- **Procedimiento Nº: E/08809/2019**

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 investigación se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por JONES DAY en representación de CAFEPRESS INC. (en adelante CAFEPRESS) en el que informan a la Agencia Española de Protección de Datos haberse enterado por fuentes externas que su base de datos de clientes había sido puesta a la venta en la "*dark web*", un conjunto de un total de 22 millones de registros. Tras investigar el caso determinaron que una tercera persona no identificada obtuvo, sin autorización, la base de datos de clientes de CAFEPRESS.
CAFEPRESS señala que la notificación se ha realizado tan pronto como han tenido resultado del análisis forense que confirma el número de afectados en España.

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 notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 10 de septiembre de 2019

ENTIDADES INVESTIGADAS

CAFEPRESS.1909, Shelbyville Road, Lousville, KY 40243, U.S.A.

elysonge@cafepress.com

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- HECHOS:

Cronología de hechos:

- Medios externos y clientes han reportado a la entidad que registros de datos de clientes de CAFEPRESS se han visto comprometido. CAFEPRESS descubre el 6 de agosto de 2019 que dos conjuntos de registros de datos de clientes estaban disponibles a la venta en la *"dark web",* unos 22 millones de registros en total de los cuales 1.060.000 son afectados de la Unión Europea y unos 17.792 de España.
- En una tabla aportada por CAFEPRESS con el desglose de afectados en Europa se aprecia que el mayor número de afectados se encuentra en Reino Unido, con 880.309 afectados, del total en Europa de un millón aproximadamente.

Se ha buscado la incidencia en el sistema de monitorización europeo con relación a la entidad CAFEPRESS, encontrando un registro en curso relativo a art. 56 del RGPD, abierto por Países Bajos.

La Autoridad de Control del Reino Unido (en adelante ICO) no se considera Autoridad de Control principal (LSA) para el caso, con base en que CAFEPRESS ha manifestado no disponer de establecimiento en la Unión Europea, pero está sujeto al Reglamento General de Protección de Datos conforme lo dispuesto en el art 3.2.a) del RGPD, en especial y respecto al U.K. a través de la web "*Cafepress.co.uk"*, por lo que ha notificado la brecha a todas las autoridades Europeas de Protección de Datos relevantes para el caso.

En respuesta a las notificaciones, algunas Autoridades de Control se han considerado interesadas (como procedimiento local, no transfronterizo) al no disponer CAFEPRESS de establecimiento en la Unión Europea con base en la afectación del incidente a sus nacionales, y otras no.

- Las categorías de datos afectados por la brecha son datos básicos y de contacto, datos identificativos como nombres de usuario y contraseñas y, solo en algunos casos, datos económico-financieros tales como información de tarjetas de crédito (cuatro últimos números y fecha de caducidad).

  Para 15 afectados de la Unión Europea se han visto comprometidos datos tales como números de identificación fiscal o equivalentes, pero ninguno de ellos de España.

- CAFEPRESS ha recibido unas 80 solicitudes de información de afectados de la Unión Europea relacionadas con el caso, pero ninguna en la que se manifieste haber sufrido daños por el incidente.

- Por todo ello CAFEPRESS considera que la probabilidad de que los afectados experimenten consecuencias significativas es neutral para las 15 personas cuyos identificadores fiscales se vieron comprometidos, e improbable para el resto.

2.- MEDIDAS PREEXISTENTES:

CAFEPRESS ha aportado copia del Registro de Actividades de Tratamiento (RAT) en el que figuran los tratamientos comprometidos (gestión de cuentas de miembros, pagos, gestión de los miembros, etc…).

CAFEPRESS indica que no trata categorías especiales de datos u otros datos sensibles a gran escala, por lo que no ha llevado a cabo una EIPD. Sí aporta copia del Análisis de Riesgo (AR) de los tratamientos.

En el AR consta considerado el riesgo de acceso ilegítimo por terceras personas, considerado con una severidad "limitada".

Constaban medidas de seguridad como Hashing para las contraseñas de los usuarios, segmentación de red, cifrado de credenciales en tránsito, política de claves robustas para empleados, firewalls perimetrales, controles de acceso físicos, formación anual en seguridad para los empleados, y protección con software antivirus. Existe otro grupo de medidas adicionales implementadas para mitigar riesgos relacionadas la

mayoría con la migración a otros servidores en julio de 2019 de las tablas de registros de clientes.

3.- MEDIDAS POSTERIORES A LA BRECHA:

La entidad ha declarado haber notificado la brecha a todas las autoridades de control de protección de datos europeas relevantes para el caso. Informa que reportó el incidente A Reino Unido (ICO) el 8 de agosto, dos días después de la determinación de la brecha. Manifiesta haber notificado al resto de las Autoridades de Control de la Unión Europea tan pronto determinó el número de afectados de cada país.

CAFEPRESS inició a raíz del incidente una investigación utilizando expertos forenses externos. No han sido capaces de confirmar que la información de los clientes haya sido obtenida de su base de datos, ya que los logs que registran el tráfico en tiempo real no reflejan el incidente.

CAFEPRESS ha contactado y está cooperando con el FBI de Estados Unidos, y ha dado varios pasos para mejorar la seguridad de sus sistemas

CAFEPRESS manifiesta haber notificado por correo electrónico a todos los afectados comenzando el 4 de septiembre de 2019, siguiendo el contenido requerido por el art. 34 del Reglamento General de Protección de Datos y en particular, especificando información de contacto que los afectados pueden usar para cualquier gestión relacionada con el incidente. También colocó un cartel notificando el incidente en su página web.

En el tiempo que la incidencia ocurrió, CAFEPRESS estaba en un proceso de borrado de datos personales de la base de datos como parte de una estrategia de largo plazo que incluía el traslado de la base de datos a otro entorno. Ahora los números identificativos tales como identificadores fiscales han sido suprimidos donde ha sido posible, o cifrados. Así mismo, a las contraseñas se les aplica un hash de 128 bits. En Julio de 2019, antes de ser conscientes de la brecha de seguridad, la base de datos se movió a un entorno distinto, con medidas de seguridad que siguen estándares industriales.

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 una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad, como consecuencia del acceso indebido por terceros ajenos a la base de datos del sistema de información de CAFEPRESS.

No consta que CAFEPRESS disponga de establecimiento en Europa pero, sin embargo, dispone de web en U.K., motivo por el que en virtud de lo dispuesto en el art 3.2.a) del RGPD ha procedido a notificar la brecha de seguridad a todas las Autoridades de Control Europeas tal y como ya se ha indicado. Dichas Autoridades de Control han concluido que el incidente no se corresponde con la ventanilla única por lo que será tratado como un tratamiento de impacto local en su caso. En relación con la intervención de la AEPD, se debe señalar que le compete la investigación al resultar afectados ciudadanos españoles, si bien como tratamiento de impacto local.

De las actuaciones de investigación se desprende que el CAFEPRESS disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, el CAFEPRESS disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación del supuesto incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la supuesta incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación. También ha interpuesto denuncia ante el FBI (USA).

En consecuencia, el CAFEPRESS disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada causada previsiblemente por un error puntual.

III

Por lo tanto, en el caso concreto consta que la actuación de CAFEPRESS 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 CAFEPRESS.1909, Shelbyville Road, Lousville, KY 40243, U.S.A., email: elysonge@cafepress.com

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