

Procedimiento N°: A/00131/2016

RESOLUCIÓN: R/00867/2016

En el procedimiento A/00131/2016, instruido por la Agencia Española de Protección de Datos a la entidad **GLOBAL FUNDRAISING SL**, vista la denuncia presentada y en virtud de los siguientes,

ANTECEDENTES

PRIMERO Con fecha de 21/4/15 tiene entrada en esta Agencia un escrito remitido por la Agencia Catalana de Protección de Datos en el que el **A.A.A.** pone de manifiesto los siguientes hechos:

Con fecha 19/3/15 se personaron en el Ayuntamiento cuatro personas para explicar que durante unos días se haría en el pueblo una campaña promocional de Gas Natural Fenosa, dejando copia de sus credenciales de empresa y de su DNI.

La campaña se realizó del 19 al 23 de marzo de 2015.

Y con fecha 31 de marzo de 2015, un trabajador del Ayuntamiento encontró en una papelera documentos de Gas Natural Fenosa y facturas de Endesa en las que constan datos personales.

Adjunto a la denuncia se ha aportado la documentación encontrada en la papelera que consta de varios contratos de Gas Natural Fenosa cumplimentados con datos de nombre y apellidos, DNI, firma, facturas de Endesa Energía XXI S.L.U. y copia de cuatro DNI y de cuatro acreditaciones de las personas que constan en los DNI en las que figuran como Agentes Comerciales de la compañía **GLOBAL FUNDRAISING SL**.

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/03121/2015 y concluye la investigación con el informe siguiente de la Inspección de Datos:

<<<<< Con fecha 26 de mayo de 2015 se solicita información a GLOBAL FUNDRAISING SL y de la respuesta remitida, en fecha de registro de entrada a esta Agencia 25 de junio de 2015, se desprende:

** GLOBAL FUNDRAISING SL tiene suscrito un contrato de prestación de servicios comerciales con Gas Natural Servicios SDG S.A. por el cual GLOBAL FUNDRAISING SL realizará asesoría y apoyo comercial y técnico para la captación de nuevos clientes de los productos y servicios comercializados por Gas Natural Servicios SDG S.A.*

** GLOBAL FUNDRAISING SL ha aportado copia del contrato mencionado de fecha 1 de enero de 2015.*

** GLOBAL FUNDRAISING SL manifiesta tener suscrito un contrato de prestación de servicios con SAEZ MARKETING SL y manifiesta que las cuatro personas que constan en las acreditaciones son empleados de esta última compañía.*

** La entidad ha aportado copia de un contrato sin firmar, de fecha 10 de abril de 2014, donde consta que la empresa SAEZ MARKETING SL comercializara productos y servicios de GLOBAL FUNDRAISING SL.*

** No obstante, GLOBAL FUNDRAISING SL ha aportado copia de "Aceptación del código de buenas prácticas en la venta presencial de Gas Natural Fenosa" firmado por los cuatro agentes comerciales cuyas acreditaciones y DNI fueron depositados en el A.A.A., en las que figura como sello de la empresa GLOBAL FUNDRAISING SL.*

** GLOBAL FUNDRAISING SL manifiesta desconocer el motivo por el cual se ha encontrado la documentación en una papelera en la población de ORISTA fuera de la oficina.*

** Con fechas 4 de septiembre de 2015 y 12 de enero de 2016 se remite solicitud de información a SAEZ MARKETING SL al domicilio que figura en el Registro Mercantil Central, sin obtener respuesta a pesar de que ambas requerimientos han sido recogidos y firmados, en fechas 9 de septiembre de 2015 y 18 de enero de 2016, tal y como constan en los acuses de recibo del servicio de Correos. >>>>>*

TERCERO: Con fecha 28/3/14 la Directora de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00131/2016.

CUARTO: Con fecha 11/4/16 se recibe en esta Agencia escrito del denunciado en el que comunica lo siguiente:

** Que han procedido a rescindir el contrato con **B.B.B.** porque dadas las circunstancias no les ofrecen las garantías necesarias de seguridad y confidencialidad en el tratamiento de los datos.*

** Que como condición indispensable para poder proceder a la contratación, los comerciantes externos, además de firmar la aceptación de buenas prácticas que exige Gas Natural y otros clientes deben firmar un documento de seguridad cuyo modelo se adjunta*

** Se ha procedido a ampliar el documento de seguridad añadiendo el apartado "Gestión de soportes y documentos – comerciales externos – con el anterior documento con el fin de ser tenido en cuenta y utilizado en todos los procesos de contratación de comerciales externos.*

- Que los hechos se produjeron con las siguientes circunstancias.*
- No existió intencionalidad.*
- No se ha causado perjuicio a terceras personas.*
- No ha existido ningún beneficio.*
- Se trata de un hecho puntual.*
- Que la infracción fue consecuencia de una anomalía de funcionamiento de los procedimientos establecido.*

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 LOPD.

II

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.....

l) 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, y en relación a los hechos denunciados la empresa GLOBAL FUNDRAISING SL debe considerarse encargada de tratamiento de Gas Natural Servicios SDG S.A. en virtud de un contrato de prestación de servicios, en virtud del cual realizará asesoría y apoyo comercial y técnico para la captación de nuevos clientes de los productos y servicios comercializados por esa entidad. Así mismo GLOBAL FUNDRAISING había subcontratado con SAEZ MARKETING manifestando que los cuatro agentes comerciales, cuyas acreditaciones y DNI fueron depositados en el A.A.A., pertenecían a esta última empresa.

III

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”

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.

IV

Se imputa e primer lugar la comisión de una infracción del art 9 de la LOPD que exige la necesidad de adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. En dicho artículo se hace referencia no sólo a medidas técnicas sino también organizativas, medida que garantice la seguridad de dichos datos.

En el caso que nos ocupa la documentación encontrada: (varios contratos de Gas Natural Fenosa cumplimentados con datos de nombre y apellidos, DNI, firma, facturas); 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 Reglamento 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 artículo 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. Debe señalarse que el incumplimiento de este tipo de previsión implica un riesgo muy importante en la divulgación no deseada de documentos con datos personales.

Los hechos, que traen causa en este procedimiento, derivan de la localización, con fecha 31 de marzo de 2015, por un trabajador del A.A.A. en una papelería de documentos de Gas Natural Fenosa y facturas de Endesa en las que constan datos personales.

En conclusión, es de aplicación lo dispuesto en artículo 92.4 del Real Decreto 1720/07, Reglamento de desarrollo de la LOPD, de 21 de diciembre, que dispone que: *“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 aquellas medidas dirigida a evitar el acceso a la información contenida en el mismo o su recuperación posterior”*. Esta previsión del artículo 92 es también de aplicación a los ficheros y tratamientos no automatizados, en virtud de la remisión que se hace desde el artículo 105.2.d.

En este apartado cuarto se regulan las obligaciones que tendrán que aplicarse cuando vaya a desecharse cualquier documento o soporte que contenga datos personales. Estableciéndose, aunque no se definen en concreto las medidas, que serán aquellas que eviten el acceso a la información contenido en los mismos, así como su posible recuperación posterior. En este caso, la aparición de documentación de cuya custodia era responsable la entidad denunciada permite deducir que está no observó la diligencia adecuada, ya que tenía que haberse asegurado las medidas que imposibilitaran la recuperación posterior de la misma, o el tratamiento confidencial de la información en el supuesto que su gestión fuera a ser subcontratada con otra empresa.

V

De los hechos probados en este procedimiento, se deduce que GLOBAL FUNDRAISING en su calidad de encargada de 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 un tercero, que la localizó tirada en el suelo y al lado de un contenedor. 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.

Dicha responsabilidad no puede atribuirse a SAEZ MARKETING SL, independientemente que actuara como entidad subcontratada por GLOBAL FUNDRAISING SL y que fue la responsable de la gestión de la documentación al no acreditarse que actuara en nombre de esta última, habiéndose aportado solo una copia de un contrato sin firmar, de fecha 10 de abril de 2014, donde consta que la empresa SAEZ MARKETING SL comercializara productos y servicios de GLOBAL FUNDRAISING SL.

A este respecto hay que tener en cuenta lo establecido en el art. 12 de la LOPD que dispone lo siguiente:

Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Hay que tener en cuenta, tal como ha señalado esta Agencia en un informe de 27 de julio de 2006 *“Para delimitar si en un supuesto concreto nos encontramos ante una cesión de datos o ante una realización de actividades reguladas por el artículo 12 de la Ley Orgánica, será preciso atender a las circunstancias de cada caso, de tal forma que existirá cesión en aquellos supuestos en los que quien reciba los datos pueda aplicar los mismos a sus propias finalidades, decidiendo sobre el objeto y finalidad del tratamiento, lo que la convertirá a su vez en un responsable del fichero o tratamiento, mientras que la figura regulada por el artículo 12 de la Ley Orgánica tendrá cabida en aquellos otros casos en que la entidad receptora de los datos se limite a efectuar determinadas operaciones sobre los mismos, sin decidir sobre su finalidad.”*

Ahora bien, para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el

artículo 12 de la Ley Orgánica 15/1999, considerando los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero (en este caso SAEZ MARTINEZ se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero GAS NATURAL SERVICIOS

En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la Ley Orgánica 15/1999 impone que *“la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”*.

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley orgánica 15/1999, de forma que *“una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”*.

El incumplimiento de la previsión señalada en el artículo 12.3, que en el presente caso queda limitada, por la propia naturaleza del servicio a prestar, evitándose, en particular, el abandono de los documentos que contengan datos personales

VI

El hecho constatado en el presente procedimiento, relativo a la aparición de documentación con datos de carácter personal en la vía pública y accesible a terceros supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte de la responsable del tratamiento

El artículo 44.3 h) califica como 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”*. De acuerdo con los fundamentos anteriores, se deduce que por parte GLOBAL FUNDRAISING S.L. se ha producido una vulneración de la de seguridad de los datos, que ha tenido como consecuencia que los datos personales, pudieran ser vistos por un tercero, infracción que procede calificarla en el grado señalado.

La exigencia de la “culpabilidad” deriva de lo que señala el artículo 130 de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común – LRJPAC- cuando dice que: *“Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia”*.

Si bien en materia sancionadora rige el principio de culpabilidad, la expresión “simple inobservancia”, del art. 130.1 de la Ley 30/92, permite la sanción por inobservancia del deber de cuidado. Tal es la interpretación que ha establecido la Audiencia Nacional en la

sentencia de 6/02/08. Existe una obligación de resultado, que no se ha cumplido, pues documentación con datos de carácter personal procedente de la entidad denunciada se encontró si destruir, de lo que se desprende una falta de negligencia del responsable del tratamiento, obligado a implementar las medidas de seguridad. No obstante, deben tenerse en cuenta otros elementos que sirven para aminorar dicha responsabilidad: que por parte de la denunciada exista documento de seguridad, que se han realizado diversas campañas de concienciación y formación entre el personal de la empresa, que el sistema informático está formado por diversos servidores independientes para proteger los accesos, que dispongan de varias destructoras de documentos ubicadas en distintos lugares, y que la denuncia procediera a prescindir de los servicios de las empresas que hasta aquél entonces recogían los residuos que generaba y contratar a otra que garantizase el cumplimiento de la normativa vigente en tratamiento y destrucción de soporte papel con datos de carácter personal,.

La necesidad de especial diligencia en la custodia de la documentación por parte del responsable y encargado del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en diversas sentencias, en particular en la sentencia de 25/06/09, Rec. 237/2008, que manifiesta: *“Es doctrina reiterada en esta Sala, SSAN, sec. 1ª, de 25/1/06 (re. 227/2004), 28/06/06 (Re. 290/2004), que “No basta con la aplicación formal de las medidas de seguridad, pues resulta exigible que aquellas se instauren y pongan en práctica de manera efectiva... Se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva la recurrente es, por disposición legal, una deudora de seguridad en materia de datos y puesto que es una deudora de seguridad en materia de datos es insuficiente, según se desprende la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad también es responsable de que las mismas se cumplan y ejecuten con rigor”*

VII

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. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: *“El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)”.*

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: *“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 automatizada mente 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 más 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, la entidad denunciada es responsable de la custodia de la documentación con datos de carácter personal, que ha sido recuperada , existiendo pues, una omisión 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.

VIII

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, se deduce que por parte de la entidad denunciada se ha producido una vulneración del deber de secreto y de seguridad de los datos, infracciones que procede calificarlas como graves. Sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: *“Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada...sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una*

persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo”.

IX

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 las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Reglamento del procedimiento para el ejercicio de la potestad sancionadora (Real Decreto 1398/1993, de 4 de agosto) que señala que *“en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida”*, procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.g) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD.

X

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”.

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6. Junto a ello se constata una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

Sin embargo, deben valorarse las circunstancias particulares en que se produjeron los hechos, que la empresa **GLOBAL FRUNDRAISING** subcontractó la prestación de una serie de servicios con SAEZ MARKETING, habiéndose procedido a rescindir el contrato con la misma, Apreciándose una conducta diligente en orden a evitar dichas situaciones en el futuro con las medidas siguientes:

- * Que como condición indispensable para poder proceder a la contratación, los comerciantes externos, además de firmar la aceptación de buenas prácticas que exige Gas Natural y otros clientes deben firmar un documento de seguridad cuyo modelo se adjunta

- * Se ha procedido a ampliar el documento de seguridad añadiendo el apartado “Gestión de soportes y documentos – comerciales externos – con el anterior documento con el fin de ser tenido en cuenta y utilizado en todos los procesos de contratación de comerciales externos.

XI

En supuesto presente, del examen de las medidas adoptadas por **GLOBAL FRUNDRAISING** que han descritas en el fundamento anterior 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 uno o unos empleados de la empresa subcontractada 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

En consecuencia, en el presente caso debe procederse a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, en aplicación de lo establecido en el artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

De acuerdo con lo señalado,

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



SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **Global Fundraising SI**
- 3.- **NOTIFICAR** el presente Acuerdo a **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 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 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 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