- **Procedimiento Nº: E/05917/2019**

940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 22/05/2018 se recibe denuncia de SECURITAS DIRECT ESPAÑA (en lo sucesivo SD) manifestando que ***A.A.A.*** remitió el 11 del mismo mes y año, dos correos electrónicos a través de la dirección electrónica ******EMAIL.1*** en los que se deduce que tienen documentos de los que son responsables SD.

La denuncia interesa requerir a la Sra. ***A.A.A.*** y a SINDICATO DE TRABAJADORES DE SEGURIDAD PRIVADA-INTERSINDICAL, (INTERSINDICAL) información sobre el origen de los documentos a los que ha tenido acceso.

Aporta copia de un correo de 11/05/2018, 10 h 59 , dirigido a varias personas con dominio securitasdirect.es y dominio *policia.es*, indica: "*Asunto<<. Contratos originales* "*"el lunes depositaremos en el juzgado todos los contratos que nos han llegado junto a una denuncia*". "*os paso unos cuantos no tengo tiempo de escanear el resto hay de todos los años ahí van los más antiguos 1998*".

En otro correo del mismo día a las 11:30 indica , "*asunto: Otros tantos*" "o*tros tantos van en bloque no puedo dedicar tiempo a escanear uno por uno, faltan más el lunes los tenéis en* ******DIRECCIÓN.1*** *que hagan lo que les dé la gana con ellos" "los de otros años pasaron por los ordenadores de algunas de vuestras antiguas distribuidoras y extrabajadores*". En el primer correo pone en el pie de firma el nombre "***A.A.A.***".

Según SD, se deduce que obran en poder de la reclamada contratos de seguridad de clientes de SECURITAS DIRECT que contienen datos de carácter personal. En algunos casos incluyen palabras de seguridad, domicilio y domicilios de los titulares. Manifiesta que toda la información contenida en los documentos, tanto físicos como digitales son tratados por SD con confidencialidad, existiendo protocolo de protección en el tratamiento de la misma, no pudiendo acceder más que las personas facultadas para ello.

Indica que "*desconoce cómo la denunciada e INTERSINDICAL han podido obtener dicha documentación*" y que "*ni la Sra. **A.A.A.** ni INTERSINDICAL cuentan con autorización para tener esta documentación*" concluyendo que no han podido acceder a través de un medio lícito.

Considera SD que la denunciada deja entrever en su correo electrónico que la documentación ha podido ser extraída en connivencia con entre otras personas, antiguas empresas distribuidoras y ex trabajadores de SD. Añade que la propia denunciada fue empleada de la compañía desde 10/12/2007 a 4/02/2008 y que la documentación está expuesta en la web oficial de Facebook de INTERSINDICAL.

Manifiesta que SD ha puesto en marcha labores de averiguación sobre el alcance de lo ocurrido y concreta que el número de contratos en posesión de la denunciada son 111, suscritos entre 1998 y 2015 la mayoría del año 98, de los cuales, 58 contratos pertenecen a clientes particulares y 53 a empresas, siendo de los particulares sólo 20 con relación vigente.

De estos 20 operativos, de 18, SD dispone de los contratos en papel encontrándose almacenados en el domicilio del proveedor de servicios NORMADAT, y de los otros dos contratos, se dispone del documento digitalizado. Indica SD que del análisis efectuado, se pudo verificar que el impacto de estos hechos no revestía especial gravedad respecto a los sistemas de información y potenciales titulares de datos afectados.

Como medida tomada, SD "*procedió a verificar la información, y a contactar de manera urgente con todos los clientes operativos referidos en los contratos remitidos por la denunciante con el fin de que pudiesen cambiar sus claves de* seguridad". "*Se han verificado los sistemas de Securitas Direct y no consta ningún acceso no autorizado a dicha información". Manifiesta que "el 14/05/2018 ha interpuesto querella por presunta comisión de delito de descubrimiento y revelación de secretos contra la denunciante y contra Intersindical*" en los juzgados de instrucción de ******LOCALIDAD.1***

SEGUNDO: La Subdirección General de Inspección dio traslado de dicha reclamación a SINDICATO DE TRABAJADORES DE SEGURIDAD PRIVADA-INTERSINDICAL, (INTERSINDICAL), para que procediese a su análisis e informase a esta Agencia.

El primer envío 25/06/2018, efectuado por notificación electrónica, fue rechazado por no acceso al transcurrir el tiempo previsto para ello.

Se vuelve a enviar por el sistema SICER (correo certificado) siendo entregado el 12/07/2018.

Con fecha 24/08/2018 responde ***A.A.A.,*** sin referencia alguna a INTERSINDICAL, a las siguientes cuestiones planteadas:

1. *"Especificación clara de las causas que han motivado la incidencia que ha dado lugar a la reclamación"*.

Manifiesta que SD no controla la información de la que dispone, que sus datos circulan sin ningún control. *"Estos hechos fueron denunciados en la Dirección General de la Guardia Civil en el año 2016 y en la Unidad Central de seguridad privada en 2017 sin que hasta la fecha hayan realizado ningún tipo de actuación".* Indica que la incidencia no es tal sino que es el funcionamiento habitual de la empresa.

2. *"Detalle de las medidas adoptadas por el responsable para solucionar la incidencia y para evitar que se produzcan nuevas incidencias como la expuesta."*

Manifiesta que esta cuestión ha de ser planteada a SD, que es el responsable del tratamiento.

3. *"Documentación acreditativa de que, de acuerdo con lo previsto en el artículo 12 del RGPD, se han tomado las medidas oportunas para facilitar al afectado el ejercicio de sus derechos en virtud de los artículos 15 a 22, incluyendo copia íntegra de las comunicaciones remitidas en respuesta a las solicitudes efectuadas*."

Manifiesta que esta información ha de ser solicitada responsable del tratamiento.

4. *“Documentación acreditativa de que se ha atendido el derecho del reclamante a ser informado sobre el curso y el resultado de la presente reclamación*.”

Manifiesta que esta información ha de ser solicitada a la SD como responsable del tratamiento e indica que estas obligaciones de custodia documental recaen sobre SD, añadiendo que “*estas bases de datos*” circulan ilegalmente entre diferentes colectivos . Añade que esta empresa hace constar en papel, datos de los clientes con palabras claves en el denominado *datos de preinstalación. A*djunta un documento con dicho título que contiene datos personales, dirección , DNI números de teléfono, palabras clave, de *cliente*, de *SD* y *coacción*.

TERCERO: La Subdirección General de Inspección realizó las actuaciones de investigación E/9019/2018:

1. Requerida información a SECURITAS DIRECT, con fecha 14 y 28/03/2019 manifiesta:

- Sobre: “*Hallazgos basados en la investigación sobre la fuga de datos personales denunciada*.”

Indica, que reitera las manifestaciones realizadas en su denuncia inicial. Aportan en documento 1, copia de correo electrónico enviado desde INTERSINDICAL el 12/07/2018 en el que le indica a personal de SD, asunto “*protección de datos*” “*preguntad a los extrabajadores que se dedican a colaborar con chorizos a los que trapichean con drogas. Tenéis unos cuantos. Perdona que no me esfuerce mucho con la AEPD*” Remite al menos 10 archivos pdf. Manifiesta SD que ese correo es una copia del escrito que iban a presentar a la Agencia. Indica también que SD dispone “*de los contratos originales de los clientes activos que fueron expuestos por INTERSINDICAL*”.

- Sobre: “*Detalle de las medidas adoptadas por el responsable del tratamiento para solucionar la incidencia y para evitar que se produzcan nuevas incidencias como la expuesta: medidas de seguridad técnicas y organizativas, custodia, anonimización, periodo de conservación, destrucción, etc.*”

indica que sobre este aspecto ya se comunicó en la denuncia . Añade que desde 1998 hasta abril 2014, la contratación era en papel, fecha en la que se introdujo el contrato digital de modo paulatino incrementando el porcentaje de contratos digitales frente al de papel, como ejemplo en el 2015 el porcentaje era 89% digital 11% en papel. Indica que cuando se firma un contrato digital se envía una copia del contrato al cliente por correo electrónico a través de un tercero de confianza que actualmente es la empresa LOGALTY, y el acceso a dicho documento requiere introducir contraseña, generalmente el DNI del cliente.

En escrito de fecha 28/03/2019, añade que la mayoría de los contratos del año 98 estaba en papel y que el documento original completo se debía llevar para registrar a la Jefatura de policía la provincia, y esta circunstancia obligaba a tener un control de la documentación en papel en el 2005. El Ministerio de Interior instauró una aplicación para comunicar los contratos de manera telemática y ya no era necesario llevar físicamente una copia de los contratos aunque dicha entidad. Los contratos originales eran enviados a la sede central desde donde se envían posteriormente a NORMADAT, empresa que custodia la documentación.

indica que los PC y móviles corporativos disponen de medidas para evitar filtración de información, se dispone de un proceso de parcheo periódico de servidores Y PC asociado a un proceso de gestión de vulnerabilidades, y otras medidas de seguridad que detalla

- Sobre: "*Comunicaciones realizadas a los afectados sobre la incidencia*."

Indica que dicha respuesta se contiene el escrito de denuncia. Añade que se trató de contactar telefónicamente con todos ellos para solicitarles como medida de seguridad cambiar sus palabras clave pues la palabra clave es el código que permite a los clientes no sólo realizar cualquier tipo de operación sobre sus propios sistemas de alarma por ejemplo activar o desactivar sino también sobre sus datos personales asociados a esta por ejemplo modificación de datos. Indica que de esa acción 21 llamadas fueron a personas físicas y 6 a jurídicas, produciéndose 21 cambios de palabras clave realizados por los clientes contactados 1 figura ilocalizable y 5 cambios de palabra clave no realizados por negativa del propio cliente.

- Sobre: "*Contratos que deban firmar todos los empleados que tengan acceso a datos personales*."

Adjunta copia de escrito en documento 2 qué es el modelo utilizado en la actualidad. Se titula normativa de seguridad y política de privacidad en SECURITAS Direct España, con unas diez páginas, la normativa de seguridad interna en sede central. Recoge normativa tanto de acceso al edificio como tarjetas seguridad de la información, confidencialidad o gestión de soportes. Lleva un pie de firma lo que significa que el firmante comprende y reconoce haber recibido

Manifiesta en el año 2009 se aprobó un código de conducta interno al que se sometían todos los empleados, qué incluye entre otras cuestiones, asuntos relacionados con Protección de Datos y seguridad de la información necesaria para concienciar a los empleados adjunta documento 3 .

Indica que en los contratos queda constancia con un código del comercial que utiliza que realiza la venta y que dos empleados vinculados al volumen de contratos que están en poder de Intersindical firmaron el documento citado en el año 2011 Adjuntan documentos como núm. 4 .

- Sobre: "*Contratos con terceros con acceso a datos (encargados de tratamiento*)"

indica que los contratos en papel se encuentran almacenados NORMADAT empresa que afecta este servicio y adjuntan documentos 5 de contrato Prestación de servicios a fecha 25/05/2018.

- Sobre: "*Comunicaciones con el cliente, o posible cliente, donde aparezcan datos personales tanto electrónicamente como en soporte físico (contratación, instalación, etc.*)."

Declara que ya ha sido contestada en algún punto anterior

2. Requerida información a INTERSINDICAL, con fecha 6/03/2019 manifiesta en un primer escrito: que la recepción de los contratos se produjo poco tiempo después de la emisión en

el programa de la cadena CUATRO “en el *punto de mira*” *sobre trabajadores y ex trabajadores de Securitas Direct que podrían estar colaborando con conocidos delincuentes de Madrid*”. Manifiesta que la documentación de Securitas ha estado circulando sin ningún tipo de control desde hace más de 20 años. Indicando el hecho de que se ha permitido a los comerciales hacer copia de los contratos de sus clientes. Manifiesta que “*cuando se han recibido en el sindicato de manera anónima más de un centenar de contratos de esta empresa firmados hace 20 años muchos de ellos originales contra sus copias es porque Securitas Direct no tiene ningún tipo de control sobre esta documentación e información*”. Manifiesta que de la denuncia que interpuso SECURITAS en el Juzgado de ******LOCALIDAD.1***, el Fiscal emitió informe de sobreseimiento provisional y aporta copia del mismo de 18/01/2019.

-Sobre las preguntas: “*Objeto de la denuncia presentada en los juzgados de* ******DIRECCIÓN.1*** *a la que se adjuntan los contratos mencionados en la denuncia. Copia de la misma*.” *y “Procedencia de los contratos depositados en los juzgados de* ******DIRECCIÓN.1***”

Indica en un segundo escrito de 6/03/2019 que “*ignoraron a que denuncia y que contratos se refieren”*. “Los únicos contratos q*ue se han recibido de 21/05/2018 de manera anónima ya fueron entregados en el decanato de los juzgados de instrucción y primera instancia de* ******LOCALIDAD.1*** *junto a una denuncia y ya facilitó la información sobre este asunto el juez instructor del juzgado 3 de* ******LOCALIDAD.1*** , y en la propia AEPD en julio 2018.

Adjunta nuevamente el escrito del fiscal de fecha 18/01/2019 en el que propone sobreseimiento dirigido al juzgado núm. 3 de ******LOCALIDAD.1***

4. Se efectúa búsqueda en la red social *Facebook*, y se encontró la publicación en el espacio de INTERSINDICAL, con fecha 22/04/2019, de tres imágenes de documentos denominados “*Plan de acción*”, probablemente de contratos de SD, pues figura el logo de esta, con datos personales de clientes, una imagen de un documento denominado “*Contrato de Instalación/Suscripción al Servicio de Atención Inmediata*” y una imagen que corresponde a un fragmento de un contrato con datos de tarjeta de crédito, cuenta bancaria y condiciones de pago. Todos los documentos están tachados, cubiertos por rectángulos blancos que posiblemente se han puesto, en los apartados que se refieren a datos personales o pueden relacionarse con los mismos, de forma que resulta imposible conocer tanto los datos personales, como los datos financieros como la cuenta bancaria.

CUARTO: Con fecha 6/06/2019 se acordó por la directora de la AEPD el archivo de actuaciones, expediente nº: E/09019/2018, por el vencimiento del plazo previsto legalmente para el desarrollo de las actuaciones previas “*sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador”,* artículo 122.4 del Reglamento de desarrollo de la LOPD (RLOPD), aprobado por Real Decreto 1720/2007, de 21/12.

Además, en el mismo acuerdo se decide iniciar nuevas actuaciones previas y se notifica a SINDICATO DE TRABAJADORES DE SEGURIDAD PRIVADA-INTERSINDICAL y a SECURITAS DIRECT ESPAÑA, S.A.

QUINTO: En el seno de las nuevas actuaciones previas de investigación E/5917/2019 se dio traslado de dicha reclamación a SINDICATO DE TRABAJADORES DE SEGURIDAD PRIVADA-INTERSINDICAL**, (** INTERSINDICAL) sobre: “*Estado de la denuncia presentada en los juzgados de* ******DIRECCIÓN.1*** *a la que se adjuntan los contratos mencionados en la denuncia, y en su caso, la sentencia que se haya dictado*.”

El resultado del envío telemático figura según el certificado:" Fecha de puesta a disposición: 22/07/2019 17:13:31, Fecha de rechazo automático: 02/08/2019 00:00:00

El envío se cursa también por correo y figura la recepción el 29/07/2019.

No se recibió respuesta, quedando concretados estos extremos en el informe de actuaciones previas.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

Los hechos sucedidos ocurren antes de 25/05/2018, y las medidas de seguridad para tener en cuenta se refieren también al momento previo de dicha fecha, que fue cuando entré en vigor la nueva normativa del RGPD, aplicándose entonces la LOPD cuyos aspectos fundamentales en cuanto a medidas de seguridad de datos personales en ficheros y tratamientos son similares a los del RGPD.

El artículo 9 de la LOPD indica: "*1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural*.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El citado artículo 9 de la LOPD establece el "*principio de seguridad de los datos*" imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos a título de ejemplo, entre otros de "*acceso no autorizado*" por parte de terceros. Así, aun cuando el artículo 9 de la LOPD establece una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en conocimiento de terceros, también es un mecanismo de garantía la seguridad

En el presente supuesto, la reclamante, SECURITAS DIRECT es la entidad que ostenta la

responsable del tratamiento de los datos que ella misma denuncia, la responsable de cumplir las medidas de seguridad del tratamiento.

La SAN 6-05-2009 Rec. 469/2008) entre otras, sobre supuestos similares ha establecido:

"*No basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados del banco la observancia de aquellas instrucciones. En el caso que nos ocupa ha quedado acreditado que la entidad ahora demandante no prestó la diligencia necesaria en orden a la efectiva observancia de aquellas medidas de seguridad, pues de otro modo no se explica que los documentos en los que figuran datos de carácter personal apareciesen publicados en una revista de amplia difusión en la que se afirmaba que habían sido encontrados en la basura*."

Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, la responsable del fichero es, por disposición legal, una deudora de seguridad en materia de datos, por lo que debe dar una explicación adecuada y razonable de cómo los datos personales han ido a parar a un lugar en el que son susceptibles de recuperación por terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues también es responsable de que las mismas se cumplan y se ejecuten con rigor. En definitiva, toda responsable de un fichero (o encargada de tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios, laborales o cualesquiera otros datos de carácter personal, puedan llegar a manos de terceras personas."

En primer lugar, no ha sido posible determinar ciertamente el sujeto responsable al que atribuir la infracción, pues no se ha determinado la naturaleza y procedencia de los documentos, esto es, si eran originales, que tipo de documentos eran, o si eran copias, y si además, dichos ejemplares correspondían en su caso a la copia que queda en poder del responsable del tratamiento, o si había otros ejemplares en poder de un encargado de tratamiento. Ello no permite establecer de forma indubitada el sujeto responsable de los documentos y los datos, o las personas que intervienen en el proceso de contratación con el fin de determinar responsabilidades.

Por otro lado, cuando la reclamada recibe la documentación con los datos personales, mayo 2018, no es posible determinar con certeza el momento en que se producen los hechos que cumplen el tipo previsto a sancionar del artículo 44.3.h) de la LOPD:"*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*." Este es el hecho que se tipifica y cuyo incumplimiento supondría la eventual ruptura de las medidas de seguridad, debiéndose conocer además del sujeto responsable, cuando se inicia o hasta cuando perdura esta falta de medidas de seguridad. En el presente supuesto, se desconocería cuando se inicia y si se mantiene o no la conducta del ilícito en su caso.

El hecho de que se pueda disponer de los documentos no es sino la exteriorización que podría revelar aquella infracción, pero se ha de acudir a la determinación del posible inicio o momento en que se consuma la ausencia de medidas que dan lugar a la supuesta

extracción documental y al sujeto al que cabe imputar la infracción.

Conectado con ello, Se caracteriza esta infracción por ser una infracción tipificada como grave en el artículo 44.3 h) de la LOPD, que prescribiría a los dos años de haberse cometido, artículo 47 LOPD, a contar desde la fecha en que se hubiera cometido (47.2 LOPD).

Para el computo de dicho periodo hay que acudir a la fecha o fechas en las que se produjera el fallo de seguridad que permitiera deducir la extracción de las copias de los contratos. En el presente supuesto se trata de contratos suscritos, los últimos de 2015. La denuncia se produce en 22/05/2018, y los contratos los recibió de forma anónima el sindicato en mayo 2018.

Siendo de aplicación al Derecho Administrativo Sancionador, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resulta clara la plena virtualidad del principio de presunción de inocencia en el presente supuesto. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del ius puniendi en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta "*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio*". De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en lo sucesivo LRJPAC), establece que "*Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia*."

En el presente supuesto, no ha sido posible acreditar la comisión de la infracción por parte de la responsable del tratamiento, SECURITAS DIRECT, ni la fecha de comisión de los hechos, por lo que se ha de archivar la reclamación.

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

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al reclamante y reclamado.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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