Procedimiento Nº: E/09014/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad XFERA MOVILES, S.A.U., y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 25/04/2018, tuvo entrada en esta Agencia una reclamación presentada por Dña. ***A.A.A.*** (en lo sucesivo la reclamante) contra la entidad XFERA MOVILES, S.A.U. (en lo sucesivo XFERA), de la que es cliente, señalando que recibió un correo de esta operadora relativo a la aplicación del nuevo Reglamento de Protección de Datos, en el que le indican que es necesaria su *"autorización para seguir comunicándose"* con la reclamante y le requieren que acepte los nuevos términos y condiciones que aparecen en un vínculo del mensaje. Añade que en el cuerpo del mensaje le ofrecen un resumen de esos términos con intención de hacerle ver que son grandes ventajas para ella misma y que al abrir el citado vínculo se informa que la primera finalidad es facilitar la prestación del servicio de telecomunicaciones, *"a lo que añaden otras once finalidades que engloban dentro del consentimiento"*. Advierte la reclamante que podría estar de acuerdo con algunas de esas finalidades, *"pero no con todas"*.

Concluye la reclamante señalando lo siguiente:

"Por todo ello, DENUNCIO:
. Que la comunicación enviada por la operadora Yoigo para conseguir mi aceptación del consentimiento para utilización de mis datos personales es ambigua y tendente a hacerme creer, como cliente, que dicho consentimiento es necesario para
a) poder seguir comunicándose conmigo
b) poder seguir dándome la prestación del servicio contratado con ellos
. Que la operadora Yoigo, mediante dicha comunicación, obliga a aceptar todos los términos simultáneamente, mediante un único consentimiento. Por lo que, como cliente, sólo tendría la opción de aceptar o no aceptar su redacción (bajo el miedo a quedarme sin servicio, al hilo del primer punto denunciado)".

Con su reclamación, aporta copia del correo objeto de la reclamación, de fecha 24/04/2018, remitido a la dirección de correo electrónico de la reclamante desde la dirección clientes@yoigo.com. El contenido de este mensaje es el siguiente:

<<YOIGO
LOS CAMBIOS SIEMPRE SON PARA MEJOR
Hola NOMBRE CLIENTE

Tenemos algo que contarte que es bueno para ti: en Europa hay una nueva normativa para proteger la privacidad de los clientes y usar bien sus datos. Por eso, a partir de mayo nuestros términos de protección de datos cambian (léelos aquí), y necesitamos tu autorización para poder seguir comunicándonos contigo.

Este es el resumen de los términos, léelo y dinos si los aceptas.

ESTARÁS MÁS Y MEJOR INFORMADO
Recibirás información y promos del resto de compañías del grupo, y de otros que te interesen. (P. ej. Seguros para Móviles, etc.).

NO MÁS PUBLICIDAD GENÉRICA
Solo te ofreceremos ofertas que se adapten a tus necesidades en función de tu uso de navegación, tráfico y geolocalización.

LO MEJOR DE LO MEJOR PARA TI
Podrás tener los mejores servicios del resto de empresas del grupo, ya que les comunicaremos tus datos.

SEGUNDAS PARTES SERÁN MEJORES
Y si te vas y tenemos ofertas que te puedan interesar, te lo diremos para que vuelvas si quieres.

SÍ, ACEPTO

En otro momento

Este correo electrónico ha sido enviado por un sistema automática, por favor no responda al mismo>>.

Aporta la reclamante, asimismo, copia de los *"Términos y condiciones de Yoigo aplicables a la protección de datos"*, a los que se accede mediante el enlace "(léelos aquí)" insertado en el mensaje reseñado.

SEGUNDO: Con fecha 11/06/2018, se dio traslado de la reclamación a XFERA. Con fecha 09/10/2018, la Delegada de Protección de Datos de la citada entidad remitió a esta Agencia, en fecha 09/10/2018, la respuesta siguiente:

1. En una alegación preliminar, al referirse a la comunicación electrónico objeto de la reclamación, señala que la misma *"informa de la existencia del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD) y del cambio, a partir de mayo, de los términos y condiciones aplicables a la protección de datos de los servicios que tiene contratados con YOIGO"*. Añade que *"En la citada comunicación YOIGO le solicitaba su autorización para poder seguir comunicándose conforme a los nuevos términos y condiciones aplicables a la protección de datos cuya información es facilitada"*.

2. En la fecha en que se realizó la comunicación, el marco normativo que regulaba el tratamiento de los datos de carácter personal estaba conformado por Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en lo sucesivo LOPD) y su Reglamente de desarrollo, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre (en lo sucesivo RLOPD), y no por el RGPD, de aplicación a partir del 25/05/2018.

Considera que la solicitud de consentimiento realizada se ajusta, en concreto, a lo establecido en el en los artículos 3.h) y 6.1 de la LOPD, y artículos 12 y siguientes del

RLOPD.

3. Se opone a las manifestaciones realizadas por la reclamante, indicando que la información facilitada está caracterizada por su claridad y sencillez en su redacción, y destaca la facilidad de acceso a la misma.

Considera que la información hace referencia exclusivamente a las finalidades que se indican, por lo que no considera cierto que se haga creer al cliente que el consentimiento que se solicita sea necesario para que la entidad siga comunicándose con la reclamante, y rechaza que este consentimiento sea necesario para continuar con la prestación del servicio. A este respecto, manifiestan que la reclamante ha podido malinterpretar la información que se le remitió, pese a la claridad de la misma, en la que se identifica como primera finalidad la prestación del servicio de telecomunicaciones, cuya legitimidad radica en la ejecución del contrato que ambas partes mantienen en vigor.

Advierte que la entidad no obliga a sus clientes a aceptar las proposiciones u ofrecimientos que les presenta, sino que éstos son libres para aceptarlas o no, como en este caso, en el que se facilitó a la reclamante la opción de aceptar los nuevos términos y condiciones haciendo mediante el botón *"SI, ACEPTO"* o no aceptarlos mediante el botón *"En otro momento"*.

Finalmente, en relación con la simultaneidad aludida por la reclamante, la entidad responsable manifiesta que desde la entrada en vigor del RGPD presenta sus solicitudes para recabar el consentimiento de forma "granulada", es decir, disociando cada una de las finalidades y obteniendo el consentimiento para cada una de ellas.

TERCERO: A la vista de los hechos expuestos, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo Reglamento General de Protección de Datos o RGPD), con el desarrollo siguiente:

Por los Servicios de Inspección de la Agencia se remitió a XFERA un requerimiento para que aportase la información siguiente:

"1. Especificación del número de clientes a los que se remitió el correo electrónico de fecha 24/04/2018, en el que se informa sobre los términos de protección de datos que estarán vigentes a partir de mayo y se solicita autorización para varios tratamientos.
2. Especificación del número de clientes que han autorizado los citados tratamientos.
3. Copia de los citados "términos de protección de datos" a los que se hace referencia en el correo y a los que se podía acceder desde el mismo.
4. Especificación detallada de los tratamientos que se autorizaban por parte del cliente al aceptar mediante la opción de "SI, ACEPTO".
5. Especificación de los tratamientos que se han realizado con los datos de los clientes que prestaron su conformidad mediante dicha acción.
6. Especificación del procedimiento por el que se identifican en sus ficheros aquellos

clientes que no autorizaron dichos tratamientos, adjuntado copia impresa de las pantallas correspondientes.

7. *Copia de los términos y condiciones de protección de datos vigentes en la actualidad, en el caso de que sean diferentes de los que se mencionaban en el citado correo"*.

Con fecha 25 de marzo de 2019, XFERA remite a la Agencia la siguiente información:

1. La comunicación recibida por la reclamante se remitió a todos los clientes de YOIGO, en previsión de la entrada en vigor del RGPD, para concienciar a los clientes de la novedad legislativa y para ir ajustando los procesos a los requerimientos de la nueva normativa, según se interpretaba en aquellos primeros momentos y sin perjuicio de constatar que la legislación vigente no era otra que la LOPD y su Reglamento de desarrollo.

2. No pueden especificar el número de clientes que autorizaron los tratamientos que se indicaban porque no se individualiza, en los registros internos, la fuente de procedencia del consentimiento, que es diversa ("correo electrónico, página web, aplicaciones para móviles, teléfono…).

3. No aporta los "Términos y condiciones" a los que hacía referencia el correo electrónico objeto de la reclamación porque ya fueron aportados por la reclamante.

4. Los tratamientos tomados en consideración son los recogidos en el propio correo electrónico, así como en los citados "Términos y condiciones".

5. *"Los tratamientos realizados son los que se describen en los antes citados "Términos y condiciones" que ya le constan a la AEPD"*.

6. *"El procedimiento que se sigue en XFERA MÓVILES a los efectos de identificar los consentimientos prestados por sus clientes se basa en la herramienta eConsent de la empresa CYBERCOMPLIANCE. A estos efectos se acompañan 4 certificados que describen y certifican como funciona esta herramienta"*.

7. En relación con la cuestión séptima requerida por los Servicios de Inspección, sobre la entrega de copia de los términos de protección de datos vigentes en la actualidad, en el caso de que sean diferentes de los que se mencionan en el citado correo, XFERA responde: *"No son diferentes. Son los mismos que ya constan como aportados"*.

XFERA aporta un informe sobre la operatividad de la herramienta *"eConsent"*, emitido en fecha 18/03/2019 por la entidad Cyber Compliance, S.L., en el que se describe el procedimiento que se sigue para identificar los consentimientos prestados por los clientes:

. La citada herramienta es un servicio tipo SaaS (software como servicio) que se integra en la página web y permite la identificación digital del usuario mediante sus datos de navegación y el registro de las actividades que realiza, es decir, si presta o no su consentimiento a los distintos tratamientos de datos que propone la empresa-cliente. Posibilita una gestión centralizada de la privacidad registrando los consentimientos que un interesado puede prestar a lo largo del tiempo.

. Por motivos de funcionalidad y de agilidad en los procesos de obtención y gestión de los consentimientos no se exige al usuario que se identifique mediante certificado electrónico.

. El proceso que se desarrolla a través de eConsent para la obtención de los consentimientos y la generación de evidencias es el siguiente:

Paso número 1: Creación de la pasarela de consentimientos del consentimiento

Cyber Compliance, S.L. da acceso a la empresa-cliente a una librería JavaScript, para que la incluyan en su plataforma. De esta manera el cliente deberá invocarla para que se genere el código HTML, que finalmente se renderizará a su plataforma web.
Dicho módulo no permite ninguna alteración de contenido por parte de la empresa-cliente, quien solo tiene acceso a los otorgamientos de consentimiento, cerciorándose de este modo de que el contenido sobre el que se lleva a cabo el certificado corresponde con el otorgado por el interesado.

Según la entidad Cyber Compliance, S.L., el mecanismo de obtención de consentimientos se llevará a cabo de forma individualizada, cumpliendo con la condición del G29 de un consentimiento granular.

Paso número 2: Obtención de consentimiento y cálculo de los diversos Códigos de verificación

Una vez insertado el código, al navegar el usuario-interesado por la plataforma web de la empresa-cliente visualizará el catálogo de consentimientos y podrá desarrollar la acción deseada, es decir, prestar, o no, su consentimiento a cada una de las preguntas que se le realizan.
Aunque visualmente no resulta perceptible al usuario, la acción de prestar el consentimiento no se ejecuta sobre la plataforma web de la empresa, sino, directamente sobre eConsent, para evitar cualquier manipulación.

Paso número 3: Generación de evidencias

Recibidos los consentimientos otorgados se procederá al desarrollo de los códigos de verificación operacionales o hashes operacionales, correspondientes a cada conjunto de consentimientos otorgados/rechazados por un interesado determinado.

La información que se conserva (hash operacional) se genera a partir de los datos: identificador del usuario en la base de datos del cliente, fecha y hora, los otorgamientos/rechazos de consentimientos, información del navegador (ej., dirección IP), información de la navegación obtenida de forma independiente por eConsent (ej., la web a través de la cual el interesado prestó/rechazó el consentimiento).
Sucesivamente, cada hora, se generará un código de certificación o hash de certificación, el cual contenga la pluralidad de los hashes operacionales generados en el mencionado espacio de tiempo.

Paso número 4: Certificación en Blockchain:

Blockchain es una base de datos que registra bloques de información entrelazándolos entre sí.
EConsent utiliza como explorador el Blockchain de Ethereum, el cual da acceso a toda la cadena de bloques, permitiendo al usuario verificar todas las operaciones que registra

de forma segura y a tiempo real. Generado el hash de certificación se procederá a su emisión al explorador Blockchain de Ethereum, del cual se recibirá la "FIRMA DE LA CERTIFICACIÓN". Por tanto, dicha Firma certificará la recepción de la información enviada (el hash operacional) por el Blockchain de Ethereum.

Paso número 5: Recopilación de la información e inserción en el Certificado de Consentimientos

Una vez toda la información ha sido generada y obtenida por eConsent se procederá a la elaboración del Certificado de Consentimientos del cual se entregará una copia a la empresa-cliente.

Dicho certificado se compone de diferentes partes:

. Intervinientes (datos del responsable del tratamiento y del interesado);
. Dominio (web a través de la que se obtuvieron los consentimientos);
. Documentos que forman parte del proceso, registrados a través de un hash;
. Información de acciones realizadas:

. Sobre la obtención de los consentimientos, se detalla lo siguiente:

. Los consentimientos solicitados por el módulo de gestión de consentimientos.
. Las correspondientes respuestas (otorgamientos o rechazos) del interesado.
. El Código de la Operación. Se trata un hash SHA-256 que resume tanto el contenido de las preguntas realizadas al usuario-interesado como su respuesta, es decir, si prestó o no su consentimiento.
. La fecha y hora de la obtención de los consentimientos.
. El hash operacional de esos determinados consentimientos.

. Certificación de los consentimientos, que detalla la información siguiente:

. El Código de la Operación.
. La fecha y la hora de emisión de la información al explorador Blockchain de Ethereum.
. La Firma de la Certificación obtenida de Ethereum. Con esta el cliente podrá acceder, a través de una de las plataformas, a Ethereum y verificar la transacción realizada por eConsent. Pudiendo comprobar, por ejemplo, a qué hora se insertó exactamente el bloque de información en Blockchain.

XFERA aporta tres *"certificados de consentimientos"* emitidos por la sociedad Cyber Compliance, S.L., en los que se indica *"La sociedad… emite este certificado en el que se resumen las evidencias electrónicas obtenidas en el proceso de obtención de consentimientos con ID… el día…"*. Dichos certificados se refieren a consentimientos obtenidos en fechas 15/09/2018, 30/11/2018 y 01/02/2019.

El certificado de fecha 30/11/2018 incluye la información siguiente:
. Intervinientes; responsable del tratamiento Xfera Móviles, S.A.; usuario: dirección IP…

ID Usuario… ID Único…
. Dominio (URL exacta desde la que se obtuvieron los consentimientos)
. Documentos (código del contenido y código del catálogo de consentimientos)
. Acciones realizadas. Obtención de los consentimientos (código de la operación, fecha y hora)
. Consentimientos otorgados/rechazados por el usuario (descripción del tratamiento y respuesta del interesado):

". Acciones comerciales:
. Envío de ofertas y promociones de productos y servicios de empresas del Grupo.
. Envío de ofertas y promociones de productos y servicios de colaboradores.
. Uso de sus datos de tráfico y navegación para ofrecerle ofertas y promociones propias, del Grupo y de terceros.
. Geolocalización: Uso de sus datos de geolocalización para ofrecerle ofertas y promociones propias, del Grupo y de terceros.
. Cesión de datos a empresas del Grupo
. Perfilado
. En base a la información proporcionada por terceros.
. En base a la consulta a sistemas de información crediticia y realización de scoring.
. Uso de datos finalizado el contrato".

. Datos de la transacción para el usuario (código de la operación, fecha y código de la transacción).

Los certificados de 15/09/2018 y 01/02/2019 incluyen la misma información, si bien la estructura del apartado *"Consentimientos otorgados/rechazados por el usuario"* presenta alguna variación. La estructura de este apartado en estos certificados es la siguiente:

". Acciones comerciales:
. Envío de ofertas y promociones de productos y servicios de empresas del Grupo.
. Envío de ofertas y promociones de productos y servicios de terceros (se sustituye el término "colaboradores" del anterior certificado por el de "terceros").
. Uso de sus datos de tráfico y navegación para ofrecerle ofertas y promociones propias, del Grupo y de terceros.
. Uso de datos de geolocalización para ofrecerle ofertas y promociones propias, del Grupo y de terceros (en el certificado anterior se incluía como un apartado diferenciado del de "Acciones comerciales").
. Cesión de datos a empresas del Grupo
. Perfilado
. En base a la información proporcionada por terceros.
. En base a la consulta a sistemas de información crediticia y realización de scoring.
. Uso de datos finalizado el contrato".

En los tres certificados aportados figura la respuesta *"Acepto"* en todos los consentimientos detallados en el apartado *"Consentimientos otorgados/rechazados por el*

usuario" (ninguno consentimiento "rechazado").

CUARTO: Con fecha 08/04/2019, por la Subdirección General de Inspección de Datos, a través de la web yoigo.com, se accede al documento *"Condiciones Generales de Prestación del Servicio Telefónico Móvil de Contrato"* y se comprueba que incluye un apartado de "Protección de Datos" que incluye la misma información que consta en el documento que se adjunta como Anexo 1.

Asimismo, se constata que el documento *"Condiciones generales de uso del sitio web de Xfera Móviles, S.A.U. términos y condiciones en protección de datos"* insertado en la misma web incluye los datos de contacto del Delegado de Protección de Datos de la entidad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Hay que señalar que la denuncia tuvo entrada en la AEPD el 25/04/2018, por tanto, vigente tanto la LOPD como su Reglamento de desarrollo.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, señala en su Disposición Transitoria Quinta *"El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor."*

La Disposición Final Segunda determina: *"El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el "Boletín Oficial del Estado".*

Habiéndose publicado el mismo el 19/01/2008, el citado R. D. por el que se aprueba el Reglamento de desarrollo de la LOPD, entró en vigor el 19/04/2008

En su artículo 126, se señala que:

"1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo

de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo".

Y en el artículo 122, se establece que:

"1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas".

III

A tenor de lo dispuesto en los artículos transcritos, las actuaciones previas han de entenderse caducadas transcurridos más de doce meses desde que tuvo entrada en la Agencia la denuncia del afectado, hasta la notificación del acuerdo de inicio del procedimiento sancionador.

Es necesario señalar que en el presente caso resulta de aplicación el plazo máximo de doce meses de duración establecido en el artículo 122 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, que establece para la realización de dichas actuaciones previas, tomando en consideración que tal norma reglamentaria es de aplicación a actuaciones iniciadas con posterioridad a su entrada en vigor (es decir, a partir del 19 de abril de 2008).

La denuncia tuvo entrada en esta Agencia Española de Protección de Datos el 25/04/2018, llevándose a cabo con posterioridad actuaciones de investigaciones previas al objeto de determinar si concurrían circunstancias que justificaran la iniciación del

procedimiento sancionador correspondiente.

No obstante, habiendo transcurrido más de 12 meses desde la entrada en la AEPD del escrito de denuncia procede declarar la caducidad de las citadas actuaciones previas.

Por otra parte, el artículo 95.3 de la LPACAP señala lo siguiente:

"3. La caducidad no producirá por sí sola la prescripción de las acciones del particular o de la Administración, pero los procedimientos caducados no interrumpirán el plazo de prescripción.

En los casos en los que sea posible la iniciación de un nuevo procedimiento por no haberse producido la prescripción, podrán incorporarse a éste los actos y trámites cuyo contenido se hubiera mantenido igual de no haberse producido la caducidad. En todo caso, en el nuevo procedimiento deberán cumplimentarse los trámites de alegaciones, proposición de prueba y audiencia al interesado".

Por lo tanto, de acuerdo con lo señalado, por **la Directora de la Agencia Española de Protección de Datos,**

SE ACUERDA:

• **DECLARAR** la **CADUCIDAD** de las presentes actuaciones.

• **NOTIFICAR** la presente Resolución a XFERA MOVILES, S.A.U. y a Dña. ***A.A.A.***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición 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 del referido texto legal.

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