos al tratamiento de datos personales (…)*"

En el presente caso, ENDESA ha aportado la Evaluación de Impacto sobre Transferencias a ***PAÍS.2, que tiene por objeto evaluar, en relación con la transferencia de datos personales del exportador al importador, el nivel de adecuación del tercer país de destino, así como la adopción de medidas de seguridad técnicas y organizativas adecuadas para mitigar el riesgo de dicha transferencia.

Así las cosas, esta evaluación se limita a valorar las medidas de seguridad técnicas y organizativas aplicadas por el importador de datos, sin abordar la necesidad o no de otras posibles medidas contractuales complementarias a las cláusulas contractuales tipo que pudieran ser necesarias.

En este orden de ideas cabe destacar que, en dicho documento, en cuanto a la evaluación legislativa del país importador ***PAÍS.2, la evaluación arroja el resultado “3 – Parcialmente adecuado”, limitándose a contemplar la existencia de una normativa de protección de datos y de una autoridad de control independiente en el tercer país, pero ni siquiera se analizan las funciones y poderes de esta autoridad.

Asimismo, aporta el documento denominado “análisis legislación y prácticas” de ***PAÍS.2, destinado a evaluar si los datos personales que se transfieren están adecuadamente protegidos en relación con el potencial acceso de las autoridades de los países a los que se transfieren los datos. En este documento se recoge que la Constitución de ***PAÍS.2 garantiza el derecho fundamental a la intimidad personal y familiar y que recoge la necesidad de orden judicial para la interceptación de las comunicaciones. También se tiene en cuenta, en este documento, la existencia de una ley de protección de datos.

Tras el análisis de las circunstancias que aborda el documento en el mismo se concluye lo siguiente:

> *CONCLUSIÓN*
> *Se entiende que ***PAÍS.2 cuenta con un marco normativo que, si bien no puede considerarse como equivalente al establecido en la Unión Europea en lo que se refiere a la protección de los datos personales, sí que puede considerarse como razonablemente adecuado.*
> *Sin embargo, para alcanzar una conclusión definitiva sobre la idoneidad de la transferencia internacional, así como sobre la suscripción de medidas de garantía adicional para que el nivel de protección de los datos transferidos se ajuste a la norma de equivalencia esencial de la Unión Europea, es necesario tener en cuenta y evaluar el resto de los componentes, vinculados a las particularidades de cada una de las transferencias.*

En definitiva, del análisis de esta documentación no puede afirmarse que la evaluación contemple un análisis del derecho y las prácticas de ***PAÍS.2 suficiente que permita valorar si el tercer país de destino ofrece un nivel de protección adecuado. De este modo, no contiene ninguna evaluación sobre la existencia de normas que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades, así como las limitaciones y garantías aplicables. Según la citada STJUE este análisis debería incluir los elementos que se recogen en el artículo 45.2. del RGPD, que incluye el análisis sobre la existencia de tratados internaciones firmados por el tercer país u otros compromisos internacionales adoptados (artículo 45.2.c) RGPD), el estudio de la legislación nacional del tercer país en el sentido pretendido por el artículo 45.2.a) del RGPD:

“*el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese*

país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos"

En este sentido el considerando (20) de la Decisión de Ejecución (UE) 2021/914 de la Comisión dispone:

"Las partes deben tener en cuenta, en particular, las circunstancias específicas de la transferencia (como el contenido y la duración del contrato, la naturaleza de los datos transferidos, el tipo de destinatario y la finalidad del tratamiento), el Derecho y las prácticas del tercer país de destino que sean de aplicación dadas las circunstancias de la transferencia y las garantías establecidas para complementar las garantías contempladas en las cláusulas contractuales tipo (como medidas contractuales, técnicas y organizativas pertinentes que sean de aplicación a la transferencia y al tratamiento de los datos personales en el país de destino). Por lo que se refiere al efecto del Derecho y prácticas mencionados sobre el cumplimiento de las cláusulas contractuales tipo, pueden valorarse diferentes elementos en una evaluación global; por ejemplo, información fiable sobre la aplicación del Derecho en la práctica (jurisprudencia, informes de organismos de supervisión independientes, etc.), la existencia o ausencia de solicitudes en el mismo sector y, en condiciones estrictas, la experiencia práctica documentada del exportador y/o el importador de datos."

Sin embargo, ninguna de estas circunstancias ha sido tenida en cuenta. Las deficiencias observadas en la Evaluación de Impacto de Protección de Datos de ***PAÍS.2 como país importador de datos personales impiden que pueda considerarse aportada la garantía de la cláusula 14.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a ENDESA, por vulneración del artículo 44 del RGPD.

XVII
Tipificación y calificación de la infracción del artículo 44 del RGPD

En el presente caso, se considera que ENDESA no ha cumplido con los requisitos exigidos para poder realizar las transferencias internacionales de datos a sus proveedores y subcontratistas ubicados en ***PAÍS.2.

Los hechos conocidos son constitutivos de una infracción, imputable a ENDESA**,** tipificada en el artículo 83.5 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

(…)

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49; (…)"

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72.1.l) de la LOPDGDD, que califica de muy grave la siguiente conducta:

> *"l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679".*

XVIII

Sanción por la infracción del artículo 44 del RGPD

Esta infracción puede ser sancionada con multa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no cumplir con los requisitos exigidos para la realización de transferencias internacionales a sus proveedores y subcontratistas ubicados en ***PAÍS.2, afectados por la brecha de seguridad en cuestión, de los datos de 30,6 millones de puntos de suministros de electricidad y 8,6 millones de puntos de suministros de gas de no clientes de ENDESA, y de los datos de identificación, domicilio, teléfono, correo electrónico, número de cuenta bancaria, entre otros, de 4,8 millones de clientes de electricidad y 1,8 millones de clientes de gas de ENDESA.

- Negligencia en la infracción (apartado b): ENDESA es una gran empresa en su sector de negocio, que debe velar por el derecho fundamental a la protección de los datos personales de su titularidad. En el presente caso, esta Agencia considera que ha sido gravemente negligente a la hora de analizar si ***PAÍS.2 como país importador de datos personales goza de una protección adecuada. En especial, teniendo en cuenta que se trata no solo de una gran empresa de la que cabría exigir una mayor profesionalidad, sino que es una entidad habituada al tratamiento de datos personales. En este sentido, resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), la cual indica que *"…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".*

Negar la concurrencia de una actuación negligente por parte de la parte recurrente equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no se comparte esta perspectiva de los hechos, puesto que ha quedado acreditada la grave falta de diligencia debida.

A lo largo del presente procedimiento sancionador ha quedado acreditado que ENDESA no ha realizado una debida evaluación de ***PAÍS.2 como país importador de datos personales (al cual se continúa enviando datos personales en la actualidad).

Por la importancia del bien jurídico protegido, ENDESA estaba obligado a ello pese a lo cual no ha cumplido con tal deber. Por lo que se considera que su comportamiento ha sido gravemente negligente.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

Como agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una empresa grande habituada al tratamiento de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite imponer una sanción de multa administrativa de 500.000 € (quinientos mil euros).

XIX
Adopción de medidas

Al confirmarse la infracción, corresponde imponer al responsable que en el plazo de 6 meses proceda a adecuar las transferencias internacionales de los datos personales que realiza ENDESA a ***PAÍS.2 a lo dispuesto en los artículos 44 y siguientes del RGPD. La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

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

Por lo tanto, 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 **ENDESA ENERGÍA, S.A.U**., con **NIF A81948077:**

- Por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, una multa administrativa de cuantía 2.500.000,00 euros.

- Por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, una multa administrativa de cuantía 1.500.000,00 euros.

- Por una infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 de dicha norma, una multa administrativa de cuantía 800.000,00 euros.

- Por una infracción del artículo 34 del RGPD, tipificada en el artículo 83.4 de dicha norma, una multa administrativa de cuantía 800.000,00 euros.

- Por una infracción del artículo 44 del RGPD, tipificada en el artículo 83.5 de dicha norma, con multa administrativa de cuantía 500.000,00 euros.

SEGUNDO: ORDENAR a **ENDESA ENERGÍA, S.A.U**., con NIF **A81948077**, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 6 meses, acredite haber procedido a adecuar las transferencias internacionales de los datos personales que realiza a ***PAÍS.2 a lo dispuesto en los artículos 44 y siguientes del RGPD.

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

CUARTO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad.
Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 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, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en

la entidad bancaria CAIXABANK, S.A.. 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 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, 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-electronica-web/], 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.

938-250923

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