- **Expediente N.º: EXP202317476**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento a través de varias reclamaciones recibidas entre el 1 de octubre y el 6 de noviembre de 2023 de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos.

Asimismo, PROCONO, en su condición de responsable del tratamiento, comunicó en esta Agencia que había sufrido una brecha de datos personales el día 2 de octubre de 2023.

En su notificación de la brecha a esta Agencia y a los afectados informaba que "*El día 29 de septiembre de 2023 a las 14:00h se sufrió un ataque en los servidores de almacenaje de datos personales de alrededor de 130.000 clientes",* y que dichos servidores pertenecen a la empresa BEKKOS SERVICIOS WEB, marca empleada por ALIVEROBOTIC TECHNOLOGY CB con NIF E27877232 (en adelante ALIVEROBOTIC).

Los hechos que se han investigado en este expediente están relacionados con ALIVEROBOTIC TECHNOLOGY CB con NIF E27877232.

SEGUNDO: Los reclamantes manifestaban ser clientes de (...), (marca de PROCONO S.A.U., en adelante PROCONO) entidad que había sufrido una brecha de seguridad, como ha reconocido públicamente en un comunicado fechado a 2/10/23 y fue notificada a esta AEPD. Los hechos que ponen en conocimiento de esta AEPD son los siguientes:

-Con fecha 1 de octubre de 2023, se ha recibido escrito de la parte reclamante 1, que manifiesta ser un cliente de (...), comunicando que dicha entidad ha sufrido en fecha 30 de septiembre de 2023 una brecha de datos personales, como ha reconocido públicamente en un comunicado fechado a 2/10/23.

Indica que los datos obtenidos a consecuencia de la brecha están expuestos en un foro.

Añade que desconoce los datos que almacenaba, pero que se trata de datos relacionados con clientes, y que puede tratarse de nombre completo, dirección y correo electrónico, y posiblemente cuenta bancaria.

-Con fecha 2 de octubre de 2023 se ha recibido escrito de la parte reclamante 2, en el que manifiesta que “en internet están todos mis datos de usuario de la empresa (...), que parece que ha sufrido un hackeo y no ha comunicado que sus datos, DNI teléfono, dirección, iban entre otros, están en internet.

Junto al escrito, se aporta un fichero (…) que, según manifiesta contienen sus propios datos personales y han sido extraídos de las bases de datos publicadas por el atacante.

-Con fecha 3 de octubre de 2023 se ha recibido escrito de la parte reclamante 3 y, en el que manifiesta que se ha producido una filtración de sus datos bancarios relativos a su cuenta corriente personal y/o tarjeta asociada, y que ha sido notificado de la existencia de una brecha de datos personales en la que sus datos personales y bancarios se han visto comprometidos y publicados en una web para su comercialización.

En su reclamación hace referencia a un link a la noticia, y a la web en la que estarían alojados los datos personales.

Asimismo, aporta la comunicación que habría recibido de (...), en el que se le informa de la existencia de la brecha, que está fechada el día 2 de octubre de 2023.

-Con fecha 3 de octubre de 2023 se ha recibido un escrito de la parte reclamante 4, en el que pone de manifiesto que ha recibido un correo por parte de PTV, compañía de internet, en el que se le comunica que ha sufrido una brecha de datos personales y que han sustraído información sensible como nombre, DNI, iban, entre otros.

Adjunta a su reclamación el contenido de dicho correo electrónico.

- Con fecha 3 de octubre de 2023 se ha recibido un escrito de la parte reclamante 5, en el que pone de manifiesto que a (...) le han hackeado los servidores y se han apoderado de datos como nombres, dirección, DNI, cuentas bancarias de los abonados, y que ha resultado afectado.
Añade que la entidad le ha comunicado los hechos con un email, señalando que sus datos personales se han visto afectados.

Adjunta a su reclamación una captura de pantalla con el contenido del correo electrónico que ha recibido, en el que se comunican los hechos.

-Con fecha 3 de octubre de 2023 se ha recibido un escrito de la parte reclamante 6, en el que comunica que quiere presentar una reclamación formal contra la empresa PROCONO, S.A., que ha tenido una brecha de datos personales por hacking y por la que existen más de 110mil datos de clientes por internet, entre los cuales es muy posible que se encuentren los suyos, así como de familiares, porque han recibido una comunicación de la entidad, y solicita que se abra una investigación.

Adjunta a su reclamación copia del correo electrónico enviado por la empresa, en el que se le comunican los hechos que reclama.

-Con fecha 4 de octubre de 2023 se recibe un escrito de FACUA mediante el que quiere presentar denuncia contra PROCONO, S.A., ((...)), al haber tenido conocimiento de que ha sufrido una brecha de datos personales que ha permitido la exposición de datos personales de miles de usuarios sin autorización.

FACUA manifiesta que los clientes que han suscrito el contrato de forma presencial han visto sus datos publicados en un archivo en una página web externa, de forma que los internautas han podido descargarlo y obtener información sensible.
Añade que los datos filtrados son nombre y apellidos, domicilio, fecha de nacimiento, número de teléfono y dirección de correo electrónico.

Asimismo, indica que los clientes que contrataron a distancia han visto comprometidos además el DNI y el número de cuenta bancaria.

Por último, indica que también se han visto afectados datos de personas que, sin ser cliente, habrían contactado con la compañía para obtener información de sus servicios.

Adjunta a su denuncia una impresión de pantalla en la que se recoge la noticia.

-Con fecha 4 de octubre de 2023 se ha recibido un escrito de la parte reclamante 7, en el que comunica haber recibido un correo electrónico de la entidad (...), en el que se le informa de que han sufrido un ataque y han quedado expuestos los datos de más de 100.000 clientes, entre los que se encuentran los suyos. Indica que los datos afectados son nombre, dirección, DNI, nacionalidad, IBAN de cuenta bancaria, y correo electrónico.

-Con fecha 4 de octubre de 2023 se ha recibido escrito de la parte reclamante 8 en el que informa que la empresa PROCONO S.A., ha sufrido un ataque, y como consecuencia han detectado un acceso no autorizado a su base de datos. Los datos que se han visto afectados son nombre y apellidos, dirección postal, teléfono, correo electrónico, DNI, fecha de nacimiento, nacionalidad, IBAN del número de cuenta.
Añade que ha tenido conocimiento de los hechos porque ha recibido un correo electrónico de la entidad comunicándolo.

Adjunta a su reclamación copia del correo electrónico recibido.

-Con fecha 4 de octubre de 2023 se ha recibido un escrito de la parte reclamante 9 en el que pone de manifiesto que ha tenido conocimiento de que el pasado día 30 de septiembre se habría producido una filtración de datos de los clientes de (...). Como era cliente, tras haberse hecho públicas las bases de datos de los clientes, ha revisado si sus datos estarían expuestos, como así había ocurrido.

Junto al escrito, se aporta un fichero que, según manifiesta contienen sus propios datos personales y han sido extraídos de las bases de datos publicadas por el atacante.

-Con fecha 5 de octubre de 2023 se ha recibido un escrito de la parte reclamante 10 en el que pone de manifiesto que el día 2 de octubre de 2023 ha recibido una comunicación de la entidad PROCONO S.A.U., en el que se le notifica que ha tenido una brecha de datos personales por la que unos desconocidos habrían robado 6 de sus bases de datos, entre los que se encuentran sus datos personales: nombre y apellidos, dirección postal, teléfono, correo electrónico, DNI, fecha de nacimiento, nacionalidad, IBAN.
Añade que, navegando por internet, ha encontrado dichas bases de datos publicadas en una web dedicada a la venta de información.

Adjunta a su reclamación el email que ha recibido de la entidad.

-Con fecha 13 de octubre de 2023 se ha recibido un escrito de la parte reclamante 11, en el que pone de manifiesto que ha recibido un correo electrónico de la compañía (...), en el que se le informa de que la entidad ha sufrido un acceso no autorizado a sus sistemas de almacenaje de datos, mediante el cual puede haber sido afectada información concerniente a su persona como nombre y apellidos, dirección postal, teléfono, correo electrónico, número de DNI, fecha de nacimiento y nacionalidad.

Añade que ha visto noticias que indicarían que los datos personales se habrían publicado en plataformas piratas en las que se ofrece esta información para usos fraudulentos.

-Con fecha 30 de octubre de 2023 se ha recibido un escrito de la parte reclamante 12 en el que pone de manifiesto que ha recibido un correo electrónico de la compañía (...) en el que le comunican que han tenido un acceso no autorizado a sus sistemas de datos de carácter personal y que puede haberse visto afectada información concerniente a su persona.
Indica que le han comunicado que los datos que se han visto afectados de su persona son correo electrónico, información importante de seguridad, DNI, y solicita que se dicte acuerdo de inicio de expediente sancionador.

Adjunta a su reclamación copia del correo electrónico que ha recibido de la entidad.

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a ALIVEROBOTIC, entidad en la que, de acuerdo con la información recibida, se habría producido la brecha de datos personales, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 1 de diciembre de 2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 1 de diciembre de 2023 se recibe en esta Agencia escrito de respuesta indicando que el día 30 de septiembre de 2023 se abrió ticket por el cliente PROCONO indicando que no tienen acceso a algunas de sus bases de datos. Desde

ALIVEROBOTIC se comunica que el sistema de vigilancia no detecta ninguna alarma y se comprueba que el servidor privado virtual está online, sin problemas aparentes por lo que se responde que el servidor se encuentra bien y que no se observa ninguna incidencia. Insisten a través de WhatsApp, de que tienen un problema, por lo que el técnico se conecta al servidor y se comprueba que efectivamente ha sido así.

ALIVEROBOTIC prosigue manifestando que dispone de medidas técnicas de seguridad suficientes, y que no se detectan indicios de ataque a sus servidores, sino que, tras realizarse las actuaciones correspondientes, "*se concluye que el problema de seguridad es ajeno a Bekkos Servicios Web (AliveRobotic Technology) y recae en los sistemas de* PROCONO S.A*.".*

CUARTO: Con fecha 7 de enero de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las reclamaciones presentadas.

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

PROCONO manifestó que el ataque se produjo "*en los servidores de almacenaje de datos personales, perteneciendo dichos servidores a Bekkos Servicios Web*".

ALIVEROBOTIC manifestaba en su escrito de contestación al traslado que solamente proporciona a PROCONO servicios de alojamiento, y que no realiza otros tratamientos para la misma.

PROCONO aportó en su escrito de fecha 30 de abril de 2024 un "CONTRATO DE TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS […]" con ALIVEROBOTIC, en el que se designa a la primera como responsable del tratamiento, y a la segunda como encargada; los expositivos y estipulaciones del contrato mencionan solamente servicios de alojamiento de datos.

PROCONO proporcionó en fecha 2 de enero y 30 de abril de 2024 dos registros de actividades de tratamiento (RAT), en ninguno de los cuales se menciona a ALIVEROBOTIC ni a su marca (Bekkos) como encargado de tratamiento.

En su escrito de contestación al traslado, ALIVEROBOTIC manifestaba:

> "*[…] El día 30/09/2023 - 09:54, nos abre ticket el cliente* PROCONO S.A. *indicando que no tienen acceso algunas de sus bases de datos, nuestro sistema de vigilancia no detecta ninguna alarma y se comprueba que el Servidor privado virtual esta online, sin problemas aparentes por lo que se responde que el servidor se encuentra bien y no observamos ninguna incidencia. Insisten a través de Whatsapp, de que tienen un problema, por lo que el técnico se conecta al servidor y comprueba que efectivamente ha sido así.*"

Asimismo, ALIVEROBOTIC manifiesta en su escrito de contestación al traslado que dispone de medidas técnicas de seguridad suficientes, y que no detectaron indicios de ataque a sus servidores, sino que, tras realizarse las actuaciones correspondientes, "*se concluye que el problema de seguridad es ajeno a Bekkos Servicios Web (AliveRobotic Technology) y recae en los sistemas de* PROCONO S.A.*"*.

Adicionalmente, ALIVEROBOTIC proporciona copia de los tiques de atención a PROCONO durante la brecha y que menciona en su respuesta.

Por otro lado, PROCONO ha proporcionado un informe en su escrito de fecha 30 de abril de 2024, que tiene fecha de 29 de abril de 2024, y que ha sido encargado a la empresa ******EMPRESA.1***, del que se infiere que la incidencia se habría producido en PROCONO.

En concreto, se pone de manifiesto la ausencia de medidas que hubiese permitido detectar que se estaba produciendo la incidencia, así como la existencia de prácticas que habrían permitido la materialización del ataque.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra

su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

III
Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

IV
Conclusión

En las actuaciones de investigación desarrolladas se ha analizado la relación de ALIVEROBOTIC con la brecha de datos personales comunicada por PROCONO S.A.U. (titular de la marca ***(...)***) como responsable de tratamiento y respecto de la que se manifestaba que la brecha se produjo en los servidores de ALIVEROBOTIC, que actuaba como encargado del tratamiento.

PROCONO ha aportado un contrato en el que se indica que ALIVEROBOTIC actuaba como encargado del tratamiento, de fecha 5 de diciembre de 2020. No obstante, los expositivos y estipulaciones de ese contrato, así como las manifestaciones de ALIVEROBOTIC, refieren solamente a servicios de alojamiento de datos. Los RAT aportados por PROCONO no mencionan a ALIVEROBOTIC como encargado de tratamiento.

ALIVEROBOTIC, en su escrito de contestación al traslado, ha manifestado que, tras realizarse las actuaciones correspondientes, *se concluye que el problema de seguridad es ajeno a Bekkos Servicios Web (AliveRobotic Technology) y recae en los sistemas de* PROCONO S.A.*"*.

Por otro lado, del estudio forense de la brecha proporcionado por PROCONO se concluye que el incidente se produjo en sus sistemas y que el mismo habría venido motivado por una deficiente actuación achacable a dicha entidad.

De todo lo anterior se concluye que no se han hallado evidencias de responsabilidad por parte de ALIVEROBOTIC en relación con la brecha y, por lo tanto, no existen indicios de que se haya producido una vulneración del RGPD por dicha entidad.

En nuestro Derecho Administrativo sancionador, es plenamente vigente el principio de presunción de inocencia reconocido en el artículo 24.2 de la Constitución Española, de modo que el ejercicio de la potestad sancionadora del Estado, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. El principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

El Tribunal Constitucional (SSTC 131/2003 y 242/2005, por todas) se ha pronunciado en ese sentido al indicar que una de las exigencias inherentes al derecho a la presunción de inocencia es que la sanción esté fundada en actos o medios probatorios de cargo o incriminadores de la conducta imputada y que recae sobre la Administración pública actuante la carga probatoria de la comisión del ilícito administrativo y de la participación en él del denunciado.

Por su parte, el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece como uno de los principios de la potestad sancionadora el de la "Responsabilidad" y determina al respecto que:

"*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa*".

Igualmente, se debe tener en cuenta lo que establece el artículo 53.2 la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el cual establece que:

"*Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables, tendrán los siguientes derechos: (…)*

> *b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario".*

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos, por lo que procede el archivo de la reclamación en relación con la investigación realizada a ALIVEROBOTIC.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

De acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ALIVEROBOTIC TECHNOLOGY CB y a las partes reclamantes.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez sea firme en vía administrativa.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia 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 de la referida Ley.

940-120525

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos