Procedimiento Nº: E/07029/2019
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 violación de seguridad de datos personales (en adelante quiebra de seguridad) remitido por *4FINANCE SPAIN FINANCIAL SERVICES, S.A.U. (*en adelante *4FINANCE)* en el que informan a la Agencia Española de Protección de Datos que han tenido conocimiento, a través de *EXPERIAN BUREAU DE CRÉDITO, S.A.* (en adelante Experian) e una brecha de seguridad producida el 21 de junio 2019. La brecha consistió en que *Experian,* empresa encargada del tratamiento, envió cartas con información de clientes de 4FINANCE a clientes de otras entidades, y a los clientes de 4FINANCE enviaron cartas con información de clientes de otras entidades.

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: 12 de julio de 2019

ENTIDADES INVESTIGADAS

4FINANCE SPAIN FINANCIAL SERVICES, S.A.U. (4FINANCE) con NIF A86521309 con domicilio en C/ GÉNOVA 27, PLANTA 2ª - 28004 MADRID (MADRID)

EXPERIAN BUREAU DE CRÉDITO, S.A. con NIF A82120601 con domicilio en C/ PRINCIPE DE VERGARA, 132, 1º PLANTA - 28002 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1 Con fecha 31 de julio de 2019 se solicita por la inspección de datos información a 4FINANCE en relación con la incidencia de seguridad comunicada, teniendo entrada con fecha 14 de agosto de 2019 escrito de dicha entidad en el que pone de manifiesto lo siguiente:

1.1. 4FINANCE aporta copia de la política de seguridad de la empresa y del procedimiento de actuación ante una brecha de seguridad.

1.2. Aportan copia del escrito emitido por Experian, como encargada del tratamiento de los datos de los clientes de 4FINANCE, en el que informan sobre las causas de la incidencia y acciones tomadas con objeto de minimizar los efectos adversos.

En relación con las causas que han dado lugar a la brecha de seguridad

1.3. Experian, en calidad de encargado del tratamiento de la entidad 4FINANCE, presta el servicio de envío y gestión de requerimientos de pago (en adelante RPP), para que ésta pueda requerir el pago a sus deudores. Las cartas se envían siguiendo el modelo proporcionado por el cliente, y se incluyen en ella, el logotipo y nombre y diseño gráfico propio de la entidad.

1.4. La incidencia ha sido causada por un error en el proceso de impresión por parte del proveedor de impresión subcontratado por Experian, la compañía mercantil IMPRE-LASER S.L.. En concreto, la incidencia fue causada por una avería que tuvo la impresora que estaba prevista para realizar el trabajo de impresión relativa a la carga del día 11 de junio, necesitando de asistencia técnica. En el momento de la impresión, se generó de nuevo el fichero de impresión para otra impresora disponible, utilizando un nuevo *driver* para fijar todos los parámetros, y esto produjo un error que causó que el anverso/reverso no coincidiese. Por tanto, el impacto de esta incidencia se reduce a que un particular ha podido conocer los datos contenidos en la comunicación de un RPP de otro particular.

Respecto a las acciones tomadas con objeto de minimizar los efectos adversos

1.5. Experian, tras conocer la incidencia y su impacto, activó un comité de crisis interno para poder actuar con la mayor celeridad, así como impedir que los particulares afectados, en ningún caso, se vieran afectados por una inclusión posterior en los sistemas de información crediticia de los que son responsables.

1.6. El día 20 de junio se realizó la oportuna comunicación a la entidad 4FINANCE, explicando la incidencia y el total de afectados impactados. Se propuso a la entidad un plan de actuación que incluía el volver a enviar al interesado el RPP correcto correspondiente a la carga del 11 de junio y se incluía asimismo, que (i) se expresa que lamentamos lo ocurrido, (ii) se indica la incidencia ocurrida y que los datos recibidos en la anterior comunicación no eran correctos, (iii) se solicita a los destinatarios que destruyan la comunicación previa, (iv) se procede a comunicar la deuda correcta, y (v) con el fin de evitar cualquier duda de los destinatarios, se incluye un número de teléfono de Experian disponible para la atención de cualquier duda de los destinatarios.

1.7. Se ha revisado el proceso de impresión con el fin de implementar verificaciones adicionales a las ya existentes (como era la verificación de muestras diarias del fichero) con el fin de reforzar aún más los procedimientos y controles aplicados hasta el momento.

1.8. El equipo de Operaciones de Experian procedió a la anulación de los RPPs generados en sus sistemas relativos a la carga afectada por la incidencia de impresión. Dicha actuación por parte de Experian tiene la finalidad de evitar cualquier vulneración de los derechos de los interesados, evitando la inclusión en sus ficheros de información crediticia por el envío de las notificaciones afectadas por la incidencia.

Respecto a las acciones realizadas para la resolución final de la incidencia

1.9. Las medidas implementadas para la resolución final de la incidencia y evitar que la misma vuelva a producirse, se han implementado con eficacia efectiva desde el 20/06/2019.

1.10. Cambios en el *driver* de las impresoras asignadas a los procesos de impresión.

1.11. Comprobaciones en cada proceso de impresión, en intervalos determinados fijos de las notificaciones que garantizan que el proceso de impresión es correcto.

Cuando esté terminado y validado el proceso de impresión, las notificaciones pasan a la zona de manipulado, donde la persona que realiza el *complet,* ensobrado, etc. vuelve a realizar comprobaciones para garantizar que el proceso es correcto.

Ya antes de la incidencia, Experian realizaba validaciones de muestras de las notificaciones para garantizar que el procesamiento del fichero por parte del proveedor de impresión era correcto. Para reforzar aún más los controles y que Experian tenga certeza de los mismos se van a realizar validaciones de muestras aleatorias tras la impresión de las notificaciones, es decir, sobre muestras ya impresas.

1.12. Experian no tiene conocimiento de que los destinatarios de los RPPs hayan utilizado los datos de terceros obtenidos a través de la brecha de seguridad, además es muy improbable que lo hagan por el tipo de datos personales comunicados.

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 acceso a los datos personales de los afectados por terceros como consecuencia del envío de notificaciones erróneas por parte del encargado del tratamiento.

No obstante, también consta que tanto el responsable del tratamiento (4FINANCE como el encargado del mismo Experian, disponías de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido la detección, identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante el mismo 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 (Responsable y Encargado del tratamiento).

También debe valorase la adopción de medidas técnicas y de gestión, como es la inclusión de controles aleatorios tras la impresión de los RRP a todos los sistemas de información afectados al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

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 y la entidad encargada de la gestión 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:

- ***4FINANCE SPAIN FINANCIAL SERVICES, S.A.U. (4FINANCE)*** con NIF ***A86521309*** y con domicilio en ***C/ GÉNOVA 27, PLANTA 2ª - 28004 MADRID (MADRID).***

- ***EXPERIAN BUREAU DE CRÉDITO, S.A.*** con NIF ***A82120601*** y con domicilio en ***C/ PRINCIPE DE VERGARA, 132, 1º PLANTA - 28002 MADRID (MADRID).***

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