A/00020/2015

RESOLUCIÓN: R/01722/2015

En el procedimiento A/00020/2015, instruido por la Agencia Española de Protección de Datos a la entidad ***KIWITEL SL***, vista la denuncia presentada por ***GENERALITAT DE CATALUNYA*** y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 11/2/14 tiene entrada en esta Agencia un escrito de la Agencia Catalana de Protección de Datos (APDCAT) dando traslado de una serie de diligencias de los Mossos D'Esquadra de la Generalitat de Catalunya. En las diligencias, cuya copia aportan, se pone de manifiesto el hallazgo de una serie de documentación con datos de diferentes personas en un contenedor de papel ubicado en la vía pública, calle ***(C/.....1) de Sabadell***.

Según figura en las diligencias policiales la persona que realizó el hallazgo indicó haber llamado a alguna de las personas cuyos datos aparecían, para avisarles. Consta que alguna de las personas avisadas han presentado declaración ante la Instrucción de los Mossos D'Esquadra. Se cita que entre los datos expuestos se encuentran números de cuentas corrientes y copias de DNI's.

En la diligencia de fecha 03/02/2014, consta lo siguiente (traducción del catalán aportada por la APDCAT):

"*Primero.-*
En el lugar en el que se han encontrado los documentos, calle ***(C/.....1)*** *de la localidad de Sabadell, se encuentran muy próximos dos establecimientos ORANGE, uno en el núm. 30 y otro en el núm. 170, ambos de la* ***(C/.....2)****.*
Teniendo en cuenta el hecho de que en alguna de las copias de contratos encontrados, aparece con la dirección del establecimiento de ORANGE, la Rambla núm. 170 de la localidad de Sabadell y atendiendo a la declaración de algunos clientes, que han manifestado que formalizaron su contrato en el mencionado establecimiento, se ha dirigido como indicativo policial para contactar con el responsable.

Segundo. -
*Una vez en el lugar, el indicativo policial compuesto por los agentes con TIP ****1 y TIP ****2, han contactado con la responsable, que ha acreditado ser* ***A.A.A.*** *nacida el día […].*
Preguntada sobre los hechos, la Sra. ***A.A.A.*** *ha manifestado a los agentes que era posible que los documentos hallados se hubieran mezclado, por error, con otros pendientes de destruir y hubieran acabado en el contenedor de papel.*

Tercero. -
Atendiendo a las circunstancias, se ha citado a la Sra. ***A.A.A.*** *para declarar ante esta instrucción en calidad de testimonio, de manera que pudiera esclarecer el motivo por el cual los documentos han acabado en el contenedor de papel próximo a su establecimiento. "*

En el acta de declaración de ***A.A.A.*** de fecha 04/02/2014 consta lo siguiente:

*"Que la señora **A.A.A.** es la encargada de la tienda ORANGE, de la (C/.....2) 170, de Sabadell.*
*Que la señora **A.A.A.** manifiesta que en la tienda tienen dos (2) contenedores de papel, uno (1) de ellos destinado a papel para reciclar y (1) otro destinado a papeles que han de pasar por la trituradora.*
Que con respecto a la documentación que se ha encontrado manifiesta que ha habido de haber algún error con respecto a qué contenedor iban los papeles.
Que alguien ha puesto la documentación que debía pasar por la trituradora en el contenedor de papel para reciclar.
*Que esta instrucción informa a la señora **A.A.A.** de que quedará denunciada por vía administrativa por incumplimiento de la Ley de Protección de Datos.*
*Que esta instrucción hace entrega a la señora **A.A.A.** de toda la documentación encontrada a fin de que proceda a su destrucción."*

También aportan copia de las actas de declaración ante los Mossos D'Esquadra de la persona que efectuó el hallazgo así como de una de las personas afectadas que fue avisada.

SEGUNDO; Por parte del Subdirector General de Inspección de Datos, en base al contenido de la denuncia, se procedió a la apertura de actuaciones previas con referencia E/026592014 y concluye la investigación con el informe siguiente de la Inspección de Datos:

<<<<< Solicitada información y documentación a KIWITEL, SL sus representantes han manifestado lo siguiente:

*"1.- El Motivo por el cual se encontró documentación de Kiwitel dentro de un contenedor cercano a la tienda que esta empresa tiene abierta al público en la (C/.....2), queda descrito en el Acta de Declaración de 4 de Febrero de 2.014, prestada por la empleada Dña. **A.A.A.,** en su condición de responsable de la referida tienda. De hecho, y siendo por ello la encargadas de la gestión de la documentación confidencial de clientes, el que fuera encontrada esa documentación en un contenedor que había en la calle, es únicamente debido a que la trabajadora desatendió o descuidó los estrictos protocolos que Kiwitel tiene establecidos en esta materia.*

2.- Kiwitel custodia escrupulosamente los datos personales de los clientes, empezando por la tienda en la que se realiza la operación, la cual tiene la obligación de GUARDAR PERMANENTEMENTE en su almacén cualquier documento que contenga este tipo de datos. No hay distinción entre clientes que realizan alguna activación con la compañía o clientes que finalmente deciden no seguir adelante con la gestión, y que en muchos casos no vuelven a recoger la documentación entregada.

En el supuesto de que el almacén de dicha tienda tenga un problema de espacio, se hacen recogidas periódicas donde se trasladan los documentos al fichero general de la empresa, situado en (C/.....3).

Adjuntamos, como documento n° 1, fotografía del almacén de la tienda de Sabadell donde se guarda la documentación confidencial, y como documento nº 2, fotografía del

almacén de la (C/.....3).

3.- El proceso de destrucción de documentación empieza también por los puntos de venta, cada uno de ellos dispone de una máquina de destrucción de documentación, si bien es importante matizar que dichas maquinas solo se usan puntualmente, toda vez que la premisa de la empresa es archivarlo todo y pilotar toda destrucción de documentación desde la central.

Llegado el momento de poder destruir documentación con más de 5 años de antigüedad, ya sea desde el punto de venta o desde el archivador central, Kiwitel utiliza los servicios de su proveedor habitual, ARA VINC, S.L., empresa que dispone del certificado de garantía de destrucción de documentación.

Acompañamos, como documento n° 3, fotografía de la destructora de documentación de que dispone la empresa en la tienda de Sabadell, y que es igual a la que hay en cada una de los puntos de venta de Kiwitel.

Acompañamos, como documentos n° 4 a 13, facturas acreditativas de la compra de las máquinas destructoras para las diferentes tiendas.

Acompañamos, asimismo, como documento n° 14, relación de facturas abonadas a la empresa ARA VINC, S.L., para la recogida y destrucción de documentación. Acompañamos, asimismo, documentos nº 15 a 20, algunas de las facturas relacionadas con los certificados de destrucción. Del resto de facturas, se ha solicitado copia al proveedor, toda vez que no han sido localizadas por el departamento de contabilidad de Kiwitel y serán aportadas tan pronto como se disponga de las mismas.

4.- En cuanto a los contenedores de recogida, las funciones las realiza el almacén de la tienda donde se guardan las carpetas con todas la documentación correspondiente, tal y como se muestra en las fotografías aportadas como documentos n° 1 y 2 de este escrito, a la espera de que sean trasladadas por problemas de espacio a nuestro archivador central.

5.- El personal que tiene acceso a este tipo de documentos son los responsables de tienda y los asesores que trabajan en ellas, por ese motivo Kiwitel advierte de la importancia del trato de la documentación y se les hace responsables a la misma firma del contrato

A los efectos de acreditar lo anterior, se adjunta, como documento n° 21, copia del documento firmado por la trabajadora Sra. ***A.A.A.*** *acerca del Manual de Gestión de Seguridad de la Información.*

7.- Adjuntamos copia de la normativa interna y de la distinta documentación existente al respecto:

Doc. 22 - Manuel de Gestión de Seguridad de la Información (Documento de Seguridad de Datos).
Doc. 23 - Anexos al Documento de Seguridad de Datos.
Doc. 24 - Anexos y Soportes al Documento de Seguridad de Datos. Doc. 25 - Libro de Incidencias.

Doc. 26 - Plan de Acogida
Doc. 27 - Derechos del Afectado (ARCO). Doc. 28 - Encargado de Tratamiento.
Doc. 29 - Videovigilancia y Tablón de Anuncios. Doc. 30 - Auditoria y Certificación.*
Doc. 31 - Documento de Seguridad de Datos de la tienda de Sabadell (aportamos únicamente el de la tienda donde se produjo la incidencia, toda vez que es idéntico al del resto de tiendas, en aras a evitar aportar documentación innecesaria, y sin perjuicio de que la Agencia considere oportuna su aportación).

8.- Aportamos, como documento n° 32, hoja del registro de incidencias donde aparece el hecho del que trae causa este expediente, y como documento n° 33, copia de la carta de amonestación-sanción entregada a la trabajadora el 2 de Julio de 2.014.

El hecho no fue registrado ni sancionado hasta fecha, que es cuando se recibió al presente requerimiento, habida cuenta de que la trabajadora no informó en su día del incidente.

9.- Tal y como se solicita, adjuntamos, como documento n° 34, copia del último contrato de distribución firmado entre KIWITEL, S.L., Y FRANCE TELECOM ESPAÑA (ORANGE).

10.- A parte de la documentación requerida, aportamos, como documentos n°35 a 52, notificaciones a la Agencia de los distintos ficheros de titularidad privada, gestionados en Abril de 2.011.

11.- Por último, aportamos, como documento n° 53, extracto de la Vida Laboral de Empresa de Kiwitel, S.L. (VILE), al objeto de dejar constancia de la extensa plantilla de esta empresa. Con ello queremos evidenciar que, a pesar de la mayor dificultad que entraña en una empresa con tal flujo de personal (numerosas altas y bajas) poder llevar un adecuado control de la seguridad de los datos confidenciales de clientes, trabajadores, proveedores, etc., es la primera incidencia en esta materia que afecta a mi representada, lo cual entendemos que evidencia su buena gestión en todo lo relacionado con el tratamiento de datos, siendo completamente inevitable que, en un momento dado, una trabajadora traspapele cierta documentación, inaplicando el protocolo impuesto por la empresa."

Se hace notar que el MANUAL DE GESTIÓN DESEGURIDAD DE LA INFORMACIÓN (documento numerado como nº 21), contiene un TEST DE CONOCIMIENTOS PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL en el cual ***A.A.A.*** contestó correctamente (opción 2) a la siguiente pregunta:

"09 Que quiere decir destruir convenientemente los soportes que contienen datos de carácter personal.

1. Romper con la mano, en 3 trozos el papel, tirarlo a la papelera y responsabilizar a la Sra. de la limpieza que lo tire al contenedor.
2. Utilizar la destructora de papel o certificar su destrucción."
Así mismo, en el documento aportado como nº 26 (PLAN DE ACOGIDA. DOCUMENTO DE SEGURIDAD DE DATOS, se especifica, en "FORMACION LOPD" "(para el empleado)" lo siguiente:
"ARCHIVO, CUSTODIA Y ALMACENAMIENTO DE LA INFORMACIÓN.

Los armarios, archivadores u otros elementos donde se almacenen los ficheros no automatizados con datos de carácter personal tendrán que encontrarse en áreas en que el acceso esté protegido con puertas de acceso dotadas de sistemas de abertura mediante llave u otro dispositivo equivalente.

Las áreas tendrán que permanecer cerradas cuando no sea necesario el acceso a los documentos incluidos en el fichero.

Mientras la documentación con datos de carácter personal no se encuentre archivada, la persona que se encuentre el cargo de la misma, la deberá custodiar e impedir en todo momento que pueda ser accedida por persona no autorizada.

En el documento aportado como nº 26 (PLAN DE ACOGIDA. DOCUMENTO DE SEGURIDAD DE DATOS, se especifica, en "NORMAS TIC" "(para el empleado)" lo siguiente:

7. DOCUMENTOS.
Se tendrán que garantizar la seguridad y correcta conservación, localización y consulta de los documentos.
1. Los armarios, archivadores u otros elementos donde se almacenen los ficheros con datos de carácter personal tendrán que encontrarse en áreas en las que el acceso esté protegido con puertas.
2. Siempre poner en lugar seguro los documentos con información confidencial o trascendental.
3. Evitar, en los puestos de trabajo, que los datos de carácter personal sean vistos por personas no autorizadas.
4. La generación de copias o la reproducción de los documentos se hará con seguridad. No dejar documentos en impresoras compartidas, debiendo recogerse de inmediato conforme van saliendo impresos.
5. No desechar soportes, ya sean magnéticos, ópticos o papel (facturas, albaranes, pedido, etc.) con datos de carácter personal, sin su total destrucción previa.
*6. No tire a la basura, papeles que alguien pueda leer y utilizar**."***

TERCERO: Con fecha 9/2/15, el Director de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00020/2015. Dicho acuerdo fue notificado a los denunciantes y al denunciado.

CUARTO: Con fecha 10/3/15 se recibe en esta Agencia escrito del denunciado en el que comunica lo siguiente:

* Que tienen implementados unos protocolos de actuación que garantizan el máximo celo en el tratamiento de los ficheros con datos personales de los clientes

* Que el hecho de encontrarse documentación con datos personales de los clientes en un contenedor se debe a que una trabajadora desatendió o descuidó los protocolos (tal como ha reconocido la misma). Dicha trabajadora había recibido la formación oportuna en materia de protección de datos lo que evidencia que se debió a un error humano.

* Que a tenor de lo establecido en el art. 45.6 ha adoptado la siguiente medida correctora: emitir una circular dirigida a todos los puntos de venta donde se informa del incidente ocurrido, y se hace especial hincapié en la importancia de repasar y tener muy presente los protocolos de actuaciones entregados por la empresa y firmados pòr cada uno de los trabajadores autorizados para su tratamiento.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director 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 LOPD.

II

El art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"*Seguridad de los datos:*
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD en su artículo 1 dispone que "*la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

El artículo 2.1 de la misma ley orgánica establece: "*1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".*

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento
…...
g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento
……
I) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

La vigente LOPD atribuye la condición de responsables de las infracciones a los responsables de los ficheros (art. 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d), arriba citado, que incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. En el presente caso, KIWITEL S.L.. es responsable de los ficheros y tratamientos, derivados de su actividad laboral, y en conformidad con las definiciones legales está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

III

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 la 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."

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

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.

La documentación encontrada procedente de esa entidad entra en la consideración de documentación en soporte papel, contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros. Debe tenerse en cuenta lo establecido tanto en el artículo 106 del RD 1720/07 de desarrollo de la LOPD que establece:

"Artículo 106. Criterios de archivo.
El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo. "

Y el art 92.2,3 y 4, (de aplicación a los ficheros no automatizados en virtud de lo establecido en el artículo 105), que disponen:

"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."

Se impone en este articulo la obligación de adoptar medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado, que incluye la atención a los protocolos que al respecto se deban aplicar cuando el traslado tenga como finalidad el desecho o destrucción de la documentación. Por lo tanto deberían de haberse adaptado, por parte de la entidad denunciada, las medidas suficientes que el acceso a la

información contenida en los mismos, así como su posible recuperación posterior.

IV

De los hechos probados en este procedimiento, se deduce que KIWITEL S.L.. en su calidad de responsable del tratamiento, debió adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información de carácter personal que contenían dichos documentos. Tales medidas no fueron adoptadas totalmente en el presente caso, como lo acredita el hecho que dicha documentación fuese recuperada por la policía en un contenedor de papel ubicado en la via pública. Esta necesidad de especial diligencia en la custodia de la documentación por el encargado del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor.*

Se alega por parte de la denunciada que la causa que dicha documentación se recuperase en la vía pública se debe a que la persona encargada de su custodia no ha cumplido con sus obligaciones, establecidas por la empresa y que le obligaban a actuar con diligencia respecto al tratamiento de datos de carácter personal

V

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad denunciada establece la base de facto para fundamentar la imputación de la infraccion del artículos 9 de la LOPD.

En supuesto presente, del examen de las medidas adoptadas por KIWITEL que han descritas en el hecho segundo, y que a raíz de los hechos se han adoptado medidas correctoras formuladas en el hecho cuarto, debe deducirse que las mismas deben considerarse suficientes para garantizar que en futuro no se repitan situaciones como la que dio lugar a la apertura del presente expediente, valorándose además que se trata de un hecho puntual, acaecido por la falta de diligencia de un empleado por lo que procede el archivo del presente expediente de apercibimiento.

En este sentido, conviene traer a colación lo señalado por la Sentencia de la Audiencia Nacional de 29-11-2013, de acuerdo con cuyo Fundamento Jurídico SEXTO, los procedimientos de apercibimiento que finalizan sin requerimiento se deben resolver como archivo, debiendo estimarse adoptada ya la medida correctora pertinente en el caso por lo que debe procederse a resolver el **archivo de las actuaciones**, sin practicar apercibimiento o requerimiento alguno al denunciado, en aplicación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a **KIWITEL S.L**. y a **Generalitat de Catalunya (Direccio General de la Policia).**

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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 lo sucesivo LJCA), 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos