Procedimiento Nº: A/00448/2017

RESOLUCIÓN: R/00478/2018

En el procedimiento A/00448/2017, instruido por la Agencia Española de Protección de Datos a la entidad SAGE SPAIN, S.L., vista la denuncia presentada por ASSESSORS FINANCIERS CASTELLAR XXI, S.L.L., y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 21 de marzo de 2017 tiene entrada en esta Agencia una denuncia presentada por ASSESSORS FINANCIERS CASTELLAR XXI, S.L.L., (en lo sucesivo, la entidad denunciante), en la que manifiesta lo siguiente:

Con fecha 26 de noviembre de 2015, la entidad denunciante suscribió tres contratos de prestación de servicios de compra, mantenimiento, asistencia técnica de software y servicios telemáticos con la empresa denunciada, SAGE SPAIN, S.L. Con fecha 7 de noviembre de 2016, la empresa denunciada, en la realización de pruebas de desarrollo de un nuevo programa, hizo uso sin autorización expresa de la entidad denunciante de todos los datos personales de los trabajadores de un cliente importante de la misma (MOBA ISE MOBILE AUTOMATION, S.L.). Desde una dirección electrónica de la entidad denunciante, realizó un envío masivo de e-mails destinados a todos los trabajadores del cliente con documentos adjuntos, consistentes en certificados de retenciones del trabajo y modelos 145 que, además, contenían datos absolutamente incorrectos. Con fecha 8 de noviembre de 2016, se informó de dicha incidencia a la denunciada por e-mail, no habiendo recibido respuesta hasta la fecha en la que se presenta la denuncia.

Con fecha 3 de mayo de 2017, la entidad denunciante remite a esta Agencia copia de varios correos recibidos por los trabajadores de la empresa de su cliente, así como diferentes correos que se han cruzado entre ambas empresas referentes a los hechos denunciados.

Anexa, entre otra, la siguiente documentación:

- Copia de dos correos con documentación de trabajadores de la empresa MOBA ISE MOBILE AUTOMATION, S.L.
- Copia de varios correos intercambiados entre la empresa denunciante y la denunciada, con relación a los hechos denunciados.
- Copia del contrato con la empresa MOBA ISE MOBILE AUTOMATION, S.L., donde se autoriza el acceso a datos por cuenta de terceros.
- Copia de los contratos de prestación de servicio con la denunciada.

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/02229/2017), teniendo conocimiento de los siguientes extremos:

Con fecha 26 de septiembre de 2017, se recibe en esta Agencia escrito de la empresa SAGE SPAIN, S.L., en el que se pone de manifiesto que:

1. La entidad denunciante otorgó consentimiento para el acceso a datos de terceros y su tratamiento, mediante los contratos de fechas 19 de noviembre de 2015 y 26 de noviembre de 2015, los cuales se adjuntan, y donde consta en su cláusula novena toda la información relativa al consentimiento y al artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Los hechos denunciados ocurrieron por los siguientes motivos:

   i. La entidad denunciante solicitó, con fecha 15 de septiembre de 2016, asistencia para solucionar un error en el cálculo de costes de un programa que permite el intercambio de ficheros con el Sistema RED de la TGSS.

   ii. SAGE SPAIN, S.L., solicitó a la entidad denunciante datos para poder repetir la operación en sus propios sistemas, para poder detectar así el error. La entidad denunciante facilitó datos de 34 empleados de la MOBA ISE MOBILE AUTOMATION, S.L.

   iii. Los datos recibidos de los clientes de la citada empresa debían eliminarse una vez solventado el problema, pero por accidente no fue así.

   iv. Como resultado del error, el 7 de noviembre de 2016, en una de las pruebas internas para la mejor del software, se emplearon las direcciones de correo electrónico de los 34 empleados, generándose y enviándose desde la dirección de correo electrónico ***URL.1 a cada uno de ellos sus respectivos certificados de retenciones y modelos 145.

   v. Hay que destacar en este tratamiento de datos lo siguiente:

      Que cada uno de los empleados recibió un correo electrónico sin contenido en texto, con el asunto “Envío Certificados”.

      Que los documentos enviados iban protegidos mediante contraseña, siendo necesaria para acceder a ellos, por lo que, a pesar de haber recibido cada titular del correo electrónico

sus respectivos documentos, no era posible el acceso a esa información por terceros.

3. Se adjunta Documento de Medidas de seguridad, donde figura en su página 6 las medidas establecidas para el acceso a datos de terceros, en las ocasiones en que se utilizan para TESTEO, entre las que figura la anonimización.

C

on fecha 4 de octubre de 2017 se recibe mediante correo electrónico informe donde figura el registro por parte de la empresa de la incidencia ocurrida con fecha 7 de noviembre de 2016 y las medidas correctoras tomadas por la entidad. Estas medidas consisten en el refuerzo de las medidas encaminadas al borrado de las bases de datos de clientes una vez que haya sido solucionado el problema por el que fueron enviadas, incluyendo al Development Manager como supervisor del proceso de borrado; la eliminación del acceso al repositorio de bases de datos de clientes a usuarios no identificados correctamente y la puesta en marcha del control de acceso del sistema para monitorizar todos los accesos que se produzcan al respositorio de bases de datos de clientes en reparación.

TERCERO: Consultada con fecha 18 de diciembre de 2017 la aplicación de la AEPD que gestiona la consulta de antecedentes de sanciones y apercibimientos precedentes, a la entidad denunciada SAGE SPAIN, S.L., no le constan registros previos.

CUARTO: Con fecha 26 de diciembre 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/00448/2017. Dicho acuerdo fue notificado a la entidad denunciada.

QUINTO: Habiendo transcurrido el plazo de quince días hábiles que se otorgó a la entidad denunciada para que formulara las alegaciones y presentara las pruebas que considerase convenientes, sin que se haya recibido respuesta de la misma, procede dictar resolución.

HECHOS PROBADOS

PRIMERO: Con fecha 26 de noviembre de 2015, ASSESSORS FINANCIERS CASTELLAR XXI, S.L.L., suscribió tres contratos de prestación de servicios de compra, mantenimiento, asistencia técnica de software y servicios telemáticos con la empresa denunciada, SAGE SPAIN, S.L.

SEGUNDO: Con fecha 15 de septiembre de 2016, la entidad denunciante solicitó a la entidad denunciada asistencia para solucionar un error en el cálculo de costes de un

programa que permite el intercambio de ficheros con el Sistema RED de la TGSS. A tal fin, SAGE SPAIN, S.L., solicitó a la entidad denunciante datos para poder repetir la operación en sus propios sistemas y poder detectar así el error. La entidad denunciante facilitó datos de 34 empleados de la MOBA ISE MOBILE AUTOMATION, S.L. Los datos recibidos de los clientes de la citada empresa debían eliminarse una vez solventado el problema, pero por accidente no fue así.

TERCERO: Como resultado del error, el 7 de noviembre de 2016, en una de las pruebas internas para la mejora del software, la entidad denunciada empleó las direcciones de correo electrónico de los citados 34 empleados, generándose y enviándose desde la dirección de correo electrónico ***URL.1 a cada uno de ellos sus respectivos certificados de retenciones y modelos 145. Dichos documentos iban protegidos mediante contraseña, siendo necesaria para acceder a ellos, por lo que, a pesar de haber recibido cada titular del correo electrónico sus respectivos documentos, no era posible el acceso a esa información por terceros.

CUARTO: La entidad denunciada ha procedido a registrar la incidencia y a adoptar medidas correctoras para evitar, en lo sucesivo, incidentes de este tipo. Estas medidas consisten en el refuerzo de las medidas encaminadas al borrado de las bases de datos de clientes una vez que haya sido solucionado el problema por el que fueron enviadas, incluyendo al Development Manager como supervisor del proceso de borrado; la eliminación del acceso al repositorio de bases de datos de clientes a usuarios no identificados correctamente y la puesta en marcha del control de acceso del sistema para monitorizar todos los accesos que se produzcan al respositorio de bases de datos de clientes en reparación.

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*".

El artículo 87.2 del citado Reglamento dispone:

"*Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación*".

SAGE SPAIN, S.L., debió, por ello, proceder al borrado o destrucción de los datos de carácter personal facilitados por ASSESSORS FINANCIERS CASTELLAR XXI, S.L.L., una vez fue solventado el error para el cual le fueron facilitados. Tal medida no fue adoptada, prueba de ello es el envío de e-mails a los trabajadores de un cliente de la entidad denunciante, con documentos adjuntos, consistentes en certificados de retenciones del trabajo y modelos 145.

En el presente caso, ha quedado acreditado que SAGE SPAIN, S.L., no cumplió con la medida de seguridad contemplada en el artículo 87.2 del Reglamento de desarrollo de la LOPD.

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 SAGE SPAIN, S.L., se considera que ha incurrido en la infracción grave descrita.

IV

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 la infracción de la LOPD de la que se responsabiliza a la entidad denunciada es "grave"; que la entidad denunciada no ha sido sancionada o apercibida por esta Agencia en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD, en concreto el carácter puntual de la infracción, la ausencia de beneficios obtenidos como consecuencia de la misma y la ausencia de intencionalidad, así como el reconocimiento espontáneo de su culpabilidad. 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, 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.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **ARCHIVAR (A/00448/2017)** las actuaciones practicadas SAGE SPAIN, 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 su artículo **9.1**, en relación con el artículo 87 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como **grave** en el artículo **44.3.h)** de la LOPD.

2. **NOTIFICAR** el presente Acuerdo a SAGE SPAIN, 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