**Expediente Nº: E/02405/2017**

## RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ALTANIA DEL MAR, S.L., en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

## HECHOS

**PRIMERO:** Con fecha 30 de marzo de 2017, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.*** en el que manifiesta que en el mes de marzo de 2017 comenzó a utilizar los servicios de psicología ofertados en la página ***WEB.1, verificando que no existe una conexión segura (Protocolo SSL), ante lo que sospecha que puedan incumplir otras medidas de seguridad.

Anexa la siguiente documentación:

Impresión de pantalla de la conversación mantenida con el profesional que le atendió, donde figura el siguiente literal: "*La conexión con este sitio web no es segura".*

**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. Con fecha 6 de julio de 2017, se realizó visita de inspección en los locales de la entidad ALTANIA DEL MAR, S.L., titular de la página: ***WEB.1, en el transcurso de la cual se pusieron de manifiesto los siguientes hechos:

   a. La entidad ALTANIA DEL MAR fue constituida el 23 de agosto de 2001, pero la Aplicación ***WEB.1 se incorpora a dicha entidad en enero de 2017. Cuando se activó la aplicación a través de la página ***WEB.1, el acceso a la plataforma no contaba con un protocolo seguro de comunicación (cifrado de las comunicaciones).

   No obstante, la entidad tenía implementadas el resto de medidas con relación al acceso (registro de acceso, control anti ataques DDOS, comprobación de acceso mediante usuario y contraseña, etc.).

   b. A partir del mes de marzo de 2017 se comienzan a realizar una serie de cambios, creando una nueva web denominada ***WEB.2, la cual cuenta con un protocolo seguro (SSL). En los documentos denominados CONDICIONES LEGALES, POLITICA DE PRIVACIDAD y POLITICA DE COOKIES, se informa de la relación existente entre el usuario y ALTANIA DEL MAR y de ésta con los terapeutas que trabajan con este servicio. El contenido de los mismos es igual que el existente en la aplicación ***WEB.1.

c. Entre el 1 de mayo y el 14 de mayo de 2017, conviven las aplicaciones ***WEB.1 y ***WEB.2. Con fecha 14 de mayo de 2017, se cierra la antigua web quedando únicamente activa la segunda. A partir de esa fecha, el intento de acceso a la página ***WEB.1 redirecciona a la página ***WEB.2, con protocolo de comunicación seguro.

d. ALTANIA DEL MAR, tiene suscritos contratos de prestación de servicios con seis terapeutas, actuando con éstos como una Plataforma de intermediación para ofrecer los servicios de salud al usuario. ALTANIA DEL MAR se limita a poner en contacto al usuario con el psicólogo, siendo ALTANIA DEL MAR el responsable de los datos de registro y el terapeuta el responsable de la información clínica.

e. Para la regulación de la relación entre los terapeutas y la entidad, se suscribe un contrato de Comisión Mercantil por Prestación de Servicios Publicitarios e Intermediación, el cual, entre otros, contiene un Anexo, en el que se estipulan las obligaciones de Protección de Datos, entre ellas, se especifica que:

   i. ALTANIA DEL MAR, realizará el tratamiento de los datos por cuenta del terapeuta y de conformidad con sus instrucciones, así como no los utilizará para una finalidad distinta a la del servicio ofertado.

   ii. ALTANIA DEL MAR, atenderá por cuenta del terapeuta las solicitudes de ejercicio de Derechos ARCO.

   iii. Cancelará el tratamiento de datos de los usuarios si el terapeuta cancela su suscripción a la Plataforma.

f. Toda la información recabada, tanto la que es responsable la Plataforma como los datos de salud (chat con el terapeuta) son almacenados en una Base de Datos que se encuentra ubicada en los servidores de AMAZON con quien la entidad tiene suscrito un contrato de prestación de servicios de almacenamiento en NUBE. Dicha información viaja cifrada.

g. Entre los servicios prestados por AMAZON se encuentra la realización de Copias de Seguridad. Desde la entidad se tiene acceso a la Base de Datos mediante una herramienta proporcionada por AMAZON. Cuando un usuario solicita el ejercicio de algún derecho desde ALTANIA DEL MAR se responde sobre los datos de registro a la Plataforma y con relación a los datos clínicos se le remite al terapeuta o bien se traslada a éste la solicitud para que dé respuesta al usuario.

h. ALTANIA DEL MAR no tiene acceso inmediato al contenido de los chats existentes en la Base de Datos, siendo necesario un procedimiento técnico, por motivos de seguridad, que supone una demora en el acceso. Hasta el momento no se ha hecho uso de dicho procedimiento.

i. Con relación a la existencia de un procedimiento establecido para el

ejercicio de Derechos ARCO, ALTANIA DEL MAR ha remitido, con fecha 20 de julio de 2017, un documento, en el que manifiesta que esa entidad actúa como encargada del tratamiento de los datos de los terapeutas que utilizan la plataforma y les asiste para atender el ejercicio de derechos ARCO por parte de sus pacientes, conforme viene obligada por el contrato que suscriben con ellos. No obstante, no tienen constancia de que ALTANIA DEL MAR haya recibido hasta el momento ningún ejercicio de derechos ARCO ni reclamación, de ningún usuario.

j. En el transcurso de la inspección se solicita la realización de un registro de un usuario de prueba a través de la página ***WEB.2 verificándose que:

- Al acceder a la opción de "Registrarse", en la primera página, aparece un cuestionario que solicita los datos de Nombre, E-mail y contraseña. Asimismo consta el siguiente literal: *Al presionar "Crear cuenta", acepto los Términos y Condiciones y la Política de Privacidad.*

  Se verifica que "*Términos y Condiciones" y "Política de Privacidad"* son links activos.

- Una vez aceptado, la aplicación introduce al usuario en un chat, que según manifestaciones del representante de la entidad ALTANIA DEL MAR, se trata de un chat con un "Asesor", al cual el usuario explicará que servicios demanda y éste le derivará a un terapeuta, en función de sus necesidades.

- Para acceder a los servicios del terapeuta, previamente, debe abonar el servicio mediante el acceso al icono de una tarjeta existente en la parte superior de la pantalla, debiendo introducir los datos de número de tarjeta, fecha de caducidad y CVC.

- Una vez realizada esta acción, aparece en el chat el mensaje "*Te has suscrito al plan: XXXX".* No obstante, el representante de la entidad manifiesta que el acceso al chat con el terapeuta no es inmediato, tarda unas horas en estar activo.

- Posteriormente, el usuario accederá al servicio con sus claves, entrando directamente al chat del terapeuta asignado. La representante de la entidad manifiesta que la información contenida en dicho chat, es también almacenada en la Base de Datos ubicada en los servidores de AMAZON.

Se verifica que durante todo el proceso la conexión que se muestra en el campo URL del navegador, es una conexión segura.

k. Con relación al número de usuarios registrados en dicha Plataforma, se hizo entrega de un informe gráfico en el que se muestran los usuarios registrados durante el periodo comprendido entre el mes de mayo y julio de 2017, en el que figuran unos 5000 registros en la Plataforma, de los cuales aproximadamente 100 han suscrito el servicio mediante abono de los honorarios correspondientes. Durante los meses de enero a abril de 2017 se han registrado un total de 1500 usuarios, de los cuales, 71 han utilizado el servicio mediante

pago de honorarios.

2. Con fecha 20 de julio de 2017, han procedido a la remisión de una copia del Documento de Seguridad, con el que acompañan copia de los servicios suscritos con AMAZON para el alojamiento de las bases de Datos. Asimismo, se adjunta copia de documentos legales más relevantes, desde el punto de vista de protección de datos, que regulan dicha relación contractual. Altania del Mar ha seleccionado, al contactar los servicios, que el alojamiento de los datos por parte de Amazon se restrinja a la zona denominada "EU (Francfort) Region", de forma que el servicio está limitado a Europa.
3. ALTANIA DEL MAR, cuenta actualmente con seis ficheros inscritos en el Registro General de Protección de Datos, entre los que se encuentran:
    a. "USUARIOS APP", con el código de inscripción: ***REG.1, cuya finalidad es la Gestión de Clientes de los usuarios de la APP XXXX.
    b. "USUARIOS", con el código de inscripción: ***REG.2, cuya finalidad es gestión de clientes usuarios de la página web XXXX.

## FUNDAMENTOS DE DERECHO

### I

Es competente para resolver la Directora 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).

El artículo 126.1, apartado segundo, del Real Decreto 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 establece:

*Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.*

### II

La denuncia se concreta que al comenzar a utilizar los servicios de psicología ofertados en la página ***WEB.1, verificó que no existía una conexión segura (Protocolo SSL), ante lo que sospecha que puedan incumplir otras medidas de seguridad

El protocolo de capa de conexión segura (SSL) permite el establecimiento de comunicaciones seguras en Internet para la navegación web, el correo electrónico, la mensajería instantánea y otros sistemas de transferencia de datos. Es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.

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 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.

El Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en su artículo 81.1 señala 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. El artículo 88, en su punto 3, se refiere al documento de seguridad.

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. En el caso que nos ocupa como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

Igualmente el art. 104 del citado Reglamento, en relación con las medidas de seguridad de nivel alto establece: ***"****Telecomunicaciones.*

*Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros."*

Esta es la concreta medida de seguridad de las legalmente previstas en la que se observa la vulneración del principio de seguridad de los datos, dado que a esto se refiere el Protocolo SSL.

Cuando los Inspectores de la Agencia Española de Protección de Datos efectuaron la visita de Inspección a la entidad denunciada, realizaron una prueba registrándose en la página web de la misma forma que lo hacen los clientes. Pudieron constatar que durante todo el proceso la conexión que se muestra en el campo URL del navegador es una conexión segura.

**III**

La falta de medidas de seguridad constituye una infracción tipificada como grave en el artículo 44.3.h) de la LOPD, que considera como tal: *"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"*.

En el presente caso, se ha producido la falta de una concreta medida de seguridad establecida en el artículo 104 del Reglamento de desarrollo de la LOPD.

No obstante, 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 la falta de protocolo de conexión

segura se produjo durante un espacio muy breve de tiempo, que ya ha sido corregido, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

Por otro lado, la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, recurso 455/2011, de 29/11/2013, analiza el apercibimiento como un acto de naturaleza no sancionadora, como se deduce del fundamento de derecho Sexto:

*<<…Debe reconocerse que esta Sala y Sección en alguna ocasión ha calificado el apercibimiento impuesto por la AEPD, en aplicación del artículo examinado, como sanción (SAN de 7 de junio de 2012, rec. 285/2010), y en otros casos ha desestimado recursos contencioso-administrativos interpuestos contra resoluciones análogas a la recurrida en este procedimiento, sin reparar en la naturaleza no sancionadora de la medida expresada (SSAN de 20 de enero de 2013, rec. 577/2011, y de 20 de marzo de 2013, rec. 421/2011). No obstante, los concretos términos en que se ha suscitado la controversia en el presente recurso contencioso-administrativo conducen a esta Sala a las conclusiones expuestas, corrigiendo así la doctrina que hasta ahora venía presidiendo la aplicación del artículo 45.6 de la LOPD…>>*

Además, la sentencia interpreta o liga apercibimiento o apercibir con el requerimiento de una actuación para subsanar la infracción, y si no existe tal requerimiento, por haber cumplido las medidas esperadas relacionadas con la infracción, no sería apercibimiento, sino archivo, como se deduce del citado fundamento de derecho: *<<…Pues bien, en el caso que nos ocupa el supuesto concreto, de entre los expresados en el apartado quinto del artículo 45, acogido por la resolución administrativa recurrida para justificar la aplicación del artículo 45.6 de la LOPD es el primero, pues aprecia "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", tal y como expresa su fundamento de derecho VII.*

*Por ello, concurriendo las circunstancias que permitían la aplicación del artículo 45.6 de la LOPD, procedía "apercibir" o requerir a la denunciada para que llevara a cabo las medidas correctoras que la Agencia Española de Protección de Datos considerase pertinentes, en sustitución de la sanción que de otro modo hubiera correspondido.*

*No obstante, dado que resultaba acreditado que la denunciada por iniciativa propia había adoptado ya una serie de medidas correctoras, que comunicó a la Agencia Española de Protección de Datos, y que esta había verificado que los datos del denunciante no eran ya localizables en la web del denunciado, la Agencia Española de Protección de Datos no consideró oportuno imponer a la denunciada la obligación de llevar a cabo otras medidas correctoras, por lo que no acordó requerimiento alguno en tal sentido a ésta.*

*Recuérdese que al tener conocimiento de la denuncia la entidad denunciada, procedió por iniciativa propia a dirigirse a Google para que se eliminara la URL donde se reproducían la Revista y el artículo, a solicitar a sus colaboradores que suprimieran cualquier nombre de sus artículos o cualquier otra información susceptible de parecer*

*dato personal y que revisaran las citas del área privada de la web para borrar cualquier otro dato sensible, y, por último, a revisar la configuración de los accesos para que los buscadores no tuvieran acceso a las Revistas.*

*En consecuencia, si la Agencia Española de Protección de Datos estimaba adoptadas ya las medidas correctoras pertinentes en el caso, como ocurrió, tal y como expresa la resolución recurrida, la actuación administrativa procedente en Derecho era al archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, pues así se deduce de la correcta interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.*

*Por el contrario, la resolución administrativa recurrida procedió a "apercibir" a la entidad PYB ENTERPRISES S.L., aunque sin imponerle la obligación de adoptar medida correctora alguna, lo que solo puede ser interpretado como la imposición de un "apercibimiento", entendido bien como amonestación, es decir, como sanción, o bien como un mero requerimiento sin objeto. En el primer caso nos hallaríamos ante la imposición de una sanción no prevista en la LOPD, con manifiesta infracción de los principios de legalidad y tipicidad en materia sancionadora, previstos en los artículos 127 y 129 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en el segundo supuesto ante un acto de contenido imposible, nulo de pleno derecho, de conformidad con lo previsto en el artículo 62.1.c) de la misma Ley…>>*

Debe señalarse que, si bien los hechos denunciados serían identificados como contrarios a la LOPD, lo anterior conllevaría el inicio de un Procedimiento de Apercibimiento al responsable, por infracción en materia de protección de datos, no es menos cierto que dicho procedimiento tiene como objeto la reparación de la infracción producida, mediante la propuesta de medidas correctoras sobre los hechos denunciados, estando ante correcciones que, de hecho, no se pueden exigir al haberlas realizado ya, y que harían innecesario el desarrollo del referido procedimiento, en la medida en que, tal y como se desprende de la documentación aportada.

Ha de ponerse de manifiesto, por tanto, que dado que la potestad administrativa con la que cuenta esta Agencia tiene una dimensión reparadora más allá de las capacidades sancionadoras que integran sus competencias en materia de protección de datos, y dado que nos encontramos ante una situación en la que se produjo la falta de una concreta medida de seguridad que ya ha sido reparada, sería contrario a los principios de intervención mínima y de proporcionalidad, como principios que informan el ejercicio de la potestad sancionadora, el iniciar el citado procedimiento de apercibimiento por los hechos denunciados, dado que éste tiene como objeto la reparación de la situación contraria a la LOPD, hecho que ya se ha producido de antemano, de ahí que, al haberse reparado la situación controvertida, no quepa en el presente caso activar el citado procedimiento.

Por lo tanto, de acuerdo con lo señalado,

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

**SE ACUERDA:**

**PROCEDER AL ARCHIVO** de las presentes actuaciones.

**NOTIFICAR** la presente Resolución a ALTANIA DEL MAR, S.L., 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 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 este 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