Procedimiento Nº: E/08205/2019
940-0419

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por PROMOFARMA ECOM S.L (en adelante PROMOFARMA) en el que informan a la Agencia Española de Protección de Datos haberse enterado por publicación periodística en la red social *Twitter* que la base de datos de usuarios registrados en la entidad había sido obtenida por un hacker y comercializada a través de la *deep web*.

Indican que la quiebra se inició el 06/08/2019. En primer lugar, estimaron 2.950.000 afectados, considerando tras la investigación un total de 1.300.000. Con respecto a la tipología de los datos, estos son básicos y de contacto de clientes y usuarios de la web de la entidad.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 9 de agosto de 2019.

ENTIDADES INVESTIGADAS

PROMOFARMA ECOM S.L con NIF B65130122 con domicilio en AV DIAGONAL Num.534 P.6 PTA.2 - 08029 Barcelona (BARCELONA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- HECHOS. La entidad informa de la siguiente cronología de hechos:

PRIMERO.- PROMOFARMA, con fecha 6 de agosto de 2019 y hacía las 17:30 horas, tuvo constancia de una noticia publicada en un medio extranjero relativa a una supuesta venta ilícita de una base de datos correspondiente a sus clientes. Inmediatamente después de realizar una primera comprobación acerca de la veracidad de dicha noticia, PROMOFARMA, activó el protocolo de seguridad establecido en el Procedimiento relativo a la gestión de incidencias y violaciones de seguridad de datos personales (en lo sucesivo Quiebra de seguridad) y, de forma paralela, comenzó la investigación de un supuesto ciberataque a través del contacto directo con el autor de la noticia, especializado en seguridad de la información.

SEGUNDO.- Tras un intercambio de mensajes a través de correo electrónico y de la red social *Twitter*, el autor de la noticia facilitó una captura de pantalla que mostraba un

ejemplo de 17 registros supuestamente filtrados a través del ciberataque, cuya tipología de datos es la siguiente:

- Nombre completo.
- Teléfono.
- Correo electrónico.
- Dirección postal.
- Contraseña cifrada mediante algoritmo seguro.

TERCERO.- El departamento de seguridad de la información de PROMOFARMA contrastó la información obtenida con la existente en la base de datos de la compañía y, de forma preliminar, llegó a la conclusión de que los registros de la captura de pantalla facilitada por el autor de la noticia podían constituir indicios de una potencial brecha de seguridad de confidencialidad, ascendiendo en un primer instante el número de afectados potenciales detectados a alrededor de 2.6 millones, siendo éste el número máximo de registros de la base de datos en ese momento. No obstante, tras una investigación posterior, se llegó a la conclusión de que el número de los registros supuestamente afectados es de 1.3 millones, habida cuenta de la existencia de múltiples registros atribuidos a un mismo usuario.

PROMOFARMA no ha podido tener acceso al contenido de la base de datos supuestamente robada.

CUARTO.- Como resultado de lo anterior, y aún sin poder afirmar con total certeza el ámbito de interesados afectados por falta de información concluyente, PROMOFARMA, actuando con prudencia y en el interés de sus usuarios, optó por tomar como referencia el más grave de los escenarios posibles y consideró como tratamientos afectados todos aquellos que involucrasen datos de carácter personal de sus clientes, potenciales clientes y proveedores, resultando en cerca de 1.3 millones de registros mencionado con anterioridad, conteniendo los siguientes datos: nombre, apellidos, teléfono, correo electrónico, dirección postal y contraseñas cifradas de acceso a PROMOFARMA.

QUINTO.- El día 9 de agosto de 2019 ante los indicios del posible ataque se presentó de forma preventiva la correspondiente notificación ante la AEPD y, de forma paralela, una denuncia al Juzgado de Guardia de Barcelona, solicitando la investigación ulterior de los acontecimientos por parte de la Policía Judicial, constitutivos de un delito tipificado en el artículo 278 del Código Penal, de descubrimiento y revelación de secretos de empresa.

SEXTO.- El mismo 9 de agosto de 2019, incluso sin poder contrastar la veracidad del robo de datos de carácter personal y teniendo en cuenta que las contraseñas supuestamente filtradas estaban debidamente cifradas, PROMOFARMA, de forma preventiva y como una de las acciones tomadas con objeto de minimizar los efectos adversos del supuesto ciberataque, fuerza un reseteo de contraseñas a todos los usuarios hacía las 20.00 horas, obligando así, a todos los usuarios de PROMOFARMA, a modificar su contraseña de acceso por otra diferente.

Adicionalmente, se comunicó al Consejo de Administración de la entidad matriz de PROMOFARMA, los detalles conocidos en el momento sobre la supuesta brecha de seguridad, así como sobre el hecho de la presentación de la notificación de la brecha ante la AEPD y la correspondiente denuncia al Juzgado de Guardia de Barcelona.

Como medida adicional para aminorar los efectos de la potencial brecha de seguridad, PROMOFARMA aumentó el tipo de algoritmo usado para cifrar la información de la base de datos, lo que reduce aún más, el riesgo de descifrado de la información.

SÉPTIMO.- El 14 de agosto, sobre las 19.50 horas, PROMOFARMA lanzó una comunicación vía correo electrónico a los usuarios potencialmente afectados en relación al supuesto ciberataque.

OCTAVO.- En línea con lo anterior, debido al hecho de que las contraseñas de los usuarios supuestamente afectados estaban cifradas en el momento de producirse el ataque, y a que PROMOFARMA procedió al pronto reseteo de dichas contraseñas, así como al cambio del algoritmo de cifrado de las contraseñas a uno de los más robustos actualmente existentes en el mercado, es escasamente probable que los usuarios puedan llegar a sufrir alguna consecuencia del ciberataque, salvo la obligatoriedad de creación de una nueva contraseña en su próximo inicio de sesión.

En este sentido, y a modo de evidencia de la inexistencia de secuelas negativas derivadas de la supuesta brecha, hasta la fecha de la presentación de este escrito no se han detectado utilizaciones fraudulentas de los datos accedidos, y ningún usuario se ha puesto en contacto con la organización para reclamar o poner en conocimiento algún aspecto relacionado con los hechos.

2.- MEDIDAS PREEXISTENTES:

PROMOFARMA, ha llevado a cabo una adecuación al RGPD en la que implementó un sistema de gestión de Gobierno, Riesgos y Cumplimiento de la citada normativa, realizándose por la entidad la identificación, revisión y adecuación de los tratamientos de la entidad en los que había implicados datos de carácter personal.

Como resultado de dicho proceso de adecuación al RGPD, elaboró una serie de documentos que conforman el sistema de gestión de la organización, que se encuentra compuesto, entre otros por los siguientes elementos:

- Registro de actividades de tratamiento realizadas por PROMOFARMA;
- Análisis de riesgos previos de todos y cada uno de los tratamientos de datos realizados por PROMOFARMA;
- Cláusulas informativas a los interesados y de legitimación de cada tratamiento;
- Modelos de contratos para regularizar la relación con terceros que tienen acceso, incluso potencial, a datos de carácter personalidad responsabilidad de PROMOFARMA;
- Inventario de empleados con acceso al sistema de información para realizar los tratamientos de datos personales, así como evaluación de cumplimiento de las medidas de seguridad efectivamente implantadas;
- Realización de diferentes evaluaciones de impacto relativas a la protección de datos de tratamientos calificados con un riesgo alto a los derechos y libertades de los interesados;

Y procedimientos relativos, entre otros, a:

- Protección de datos desde el diseño y por defecto.
- Deber de información y obtención y revocación del consentimiento.
- Altas y bajas de usuarios y gestión de contraseñas.
- Selección y contratación de personal.
- Control de acceso a las instalaciones.
- Encriptación y cifrado.
- Definición y asignación de roles y responsabilidades en el tratamiento de datos.
- Comunicaciones y cesiones de datos a terceros.
- Contratación de terceros con acceso a datos.
- Ejercicio y atención a los derechos de los interesados.
- Notificación y gestión de incidencias y violaciones de seguridad.
- Evaluación del riesgo inherente y del impacto en la privacidad.
- Identificación y regularización de transferencias internacionales.
- Destrucción y conservación de datos.

PROMOFARMA ha aportado copia del Registro de actividades de tratamiento de la compañía, con los tratamientos afectados por la brecha de seguridad. El Registro de actividades de tratamiento incluye el Análisis de los Riesgos de cada uno de los tratamientos. La metodología utilizada para la determinación de los riesgos de tratamientos se describe en el Procedimiento de evaluación del riesgo inherente y del impacto en la privacidad del que también aportan copia.

Los representantes de la entidad indican que de la valoración de los riesgos de tratamientos derivó la necesidad de realizar determinadas Evaluaciones de Impacto sobre la Protección de Datos (EIPD) de una serie de tratamientos, adjuntando cinco EIPD. También, en el proceso de adecuación al RGPD se llevó a cabo un inventario de sistemas de información (software, bases de datos, etc.), cuya copia aportan, asociándose y evaluándose a cada uno de éstos el cumplimiento de las correspondientes medidas de seguridad tomando en consideración las medidas de seguridad recomendadas por los siguientes estándares y guías de referencia:

- ISO/IEC 27001:2017.
- ISO/IEC 27002:2013.

- “Handbook on Security of Personal Data Processing” publicada por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Del mismo modo, debe tenerse en cuenta que la plataforma online de PROMOFARMA se encuentra almacenada en los servidores de alojamiento externos con la que PROMOFARMA mantiene un contrato de encargado de tratamiento de datos cuya copia aportan.

La información de PROMOFARMA se encuentra alojada en los nodos ubicados dentro del Espacio Económico de la Unión Europea (EEE) cuyas medidas de seguridad, tanto físicas, como lógicas se encuentran ampliamente descritas en el documento denominado “White Paper Security” cuya copia aportan en la que se destaca que el servidor de alojamiento cumple con la práctica totalidad de estándares de seguridad de la información existentes a nivel mundial.

PROMOFARMA tiene implementado, como parte importante de su sistema de gestión de cumplimiento, un Procedimiento relativo a la notificación y gestión de incidencias y violaciones de seguridad que se adjunta al presente escrito como ANEXO VIII, respecto al cual puede verificarse por parte de la AEPD que PROMOFARMA da cumplimiento íntegro a los requisitos establecidos por el RGPD, al mismo tiempo que éste fue aplicado y cumplido de forma íntegra por la compañía.

3.- MEDIDAS POSTERIORES A LA BRECHA:

Además de las medidas ya indicadas en la cronología de hechos, consistentes en el forzado del reseteo de las contraseñas de los usuarios, presentación de la notificación de la brecha a esta Agencia, denuncia al Juzgado de Guardia de Barcelona y mejora del algoritmo de cifrado, PROMOFARMA ha aportado un Informe Técnico con la identificación de todas y cada una de las medidas implantadas con posterioridad a la brecha de seguridad, así como la indicación de medidas de seguridad planificadas o en proceso de implantación.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 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 Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra de seguridad) como “todas aquellas violaciones de la seguridad que ocasionen 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."

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el posible acceso de datos personales por terceros, como consecuencia del acceso indebido a la base de datos de clientes y usuarios como consecuencia de un ataque externo y posteriormente puesta en comercio en la *Deep web*.

No obstante, también consta que PROMOFARMA, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado y en especial el cifrado y encriptado de contraseñas, lo que ha permitido la detección, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorase la adopción de medidas técnicas y de gestión, como es la contratación de un sistema de cifrado más robusto y denuncia ante el Juzgado de Guardia de Barcelona al objeto de minimizar futuros riesgos similares y mejorar la calidad de las aplicaciones de gestión de datos personales de la que es responsable.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***PROMOFARMA ECOM S.L*** con NIF ***B65130122*** y con domicilio en ***AV DIAGONAL Num.534 P.6 PTA.2 - 08029 Barcelona (BARCELONA)***

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

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 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 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos