Procedimiento Nº: A/00079/2017

RESOLUCIÓN: R/01166/2017

En el procedimiento A/00079/2017, instruido por la Agencia Española de Protección de Datos a la entidad RESIDENCIA DE LA ASUNCIÓN, S.L., vista la denuncia presentada por la POLICÍA LOCAL DEL AYUNTAMIENTO DE NAVALCARNERO, y en virtud de los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 6 de julio de 2016, tiene entrada en esta Agencia un escrito remitido por la Policía Local del Ayuntamiento de Navalcarnero en el que expone que, el día 12 de junio de 2016, ha encontrado, junto a los cubos de basura de la (C/...1), una caja de cartón con documentación de carácter sanitario; en concreto, se encuentran varios informes médicos y datos confidenciales sobre residentes con el membrete de la Residencia XXXX.

Se remiten a esta Agencia una muestra de los documentos encontrados.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se tiene conocimiento de los siguientes extremos:

Con fecha 10 de enero de 2017, se persona en esta Agencia Dña. ***A.A.A.***, Directora del Hospital CASA VERDE, con denominación social Residencia de la Asunción, S.L., la cual manifiesta que:

a. Con fecha 18 de marzo de 2016, se realizó una solicitud a la Consejería de Políticas Sociales y Familia, para el cierre del Centro XXXX, para su reconversión en Hospital de Media y Larga estancia, la cual se hizo efectiva con fecha 4 de mayo de 2016, denominado RESIDENCIA DE LA ASUNCION, S.L. (HOSPITAL CASA VERDE)

b. Para proceder al cese de la actividad se siguió un protocolo de actuación cuya memoria se adjunta a estas actuaciones de investigación, con el que se adjuntó un listado de pacientes que quedaban como pacientes del nuevo Centro y los que fueron trasladados.

c. Se procede a cotejar los datos de los pacientes que quedaron en el nuevo Centro, con los de la documentación encontrada en la vía pública por la Policía Local, comprobando que nueve de los documentos encontrados pertenecen a personas que han estado en el Centro, aunque en la actualidad solo queda uno.

d. Con fecha de febrero de 2016 se realizó una auditoria sobre la cual Hospital Casa Verde ha elaborado un Documento de Seguridad subsanando las deficiencias

existentes cuando se realizó, y se procedió a la elaboración de una guía para el personal que trabaja en el Hospital.

e. Con relación a la documentación existente en los locales donde se encuentra el Hospital actualmente y que correspondía al Centro XXXX, pudo ocurrir que los trabajadores que pertenecían a dicho Centro, que en la actualidad no queda ninguno, procedieran a tirar la documentación de los enfermos, que consideraran que ya no era actual".

TERCERO: Con fecha 14 de marzo 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/00079/2017. Dicho acuerdo fue notificado al denunciado.

CUARTO: Con fecha 11 de abril de 2017, se recibe en esta Agencia escrito del denunciado en el que alegan que como ya informaron, esa sociedad se hizo cargo de la Residencia el 18 de marzo de 2016. Como consecuencia de ello, algunos pacientes se quedaron en el Centro y otros fueron derivados a otros Centros residenciales. La explicación que encuentran a que se encontrasen algunos documentos con informes médicos de residentes de la Residencia XXXX, es que antiguos trabajadores los tiraran pensando que no eran actuales ni necesarios. Añaden que se trató de un hecho puntual; no existe ningún expediente anterior; no existe intencionalidad; lo más probable es que la actuación la realizasen trabajadores de la Residencia desaparecida; que se trataba de muy pocos documentos; y que no se han producido perjuicios. Por último, han elaborado un documento de Buenas Prácticas y de cumplimiento de medidas de seguridad.

HECHOS PROBADOS

PRIMERO: El día 12 de junio de 2016, la Policía Local del Ayuntamiento de Navalcarnero encontró, junto a los cubos de basura de la (C/...1), una caja de cartón con documentación de carácter sanitario; en concreto, se encuentran varios informes médicos y datos confidenciales sobre residentes con el membrete de la Residencia XXXX.

SEGUNDO: La caja contenía documentos con datos personales pertenecientes a los residentes de la Residencia XXXX, ya que tenían el membrete de la misma, y se encontraban al alcance de cualquier persona en la vía pública.

TERCERO: Se comprobó que los documentos pertenecían a personas que habían estado en la Residencia XXXX.

CUARTO: La Residencia XXXX fue adquirida por la entidad Residencia La Asunción, S.L., en fecha 18 de marzo de 2016.

QUINTO: Residencia La Asunción, S.L., realizó una auditoria antes de la adquisición de la Residencia XXXX; elaborando un Documento de Seguridad que subsanaba las deficiencias existentes, y ha elaborado de una guía para el personal que trabaja en el Hospital

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."

Residencia La Asunción, S.L., 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 la Policía Local de en la vía pública muy próximo a sus instalaciones.

En el presente caso y teniendo en cuenta la documentación encontrada por la policía denunciante, ha quedado acreditado que Residencia La Asunción, S.L., 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 Residencia La Asunción, S.L., 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.

En el caso que nos ocupa, Residencia La Asunción, S.L., es responsable del fichero en el que constan los datos personales, así como de la custodia de la documentación relativa a los mismos y que apareció en la ya referida acera de la vía pública. Atendiendo a las medidas de seguridad adoptadas por el denunciado, se comprueba la existencia de un incumplimiento del deber de secreto, produciéndose una ausencia de confidencialidad, 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 muy 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 de Residencia La Asunción, S.L., se ha producido una vulneración del deber de secreto que procede calificar como infracción grave.

VI

En el presente caso ha quedado acreditado que Residencia La Asunción, S.L., 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 el denunciado ha incurrido en las infracciones graves descritas.

El artículo 45.6 de la LOPD, dispone:

"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 la infracción de la LOPD de la que se responsabiliza al denunciado es una infracción "grave"; que el denunciado no ha sido sancionado o apercibido 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. 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 denunciado, debe procederse en consecuencia, a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno al denunciado, 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/00079/2017**) las actuaciones practicadas a Residencia La Asunción, S.L., 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) de la citada Ley Orgánica.

2.- NOTIFICAR el presente Acuerdo a Residencia La Asunción, S.L.

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