**Procedimiento Nº: A/00413/2017**

**RESOLUCIÓN: R/03500/2017**

En el procedimiento A/00413/2017, instruido por la Agencia Española de Protección de Datos a la entidad LEVI STRAUSS DE ESPAÑA, S.A, vista la denuncia presentada por Don ***A.A.A.*** y en virtud de los siguientes,

## ANTECEDENTES

**PRIMERO**: Con fecha 28 de junio de 2017 tiene entrada en esta Agencia una denuncia presentada por Don ***A.A.A.*** (en lo sucesivo, el denunciante), en la que manifiesta que, en las inmediaciones del Centro Comercial "Factory" de San Sebastián de los Reyes (Madrid), ha encontrado en un contenedor de obra una bolsa que contiene currículos vitae.

Aporta la bolsa con la documentación encontrada que consiste en alrededor de 200 CV y algún otro documento identificado con el logotipo de Levi's.

**SEGUNDO**: Tras la recepción de la denuncia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados (Informe E/04263/2017), teniendo conocimiento de los siguientes extremos:

1. Con fecha 17 de julio de 2017 se mantiene una conversación telefónica con la tienda de Levi's situada en el Centro Comercial "Factory" de San Sebastián de los Reyes (Madrid), con objeto de determinar la empresa responsable de la misma, en la conversación mantenida se informa de que la tienda pertenece a LEVI STRAUSS DE ESPAÑA, S.A. Esta información se confirma por la empresa en la llamada telefónica realizada con fecha 25 de julio de 2017.

2. Con fechas 9 y 19 de octubre de 2017, LEVI STRAUSS DE ESPAÑA, S.A. ha remitido a esta Agencia la siguiente información en relación con los hechos denunciados:

    a. La empresa tiene establecido que la información confidencial como los CVs no tiene que ser desechada sin ser previamente destruida. En particular, no está permitido depositarla en las bolsas de basura de las tiendas.

    b. Según el citado procedimiento, en caso de que la tienda no disponga de destructora de papel, debe remitir la documentación a los servicios centrales mediante el servicio de mensajería semanal o valija interna existente para el intercambio de información entre las tiendas y la oficina central.
    c. Aportan copia del apartado del Documento de Seguridad de la

empresa titulado “GESTION DE SOPORTES Y DOCUMENTOS” donde consta que:

i. *“Cualquier soporte que vaya a ser desechado, de cualquier tipo, que puede contener datos de carácter personal, ya sea papel impreso, soportes magnéticos, ópticos y otros, o los propios ordenadores obsoletos que vayan a desecharse, deberán ser tratados mediante los procedimientos de destrucción y reutilización de soportes informáticos y destrucción de documentación*.”.

ii. Así mismo, en el punto “DESTRUCCION DE DOCUMENTACIÓN”, se especifica que: “*Ningún documento deber ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información*”.

d. Los trabajadores son informados del citado procedimiento en los cursos de formación que reciben regularmente los encargados de tienda. Aportan, a modo de ejemplo, el documento correspondiente a la formación realizada en marzo de 2017, donde consta un apartado de “Protección de Datos- Gestión de datos por parte del store manager en tienda”, donde se indica que:

i. “*todos los curriculums recibidos en tienda a través de candidatos espontáneos es responsabilidad del store manager gestionarlos de forma adecuada haciendo un uso responsable de los datos y toda la información contenida en los mismos. Todos los curriculums deberán ser enviados al departamento de Recursos Humanos de forma regular a través de valija para su posterior custodia y almacenamiento en el departamento de recursos humanos*”.

e. Además, continuamente existe comunicación entre el personal de las tiendas y las oficinas centrales, por las más diversas cuestiones. Desde la oficina central siempre se trasmite a las tiendas el mensaje de aplicar el mencionado procedimiento. A este respecto aportan copia de un correo electrónico recibido de la encargada de una de las tiendas donde solicita instrucciones para el desecho de dos cajas con CVs y de la contestación al mismo en el que se le indica que si no tiene medios para destruirlos en la tienda los remita a la central por valija para su destrucción.

f. Así mismo, aportan un correo electrónico remitido desde la central a varias encargadas de tiendas, con fecha 27 de julio de 2017, en el que se indica que ha habido un problema con una tienda y se les recuerda que todos los CVs que les dejan son información confidencial, y por esta razón no pueden ser tirados nunca a la basura. O los mandan a la oficina o los destruyen con una destructora de papel o algún proveedor especializado.

g. Por último aportan copia de las cláusulas anexas a los contratos de trabajo que firman los trabajadores en relación a la Protección de Datos.

h. Respecto a la incidencia de los hechos objeto de la denuncia aportan copia del registro de incidencias, donde consta la misma con fecha 26 de julio de 2017, comunicada por la Directora de Recursos Humanos, que tiene conocimiento de los hechos por la llamada realizada desde esta Agencia. Se acuerda que la encargada de la tienda se ponga en contacto con la empresa de limpieza de la tienda afectada para recordar que sus trabajadores deben seguir las instrucciones del personal de la tienda y enviar un correo electrónico a los encargados de tiendas, para recordarles cómo tienen que tratar la información confidencial en papel. Según manifiestan, es la primera vez que se produce una incidencia de este tipo.

i. Con fecha 19 de octubre de 2017, la empresa informa de que tiene contratado el servicio de limpieza de las tiendas con la empresa SERVICIOS INTEGRALES DE FINCAS URBANAS DE MADRID, S.L. Aportan copia del contrato de fecha 1 de marzo de 2016 y del anexo de confidencialidad al mismo firmado con fecha 6 de octubre de 2107, en el que, entre otros extremos, la empresa de limpieza se compromete a dar cumplimiento a las instrucciones de LEVI STRAUSS DE ESPAÑA, S.A., como la prohibición expresa de desechar cualquier documento que contenga datos de carácter personal a los contenedores ubicados en la vía pública, debiendo depositar dicha documentación en los espacios habilitados por la propia empresa para su posterior destrucción mediante destructoras de papel.

j. Según manifiestan, el personal de la citada empresa de limpieza se caracteriza por ser personas con discapacidad con riesgo de exclusión social y, según las actuaciones realizadas por la empresa para determinar lo que dio lugar a la incidencia objeto de la denuncia, deducen que fue el trabajador de la empresa de limpieza el responsable de que los CVs se depositaran en un contenedor de la vía pública, ya que en ocasiones anteriores había desechado objetos personales de los trabajadores de la tienda, pese a haber recibido instrucciones de no desechar nada que expresamente no se le indicara.

**TERCERO**: Consultada la aplicación de la AEPD que gestiona la consulta de antecedentes de sanciones y apercibimientos precedentes, a la denunciada, LEVI STRAUSS DE ESPAÑA, S.A., no le constan registros previos.

**CUARTO**: Con fecha 24 de noviembre de 2017, la Directora de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente

procedimiento de apercibimiento A/00413/2017. Dicho acuerdo fue notificado a la entidad denunciada.

**QUINTO**: Con fecha 19 de diciembre de 2017 se recibe en esta Agencia escrito de la entidad denunciada en el que comunica que, como ya informó, el procedimiento que tiene establecido para desechar información confidencial, tal como CVs, consta en su Documento de Seguridad, y consiste en su eliminación mediante destructoras de papel, si la tienda dispone de ella, o remisión a las oficinas centrales mediante el servicio de mensajería o valija interna para su destrucción en la trituradora. Manifiesta de nuevo que este procedimiento se comunica regularmente a los trabajadores y que a raíz de este caso se ha realizado un nuevo recordatorio. Así mismo, comunica que, como ya puso de manifiesto, el servicio de limpieza de sus tiendas corre a cargo de una tercera empresa, SERVICIOS INTEGRALES DE FINCAS URBANAS DE MADRID, S.L., habiéndose suscrito un anexo al contrato con la misma para incluir expresamente la instrucción de no depositar en los contenedores de la vía pública documentación confidencial.

## HECHOS PROBADOS

**PRIMERO**: Don ***A.A.A.***presenta una denuncia en esta Agencia en la que manifiesta que, en las inmediaciones del Centro Comercial "Factory" de San Sebastián de los Reyes (Madrid), ha encontrado en un contenedor de obra una bolsa que contiene currículos vitae.

Aporta la bolsa con la documentación encontrada que consiste en alrededor de 200 CV y algún otro documento identificado con el logotipo de Levi's.

**SEGUNDO**: La tienda de Levi's situada en el citado centro comercial pertenece a LEVI STRAUSS DE ESPAÑA, S.A.

**TERCERO**: En el Documento de Seguridad de la entidad denunciada se incluye un apartado titulado "GESTIÓN DE SOPORTES Y DOCUMENTOS" donde consta que:

i. *"Cualquier soporte que vaya a ser desechado, de cualquier tipo, que puede contener datos de carácter personal, ya sea papel impreso, soportes magnéticos, ópticos y otros, o los propios ordenadores obsoletos que vayan a desecharse, deberán ser tratados mediante los procedimientos de destrucción y reutilización de soportes informáticos y destrucción de documentación*.".

ii. Así mismo, en el punto "DESTRUCCION DE DOCUMENTACIÓN", se especifica que: "*Ningún documento deber ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información*".

**CUARTO**: Los trabajadores de la entidad denunciada son informados del procedimiento de destrucción de documentación con datos de carácter personal en los cursos de formación que reciben regularmente los encargados de tienda.

**QUINTO**: A raíz del presente procedimiento se ha realizado un nuevo recordatorio específico a los encargados de las tiendas en relación con el procedimiento de destrucción de documentación con datos de carácter personal.

**SEXTO**: Con fecha 6 de octubre de 2107, la entidad denunciada firma anexo al contrato suscrito con la empresa que le presta el servicio de limpieza en tiendas, incluyéndose expresamente la instrucción de no depositar en los contenedores de la vía pública documentación confidencial.

## FUNDAMENTOS DE DERECHO

### I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en lo sucesivo LOPD).

### II

El artículo 9 de la LOPD, dispone:

*"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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 o 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 art. 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 aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.
b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.
c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.
d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Es necesario analizar las previsiones que el R. D. 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, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento define en su artículo 5.2 ñ) el *"Soporte"* como el "*objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*".

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma.

El Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

Entre las medidas de seguridad de nivel básico, el Reglamento expone en su artículo 92, respecto de la gestión de soportes y documentos, que:

*"1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.*
*Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.*
*2. La salida de soportes y documentos que contengan datos de carácter personal,*

*incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.*
*3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.*
*4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.*
*5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."*

LEVI STRAUSS DE ESPAÑA, S.A., debió, por ello, adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información que contenían los documentos encontrados. Tales medidas no fueron adoptadas totalmente en el presente caso. Prueba de ello es el hecho de que la documentación fue encontrada por el denunciante en las inmediaciones del Centro Comercial "Factory" de San Sebastián de los Reyes (Madrid).

En el presente caso, y teniendo en cuenta la documentación encontrada por el denunciante, ha quedado acreditado que LEVI STRAUSS DE ESPAÑA, S.A., no adoptó las medidas de índole técnica y organizativas necesarias que garantizasen la seguridad de los datos de carácter personal de sus ficheros, de manera que se evitase el acceso no autorizado a los datos de los mismos.

**III**

El artículo 44.3.h) de la LOPD, considera infracción grave:

*"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."*

Dado que ha existido una vulneración en las medidas de seguridad por parte de LEVI STRAUSS DE ESPAÑA, S.A., se considera que ha incurrido en la infracción grave descrita.

**IV**

El artículo 10 de la LOPD establece que*: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos,*

*obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

En este sentido, la Audiencia Nacional recoge en numerosas Sentencias lo siguiente: "*El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.*

*Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"*

En el caso que nos ocupa, LEVI STRAUSS DE ESPAÑA, S.A., es responsable del fichero en el que constan los datos de carácter personal, así como de la custodia de la documentación relativa a los mismos y que apareció en un contenedor de obra. Se comprueba por tanto la existencia de un incumplimiento del deber de secreto, produciéndose una ausencia de confidencialidad por el acceso a datos de carácter personal por parte de un tercero no autorizado, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

**V**

El artículo 44.3.d) de la LOPD, califica como infracción grave:

*"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley."*

De acuerdo con los fundamentos anteriores, entendemos que por parte LEVI STRAUSS DE ESPAÑA, S.A., se ha producido una vulneración del deber de secreto que procede calificar como infracción grave.

**VI**

En el presente caso ha quedado acreditado que LEVI STRAUSS DE ESPAÑA, S.A., no custodió debidamente documentación que estaba en sus instalaciones, que fue abandonada en la vía pública conteniendo datos de carácter personal. Estos hechos suponen una vulneración de las medidas de seguridad así como del deber de guardar secreto por lo que la entidad denunciada ha incurrido en las infracciones graves descritas.

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) ha añadido un nuevo apartado 6 al artículo 45 de la Ley 15/1999 de Protección de Datos en lugar del existente hasta su promulgación del siguiente tenor:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

*a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*
*b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

*Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento*".

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que las infracciones de la LOPD de la que se responsabiliza a la entidad denunciada son infracciones "graves"; que la entidad denunciada no ha sido sancionada o apercibida por este organismo en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD: el carácter puntual de la infracción, el hecho de que la denunciada no tenga como actividad principal el tratamiento de datos, la ausencia de beneficios derivados de la comisión de la infracción y el grado de intencionalidad apreciado. Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella y cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando no se requieran medidas correctoras, lo procedente en Derecho es acordar el archivo de las actuaciones.

En este caso concreto, atendida la naturaleza de la infracción consistente en un hecho puntual, y vistas las medidas ya adoptadas por el responsable de la misma, debe procederse en consecuencia, a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, en aplicación de la interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica. Recordando que la reiteración en conductas como la denunciada constituye un supuesto sobre el que concurren las circunstancias previstas para la aplicación del régimen sancionador contemplado en la LOPD.

A la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) de acuerdo con lo señalado se debe proceder al archivo de las actuaciones.

De acuerdo con lo señalado,

**Por la Directora de la Agencia Española de Protección de Datos,**

**SE ACUERDA:**

**1.- ARCHIVAR** (**A/00413/2017**) las actuaciones practicadas a LEVI STRAUSS DE ESPAÑA, S.A., con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por infracción de los artículos 9.1 y 10 de la LOPD, tipificadas como graves en los artículos 44.3.h) y 44.3.d).

**2.- NOTIFICAR** el presente Acuerdo a LEVI STRAUSS DE ESPAÑA, S.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 esta 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