



Expediente Nº: E/03228/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

Examinado el escrito presentado por COPIFAX, S.L., relativo a la ejecución del requerimiento de la resolución de referencia R/01310/2015 dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento de apercibimiento A/00046/2015, seguido en su contra, y en virtud de los siguientes

ANTECEDENTES DE HECHO

PRIMERO: En esta Agencia Española de Protección de Datos se tramitó el procedimiento de apercibimiento de referencia A/00046/2015, a instancia de Doña **A.A.A.**, con Resolución del Director de la Agencia Española de Protección de Datos por infracción del artículo [XX] de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD). Dicho procedimiento concluyó mediante resolución R/01310/2015, de fecha 1 de junio de 2015 por la que se resolvía ***“REQUERIR a COPIFAX, S.L. para que CUMPLA lo previsto en el artículo 9 de la LOPD. En concreto se insta al denunciado a adoptar, de manera efectiva, las medidas técnicas y organizativas que garanticen la seguridad de los datos personales, que impidan el acceso por parte de terceros a los datos personales registrados en sus sistemas de información y en los equipos de su responsabilidad, y sin el consentimiento de los afectados, estableciendo mecanismos para que la información resulte accesible únicamente a los interesados y no a terceros y comprometiéndose expresamente a verificar que la información que incluyen en los discos duros corresponde a la del albarán de su titular, de acuerdo con lo establecido en el apartado 6 del artículo 45 de la LOPD, debiéndolo acreditarlo ante esta Agencia en el plazo de UN MES desde este acto de notificación, advirtiéndole que en caso contrario se procederá a acordar la apertura de un procedimiento sancionador.”***

Con objeto de realizar el seguimiento de las medidas a adoptar el Director de la Agencia Española de Protección de Datos insto a la Subdirección General de Inspección de Datos la apertura del expediente de actuaciones previas de referencia E/03228/2015.

SEGUNDO: Con motivo de lo instado en la resolución, el denunciado remitió a esta Agencia con fecha de entrada de 8 de julio de 2015, escrito en el que informaba a esta Agencia en los siguientes términos:

- 1) Aporta impreso de notificación de incidencias nº 01-2014, de fecha 5 de junio de 2014, referido a la prohibición de restauración de datos, dirigido a todo el personal de la empresa, y consecuencia de la reclamación de la denunciante.
- 2) Acompaña impreso de notificación de incidencias nº 01-2015, de fecha 5 de junio de 2015.

- 3) Aporta como Anexo I, la Instrucción técnica de despiece de ordenadores e Instrucción técnica IT-01, sobre despiece de equipos informáticos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la LOPD.

II

El artículo 9 de la LOPD dispone lo siguiente:

“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”.

El transcrito 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 dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el “acceso no autorizado” por parte de terceros.

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.

En lo que respecta al concepto de “fichero” el artículo 3.b) de la LOPD lo define como “todo conjunto organizado de datos de carácter personal”, con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la “comunicación” o “consulta” de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son

automatizados o no.

Y el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal *“cualquier información concerniente a personas físicas identificadas o identificables”*. En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *“toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*.

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *“...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen”*.

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.

Partiendo de tales premisas, procede analizar a continuación las previsiones contenidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, para garantizar la seguridad de los datos personales y, en concreto, que no se produzcan accesos no autorizados.

De acuerdo con lo establecido en dicho Reglamento, 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.

Los artículos 88 y 89 del citado Reglamento, aplicables a todos los ficheros y tratamientos automatizados, establecen:

“Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de

información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal”.

“Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento”.

En definitiva, COPIFAX está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

Sin embargo, COPIFAX, S.L., incumplió estas obligaciones, ya que se facilitaron datos personales a una tercera persona al entregarle un disco duro que no era suyo. Si COPIFAX hubiese actuado con la diligencia debida no habría incluido datos de un tercero en el disco duro de la denunciante, facilitando el acceso a un tercero de datos personales sin consentimiento del afectado.

III

En supuesto presente, del examen de las medidas adoptadas por COPIFAX, S.L., se constata que ha enviado a todo el personal de la empresa las instrucciones oportunas para que no vuelva a producirse la entrega de datos de una persona a un tercero, por lo que ha cumplido el requerimiento efectuado por la Agencia Española de Protección de Datos.

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 COPIFAX, S.L., y a Doña **A.A.A..**

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