

Expediente N°: E/02273/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **FILIASUR SARL** en virtud de denuncia presentada por Don **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 24 de enero de 2013, tuvo entrada en esta Agencia escrito de D. **A.A.A.** (en lo sucesivo el denunciante) frente a la Entidad denunciada--**FILIASUR SARL**-- en lo sucesivo el/la denunciado) en el que denuncia de manera sucinta que:

“La Aseguradora Filiassur ha contratado en mi nombre un seguro de salud, al cual yo no he accedido facilitándoles dato alguno mío, ni estando en su poder contrato alguno firmado por mí, tales como el nº de cuenta de cobro al cual han remitido un primer recibo, con fecha 03/01/13...”.

Aporta

Copia de la póliza nº *****PÓLIZA.1** emitida por la aseguradora CHUBB INSURANCE COMPANY OF EUROPE SE SUCURSAL EN ESPAÑA (NIF *****, CALLE (C/.....1) MADRID). El documento incluye como tomador a Don **A.A.A.** NIF *****NIF.1, (C/.....2)**, fecha nacimiento DD/MM/AA, Cónyuge: **B.B.B.**, fecha nacimiento: DD/MM/AA1 y como empresa mediadora FILIASUR (CORREDURIA DE SEGUROS). Incluye domicilio bancario para el cobro (CCC: *****CCC.1**) fecha de 12/11/2012 y carece de la firma del tomador.

Copia del recibo bancario de fecha 3/1/2013 emitido por CAJA ESPAÑA relativo a un cargo por importe de 23 € en la cuenta *****CCC.1** de la que es titular A.A.A. figurando como entidad emisora del recibo FILIASUR HOSPITALIZACION.

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, teniendo conocimiento de los siguientes extremos:

1. En fecha de 25/11/2013 se solicita información a **FILIASUR SARL** quien remite escrito de respuesta recibido en fecha de 22/11/2013 del que se desprende lo siguiente:
 - 1.1. **FILIASUR SARL** es una empresa francesa que opera en España en calidad de mediador de seguros.
 - 1.2. Respecto al contrato objeto de la denuncia manifiesta que se realizó a través de un operador telefónico de la empresa QUALITEL JEREZ a partir de datos

obtenidos de la base de datos de clientes del operador de telecomunicaciones ONO.

1.3. Añade **FILIASSUR SARL** que ellos únicamente disponen de acceso a los datos de los clientes de ONO que han realizado la contratación telefónica del seguro ofrecido.

1.4. Como soporte de la contratación **FILIASSUR SARL** aporta grabación de la contratación y copia de un contrato en el que figura como tomador **A.A.A.** sin que conste la firma de éste.

1.4.1. Respecto de la grabación presenta el siguiente contenido:

Se escucha una voz femenina que corresponde a una operadora hablando con un interlocutor con voz masculina. El resumen de la conversación es el siguiente:

La operadora informa de que le llaman en su calidad de cliente de ONO para ofrecerle una oferta de seguros con la compañía CHUBB que incluye una promoción especial por ser cliente de ONO. Seguidamente le facilita la identificación de la empresa FILIASSUR como mediadora de seguro así como términos generales del contrato.

A petición de la operadora, quien dice ser **A.A.A.**, con DNI *****NIF.1** y domicilio en calle (C/.....2), provincia de LEÓN, afirma que trabaja por cuenta ajena en una empresa de cables y que nació el DD/MM/AA.

La operadora facilita información sobre las coberturas del seguro de hospitalización.

A petición de la operadora el cliente confirma sus números de teléfono móvil y fijo y facilita información sobre su pareja aportando el nombre de **B.B.B.**, nacida el DD/MM/AA2, y trabajadora por cuenta ajena como contratada laboral en la Junta. La operadora solicita el DNI de la mujer y el cliente afirma no conocerlo escuchándose como una voz femenina aporta dicho DNI.

La operadora solicita autorización para poder utilizar el número de cuenta bancaria utilizado para los cargos de ONO en los cargos del seguro accediendo el cliente a ello.

Seguidamente la operadora le informa de los aspectos relativos a la protección de datos personales informando de que los datos recabados así como la grabación de la contratación van a formar parte de un fichero del que es responsable la entidad FILIASSUR y que dichos datos serán utilizados para formalizar la póliza de seguros. Le informa también de la posibilidad de ejercer sus derechos de acceso, rectificación y cancelación facilitando para ello diversas vías: número de teléfono y una dirección en España y otra en Francia.

Finalmente la operadora le informa de que el primer mes es gratuito y que durante dicho mes puede cancelar la póliza sin coste alguno dirigiéndose por escrito a la dirección de Madrid. Añade que queda cubierto desde las 12 horas de la noche del día de la grabación manifestando el cliente su conformidad.

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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 6 de la LOPD, determina:

*“1. El tratamiento de los datos de carácter personal requerirá el **consentimiento inequívoco** del afectado, salvo que la Ley disponga otra cosa.*

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.

El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo) señala que:

“...consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele”.

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

III

En el presente caso, se procede a analizar la reclamación de entrada en esta AEPD de fecha **24/04/13** en dónde el epigrafiado pone de manifiesto de manera sucinta que:

“La Aseguradora Filiassur ha contratado en mi nombre un seguro de salud, al cual yo no he accedido facilitándoles dato alguno mío, ni estando en su poder contrato alguno firmado por mí, tales como el nº de cuenta de cobro al cual han remitido un primer recibo, con fecha 03/01/13...”.

A requerimiento de esta AEPD la Entidad denunciada —**Filiassur**—alega como mejor proceda en Derecho en fecha 12/12/13 lo siguiente:

*“Que se procedió a la contratación del servicio de seguros para el denunciante, por medio de llamada telefónica, a través de la cual recabó el **consentimiento** del cliente”.*

Item, pone de manifiesto que la Entidad—**Filiassur**—no tiene acceso a los datos del cliente hasta que **QUALITEL JEREZ** (encargada del tratamiento del fichero) finaliza la contratación de la póliza ofertada.

Como medio de prueba admisible en Derecho aporta grabación de la conversación telefónica en dónde tras escuchar la misma se escucha una “voz masculina” que se identifica como D. **A.A.A.**, aportando el número del DNI y una serie de datos de carácter personal que legitiman la contratación.

La **presunción de inocencia** debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del ius puniendi en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional en su Sentencia 76/1990, de 26/04, considera que el derecho a la presunción de inocencia comporta: “que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio.

La **presunción de inocencia** rige sin excepciones en el Ordenamiento sancionador y ha de ser respetada en la imposición de cualquier sanción, ya sea penal o administrativa (TCo 13/1981), pues el ejercicio del derecho sancionador en cualquiera de sus manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

Conforme a este principio, no puede imponerse sanción alguna en razón de la culpabilidad del imputado si no existe una actividad probatoria de cargo, que en la apreciación de las autoridades u órganos llamados a resolver, destruya esta presunción (TCo Auto 3-12-81).

Por tanto, una vez analizada la documentación presentada cabe concluir que la Entidad denunciada—**Filiassur**—adoptó la diligencia mínima exigible en estos casos para proceder a la contratación de los servicios ofertados (póliza de seguros) aportando copia de la grabación.

Sobre supuestos similares se ha pronunciado la Audiencia Nacional, la SAN 29-04-2010 *"La cuestión no es dilucidar si la recurrente trató los datos de carácter personal de la denunciante sin su consentimiento, como si empleo o no una diligencia razonable a la hora de tratar de identificar a la persona con quien suscribió el contrato de financiación"*.

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998 , parcialmente transcrita en las SSTs de 9 de octubre de 2009, Rec 5285/2005 , y de 23 de octubre de 2010, Rec 1067/2006 , que *"aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa"* .

Todo ello determina que la entidad sancionada actuó de **buena fe**, sobre la base de una documentación con apariencia de legalidad.

Por todo lo expuesto, se procede a ordenar el **ARCHIVO** del presente procedimiento al no considerarse que la Entidad denunciada haya infringido la normativa vigente en materia de protección de Datos.

Finalmente, sobre la utilización con fines "maliciosos" de los datos del afectado por un tercero, esta AEPD carece de competencias materiales sobre la cuestión, siendo el órgano jurisdiccional del lugar de comisión del "presunto" hecho delictivo el que deberá en fase de instrucción ordenar en caso de estimarlo oportuno la realización de un cotejo pericial de la voz de la grabación aportada.

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 la Entidad-- **FILIASSUR SARL--** y a Don **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 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