Expediente Nº: E/01361/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad AIXA CORPORE, S.L., y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de marzo de 2018, la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación con la finalidad de determinar si los tratamientos de datos personales que realiza la entidad AIXA CORPORE, S.L., cumplen con lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personal.

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 fechas 24 y 25 de abril de 2018 se realizaron visitas de inspección en los locales de la entidad AIXA CORPORE, S.L., en el transcurso de las cuales se puso de manifiesto lo siguiente:

   1.1. AIXA CORPORE, S.L., es una empresa que se creó en el año 2004, especializada en el Derecho de las Tecnologías de la Información y la Comunicación, Compliance y Normas ISO.

   1.2. La sociedad es responsable de un total de ocho ficheros con datos de carácter personal; no obstante, el fichero denominado “VIDEOVIGILANCIA”, a pesar de haber sido inscrito en el Registro General de Protección de Datos, no tiene contenido puesto que finalmente no se llegó a realizar la instalación de videocámaras.

   1.3. La sociedad cuenta con un total de 9 trabajadores, aunque tienen clientes en diferentes puntos de España, cuenta con una única sede ubicada en los locales donde se realizó la inspección, en ***LOC.1 (Santa Cruz de Tenerife).

   1.4. Los datos que se tratan en la Sociedad, corresponden a empresas, representantes de empresas, autónomos, personas físicas, trabajadores, etc… a las que se ha prestado algún servicio o que han solicitado información sobre los servicios que ofertan, o bien que prestan servicio como trabajadores de la entidad. Todos los datos que se tratan son de nivel básico, excepto los que contiene el fichero de usuarios de la web, que se ha declarado como de nivel medio en previsión de que se pudiera hacer algún tratamiento en el futuro con dichos datos y que según la nueva normativa de protección de datos, necesitara disponer de especiales medidas de seguridad.

   1.5. La sociedad es titular de la página web ***WEB.1, a través de la cual ofrece sus servicios y recaba datos de las personas interesadas en ellos. En relación con la citada página web, recibieron un escrito de la Agencia, con fecha de

registro de salida 16 de marzo de 2018, en el que se les requería para que cesaran en la utilización del nombre de la Agencia en dicha página.

Con fecha 22 de marzo de 2018, la empresa dio contestación al mismo en el que informaban de la retirada inmediata de toda referencia a la Agencia de Protección de Datos en su página web, que pudiera dar lugar a malas interpretaciones.

1.6. Todos los ficheros de los que son Responsables, se alojan en un servidor propio situado en la oficina donde se realizó la inspección excepto los siguientes ficheros:

Gestión Fiscal y Contable y Personal y Nóminas, que se encuentran externalizados, en la empresa XXX Asesores, con quien tienen firmado un contrato de prestación de servicios de Asesoría.

Usuarios web, el cual se encuentra en los servidores de la empresa Grupo Loading System, S.L., ubicados en Alicante.

1.7. Con relación a la página web y a los datos que se recaban a través de la misma, y que son incorporados al fichero “Usuarios web”, la empresa ha suscrito un contrato de prestación de servicios de hosting (alojamiento) y correo electrónico con la empresa Loading System, S.L. Se adjuntó contrato.

1.8. También se encuentran alojados en los servidores de Loading System, S.L., los datos incluidos a través de la plataforma denominada “área privada” en la que se gestionan los datos de los clientes (empresas o autónomos), que han suscrito un contrato con AIXA CORPORE, para los servicios de adecuación a la normativa de protección de datos. Los datos que contiene son datos identificativos del cliente: nombre y apellidos, DNI, dirección, correo electrónico, teléfono y próximamente tienen previsto recoger también el dato de la dirección IP de conexión.

1.9. A los clientes se les facilita un usuario y una contraseña para que accedan al área privada. La primera contraseña se le asigna y se les indica que deben cambiarla en el primer acceso.

1.10. Además, para el desarrollo de la citada web, posicionamiento de la web y marketing on-line: Google Adwords (Google ofrece la posibilidad de anunciar la empresa destacándola en los resultados de búsqueda sin que suponga en ningún caso remitir información a los usuarios), la empresa ha suscrito un contrato de prestación de servicios con la entidad C.B. SMEDIALAB, de fecha 5 de febrero de 2018. Acompañaron contrato.

1.11. Las personas interesadas en obtener información sobre los servicios que presta la empresa, pueden facilitar sus datos personales a través de los formularios existentes en la página web de la entidad o mediante el envío de correos electrónicos. La citada página, cuenta con diferentes leyendas informativas con relación al tratamiento de los datos que se recaban mediante los formularios disponibles en ella.

1.12. Los datos que se facilitan en los citados formularios: nombre y apellidos, empresa, teléfono y correo electrónico, se reciben en la empresa a través de correo electrónico, en el buzón ***EMAIL.1. Con los datos recibidos del usuario, se da respuesta, bien por teléfono o por correo electrónico. Los

correos electrónicos que se reciben y no vuelven a contactar con la empresa, se eliminan, aunque la página solo está activa desde el 18 de enero de 2018.

1.13. Las direcciones de correo electrónico no se utilizan para el envío de información sobre la empresa, solo se utilizan para la relación con los clientes. Aunque la empresa no realiza ninguna acción de marketing directo, en la información que se facilitaba hasta la fecha de la inspección, en las páginas web, se informa sobre esta posibilidad, para el caso de que en el futuro se decidiera realizar este tratamiento. No obstante, la leyenda informativa se modificó en el transcurso de la inspección. Se adjunta la leyenda informativa antigua y la misma actualizada con fecha de 24 de abril de 2018.

1.14. En la actualidad la empresa cuenta con una cartera de 1500 clientes, entre los que se encuentran organismos públicos, empresas privadas y profesionales autónomos, prestando los siguientes servicios:

Consultoría, Auditoría y Formación a los clientes. Entre la formación que se imparte se encuentra la referida a la normativa de protección de datos y estándares de seguridad en el ámbito público y empresarial, así como asesoramiento jurídico en los sectores especificados en el apartado 2.1 del presente Acta de inspección.

1.15. Con respecto a la formación: el servicio se presta únicamente a sus clientes; no obstante, en algunos casos la representante de la sociedad ha acudido como profesora a dar algún curso o charla sobre normativa de protección de datos. En ningún caso se recaban los datos de los alumnos. Tienen prevista la realización de cursos de formación a través de la Plataforma de formación (Aplicativo Moodle), alojada también en los servidores de la empresa Grupo Loading System, S.L., que en la actualidad no se encuentra activa. En este caso sí recogerán datos de los alumnos, que serán incorporados al fichero ALUMNOS, notificado al Registro General de Protección de Datos.

1.16. Respecto a la POLITICA DE PRIVACIDAD:

En la leyenda informativa que se incluía en la página web hasta su modificación el día 24 de abril, se comunica la denominación del fichero donde se incluye la información y datos de contacto y la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y la dirección del responsable.

También se informa de que los datos se recogen: al rellenar el formulario de contacto en el que se marcan los datos obligatorios: nombre, empresa y correo electrónico, y también se recogen datos de los usuarios, al usar la plataforma a través de cookies propias o de terceros, como Google Analytics o Google Maps.

Con relación a la finalidad del tratamiento de los datos, informan que:

Al rellenar el cuestionario o remitir un correo a AIXA CORPORE, S.L., solicitando información, autoriza a utilizar y tratar los datos personales suministrados para el mantenimiento de la relación y tramitar la solicitud realizada.

Según se informa: los datos serán cedidos a las entidades colaboradoras, cuando sea necesario para la tramitación de los servicios solicitados.

> Asimismo, el titular mediante la presente cláusula de protección de datos presta su consentimiento expreso a AIXA CORPORE, S.L., para que utilice sus datos para el envío de ofertas y promociones propias y de terceros del sector que puedan ser de su interés, por el medio que estime más oportuno, incluidos medios electrónicos. Si prefiere no recibir ofertas nuestras o de nuestros socios, le ofreceremos a través de los mismos la posibilidad de ejercer su derecho de cancelación y renuncia a la recepción de estos mensajes, en conformidad con el art. 22 de la Ley 34/2002 de Servicios para la Sociedad de la Información y Comercio Electrónico.

Los representantes de la entidad manifiestan que aunque en la leyenda informativa se hace referencia a cesiones y al tratamiento de los datos con fines publicitarios, no se ha realizado ninguna cesión de los datos de los clientes o usuarios, ni se tiene previsto realizarla y que tampoco se han utilizado los datos de los clientes ni de los usuarios de la web para realizar ninguna acción de marketing y que tal como se ha indicado anteriormente dicha leyenda ha sido modificada.

Con relación a la Confidencialidad de los datos y medidas de seguridad se informa que:

> AIXA CORPORE, S.L., garantiza la adopción de las medidas oportunas para asegurar el tratamiento confidencial de los datos, establecidas en el RD 1720/2007, de 26 de diciembre por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Daos de Carácter Personal.

Respecto a la nueva leyenda informativa disponible en la página web desde el día 24 de abril de 2018, se han suprimido las referencias al tratamiento de los datos con fines publicitarios y a las cesiones de datos a entidades colaboradoras según se informaba en la leyenda antigua.

2. Las inspectoras de la Agencia solicitan a la representante de la sociedad que les muestre el documento de seguridad de la empresa, teniendo acceso a la última versión del mismo que se ha modificado con fecha 23 de abril de 2018, en el que se detallan las medidas de seguridad implementadas por la sociedad, entre otras:

   2.1. Acceso a datos mediante dispositivos portátiles (trabajo fuera de los locales): en el que se especifica que solo podrán usar dispositivos portátiles las personas autorizadas debiendo adoptar medidas de seguridad idénticas a las adoptadas en equipos fijos. Se detalla el procedimiento para solicitar autorización: mediante un impreso anexo al documento “Autorizaciones de salidas de soportes, dispositivos portátiles y de acceso remoto”, el documento debe ser aprobado por parte de la dirección y se comunica la decisión al peticionario por parte del Responsable de Seguridad mediante el modelo anexo al documento, por último se archivan los documentos utilizados en el procedimiento y se registra en una hoja denominada “usuarios del sistema”.

   2.2. Gestión de usuarios y contraseñas: Solo la dirección o el Responsable de Seguridad puede dar de alta usuarios y asociarles perfiles de acceso. El usuario debe tener como mínimo cuatro caracteres y no se pueden reutilizar. La contraseña debe cambiarse al menos una vez al año y se almacenan de forma ininteligible siendo solo accesibles por el responsable de seguridad.

   2.3. Control de acceso: Los usuarios solo tienen acceso a los datos necesarios para el desarrollo de sus funciones. En el anexo “usuarios del sistema” se

detalla la relación de usuarios con acceso autorizado y en el anexo “perfiles de usuarios” se detallan los permisos concedidos a cada usuario.

2.4. Gestión de soportes y documentos: La empresa mantiene una relación de entradas y salidas de los mismos.

2.5. Copias de seguridad: se refleja el procedimiento en el anexo “copias de seguridad”, se hacen diariamente.

2.6. Registro de Incidencias: recoge por escrito todas aquellas incidencias de seguridad que afecten directa o indirectamente a los datos de carácter personal que se tratan. Se ha difundido una circular de información interna al personal para que sean conocedores de la obligación de comunicar las incidencias en materia de seguridad al responsable de seguridad (anexo XI).

3. Mediante acceso al sistema informático, se realizan las siguientes comprobaciones:

3.1. Se accede al buzón de correo electrónico ***EMAIL.1, verificando que en su bandeja de entrada constan cuatro correos electrónicos con el asunto “contacto desde la web”, el más antiguo de fecha 17 de abril de 2018. La representante de la empresa manifiesta que los correos que recibe en este buzón los reenvía al comercial para que se ponga en contacto con los solicitantes y que se borran del buzón de administración.

Se accede al buzón de correo electrónico del comercial, verificando que en su bandeja de entrada existen 6 correos con el asunto “contacto desde la web”, siendo el más antiguo de fecha 18 de abril. El comercial manifiesta que elimina los correos recibidos en un plazo de entre 7 y 10 días, una vez contactado el solicitante.

3.2. Se accede a la plataforma web denominada “área privada” con el usuario y contraseña del administrador, verificando que se accede a un menú principal con diferentes opciones, entre las que se encuentra la gestión de los usuarios en la que se pueden dar de alta nuevos usuarios, según manifiestan las contraseñas tienen que ser como mínimo de 8 caracteres y contener letras y números, gestión de clientes y también dispone de un “registro de accesos” donde pueden auditar los accesos realizados por los clientes, también dispone de una opción de papelera donde se pueden ver los documentos que han sido eliminados por todos los clientes.

A continuación se accede a la misma plataforma con el usuario y contraseña de un cliente (la empresa inspeccionada), verificando que en el menú principal aparecen las mismas opciones, sin embargo en algunas de ellas como en la gestión de usuarios y clientes, solo pueden gestionar los usuarios propios de ese cliente y ver su información, en el registro de accesos solo puede ver los accesos realizados por el mismo, también dispone de la opción de papelera, donde solo se puede ver los documentos eliminados por ese cliente.

3.3. Se accede a la aplicación que gestiona los ficheros de la empresa, mediante el usuario y contraseña del administrador verificando que se accede a un menú principal con diez opciones, entre las que se encuentran: fichero de clientes, comerciales, administración e incidencias. Desde la opción de clientes se pueden dar de alta nuevos clientes y modificar los datos de los existentes así como darlos de baja.

A continuación se accede a la misma aplicación con el usuario y contraseña de un usuario, verificando que las opciones de administración y consultoría no están accesibles.

4. Las inspectoras de la agencia comprueban que en la oficina donde se realiza la inspección hay cuatro armarios metálicos cerrados con llave, donde se guardan los expedientes y documentos en papel de los clientes, tres de ellos contienen una carpeta por cada uno de los clientes en activo y el cuarto contiene una carpeta por cada cliente dado de baja, además de expedientes del personal que ha sido dado de baja. Esta documentación se conserva durante cinco años desde la fecha de baja procediendo a su destrucción posteriormente.
5. Se verifica la existencia en el local, de una trituradora de documentos.
6. Se comprueba que no existe instalación de un sistema de video vigilancia.

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).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) 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."

III

Durante la inspección efectuada en los locales de Aixa Corpore se ha comprobado el cumplimiento de la normativa de protección de datos. En relación a la información recabada de los afectados hay que señalar que el artículo 5 de la LOPD recoge lo siguiente:

"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

…2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

La obligación que impone este artículo 5 es, por tanto, la de informar al afectado en la recogida de datos, pues sólo así queda garantizado el derecho del mismo a tener una apropiada información y a consentir o no el tratamiento, en función de aquélla.

Así, de acuerdo con lo establecido en el artículo 5 transcrito, la entidad Aixa debe informar a los interesados de los que recabe datos sobre los extremos establecidos en el aludido artículo 5.1. La información a la que se refiere el artículo 5.1 de la LOPD debe suministrarse a los afectados previamente a la solicitud de sus datos personales, y deberá ser expresa, precisa e inequívoca.

En el apartado de Política de Privacidad de la entidad Aixa, se indica quien es el responsable del tratamiento de los datos; para qué se utilizan sus datos personales; cual es la legitimación para el tratamiento de los datos; posibles cesiones de datos; derechos que le asisten y cómo ejercitarlos; en qué momento se recogen los datos, edad para consentir…; cuanto tiempo se conservarán los datos; seguridad de los datos; necesidad de cuenta y contraseña; y posibilidad de enlaces a otros sitios web.

La amplia cláusula informativa cumple lo establecido en el artículo 5 de la LOPD e incluye obligaciones establecidas en el Reglamento Europeo de Protección de Datos.

IV

Referente a los ficheros de datos de los que es responsable la entidad Aixa Corpore, el artículo 26.1 de la LOPD, que bajo la rúbrica "*Notificación e inscripción registral*" establece:

"*1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos."*

Dicho precepto debe ponerse en relación con lo dispuesto en el artículo 55.2 del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que dispone sobre la "*Notificación de ficheros*" lo siguiente:

"*Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el*

procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos."

En el presente caso, ha quedado acreditado que la entidad inspeccionada cuenta con ocho ficheros inscritos relativos a los clientes, proveedores, trabajadores, solicitantes de información, y gestión fiscal y contable, inscritos en el Registro General de Protección de Datos.

V

En relación a las medidas de seguridad, 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 transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son los accesos que la Ley pretende evitar, exigiendo las pertinentes medidas de seguridad, es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

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

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Sintetizando las previsiones legales citadas 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, regulado en normas reglamentarias.

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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, 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*".

Por su parte el artículo 81.1 del mismo Reglamento 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.

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, las Inspectoras de Datos comprobaron el documento de seguridad de Aixa Corpore en el que se detallan las medidas de seguridad implementadas por la sociedad, comprobando, entre otras, lo referente a accesos a datos mediante dispositivos portátiles, gestión de usuarios y contraseñas, control de accesos, gestión de soportes y documentos, copias de seguridad y registro de incidencias.

Asimismo, verificaron que en los locales hay una trituradora de documentos y cuatro armarios metálicos cerrados con llave en los que se guardan expedientes de clientes.

VI

Aixa Corpore tiene suscritos distintos contratos de prestación de servicios con tres empresas: XXX Asesores, Grupo Loading System, S.L., y C.B. Smedialab.

El artículo 12 de la LOPD, habilita el acceso de terceros a los datos personales cuando éste se efectúe para prestar un servicio al responsable del fichero o del tratamiento. Así, bajo la rúbrica *"Acceso a los datos por cuenta de terceros"* establece:

"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." (El subrayado es de la AEPD)

En definitiva, el artículo 12.1 de la LOPD permite que la persona o entidad que presta un servicio al responsable del fichero acceda a datos de carácter personal sin que este acceso se considere, por imperativo legal, una cesión o comunicación de datos.

Las investigaciones llevadas a cabo por la Subdirección de Inspección de Datos han permitido comprobar que Aixa Corpore ha suscrito contratos de Prestación de Servicios con tres entidades y que en el marco de dicho contrato se facilitan los datos de los empleados y clientes.

VII

Por último, y acerca del tratamiento de los datos que efectúa, el artículo 6.1 de la LOPD, señala lo siguiente: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".*

El apartado 2 del mismo artículo añade que "*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 sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11, (Fundamento Jurídico 7, primer párrafo) *"... 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 (...)".

Son pues elementos característicos 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.

Para que dicho tratamiento de datos realizado por Aixa Corpore resultara conforme con los preceptos de la LOPD, debía concurrir alguno de los supuestos contemplados en el artículo 6 de la dicha norma. En el presente caso, ha quedado acreditado que los datos tratados por la entidad son de clientes, proveedores y trabajadores, no siendo preciso su consentimiento para el tratamiento de sus datos con finalidades relacionadas con tal relación laboral o contractual.

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 AIXA CORPORE, 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 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