- **Procedimiento Nº: E/11114/2020**

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 brecha de seguridad de los datos personales remitido por BANCO MEDIOLANUM, S.A. (en adelante Banco Mediolanum o entidad investigada) en el que informan a la Agencia Española de Protección de Datos que la Auditoria interna de seguridad informática de la entidad ha detectado que la *App* del Banco contenía la agenda de contactos de un usuario en el código fuente y que existía la posibilidad de acceso a estos datos utilizando métodos sofisticados de descompilación.

Los datos que contenía la citada agenda del usuario corresponden a nombre del contacto, teléfono y dirección de mail y en un caso datos de código de dos tarjetas de crédito y de una cuenta bancaria.

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 la brecha de seguridad de datos personales: 6 de noviembre de 2019.

ENTIDADES INVESTIGADAS

BANCO MEDIOLANUM, S.A. con NIF A58640582 y con domicilio en Avenida Diagonal 668, 08034 Barcelona.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 27 de noviembre de 2019 se solicitó información al Banco Mediolanum y de la respuesta recibida se desprende lo siguiente:

   Respecto de la entidad investigada.

   - Banco Mediolanum pone a disposición de los clientes la figura de *Family Banker* (profesional para la gestión de los recursos financieros).
   - Banco Mediolanum tiene suscrito un contrato de prestación de servicio de mantenimiento de la App con EVERIS SPAIN, S.L.U. de fecha 18 de agosto de 2017. A este respecto, la entidad bancaria ha aportado contrato suscrito al efecto.

Respecto del servicio BIZUM.

- El servicio BIZUM permite a los clientes solicitar y enviar dinero a terceros mediante una *App* sin necesidad de conocer los datos bancarios del tercero. El único dato necesario para realizar una operación BIZUM es el número de teléfono móvil.

  El cliente ordenante accede a la *App* y selecciona la opción de pago del servicio BIZUM que va a realizar (enviar o solicitar dinero) e introduce el número de teléfono móvil de la persona sobre la que se realizará el servicio.

  Para facilitar la operativa se ofrece al cliente la posibilidad de acceder a la agenda de contactos de su propio teléfono móvil para aportar el número de teléfono del tercero.

- El responsable del servicio BIZUM es Sociedad de Procedimiento de Pago, S.L., y se encuentra adherida a varias entidades bancarias, siendo una de ellas Banco Mediolanum la cual ofrece este servicio a través de su propia *App*. En la web del Banco Mediolanum figura "*Para empezar a usarlo descárgate la app Banco Mediolanum y activa el servicio dentro de la aplicación con tu número móvil y la cuenta bancaria que tu elijas*".

Respecto de la incidencia detectada y comunicada a la Agencia

- Un *Family Banker* comunicó a Banco Mediolanum que no podía utilizar el servicio BIZUM con la *App* del móvil al no reconocer un contacto de su agenda.

  Tras realizar diversas verificaciones se vio la necesidad de acceder a la agenda de contactos del móvil con la finalidad de identificar el motivo de la incidencia comprobando que la agenda contenía caracteres no reconocibles y que la *App* no identificaba al intentar utilizar el servicio BIZUM. Esta incidencia no está relacionada con un acceso indebido a ningún dato.

  Una vez finalizadas las comprobaciones, en el mes de junio de 2019, por un error de la entidad encargada del mantenimiento (EVERIS SPAIN) no se eliminó la lista de contactos telefónicos del *Family Banker* que se había incrustado en el código fuente de la *App* durante las comprobaciones de la incidencia reportada.

- El 4 de noviembre de 2019, la Auditoria interna de seguridad informática del Banco al ejecutar los controles previstos, entre ellos, un proceso de descompilación (proceso por el cual se traduce el código fuente de un programa) de la *App* del Banco detectó que una lista de contactos se había "quedado indebidamente incrustada" en el código fuente de la *App*.

  La Auditoria concluyó que había un riesgo identificado ya que existía una posibilidad de acceso a dicha lista de contactos mediante el uso de técnicas avanzadas de *descompilación* de *Apps.*

  Nada más detectarlo, se procedió a comunicar la incidencia a la entidad EVERIS SPAIN, S.L.U., encargada del mantenimiento de App.

- Con fecha 6 de noviembre de 2019 se procedió a notificar la brecha de seguridad a la Agencia Española de Protección de Datos con el incidente ya solucionado.
- Banco Mediolanum manifiesta que esta incidencia ha sido un tema puntual ya que en los controles anteriormente realizados nunca se había presentado datos incrustados en el código fuente de la *App*.

Medidas de minimización del impacto de la brecha

- El 4 de noviembre se contactó con la empresa encargada del mantenimiento de la *App* para que eliminará la información indebidamente incrustada en el código fuente y verificara todo el código fuente de la *App* conforme a la metodología de desarrollo seguro.
- El 6 de noviembre ya estaba modificada y disponible la *App*.

Respecto de los datos afectados.

- La incidencia ha sido sobre un solo usuario (*Family Banker)* y su agenda telefónica que contenía 1419 contactos con el nombre o alias y el número de teléfono. Y en algunos casos apellidos y dirección de mail.

  Como resultado de la Auditoria se comprobó la existencia del nombre-apellidos, código IBAN y dos códigos PAN (número que aparece en el anverso de la tarjeta de pago) de tarjetas bancarias canceladas de un cliente.
- Ningún otro usuario tuvo problemas con la *App* y el servicio BIZUM.
- No se ha realizado ninguna comunicación a posibles afectados ya que se ha evaluado el riesgo con los criterios de:
  - Tipo de violación: El posible acceso a los datos se produjo cuando se descompiló la *App*, no cuando estaba en funcionamiento.
  - Naturaleza y carácter de los datos: Datos de contacto y bancarios.
  - Gravedad de las consecuencias para las personas: Escasa gravedad del impacto potencial (sólo una)
  - Características particulares de las personas.

  La entidad concluyó no comunicar al afectado debido a la escasa gravedad del impacto potencial y la baja probabilidad de que se produjera, con resultado de un nivel de riesgo bajo.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

- Banco Mediolanum manifiesta que con motivo de implantar los nuevos requisitos exigibles en el Reglamento Europeo de Protección de Datos y en aras al cumplimento del principio de responsabilidad proactiva se realizan controles internos y la Auditoria de seguridad de la *App* estaba programada para noviembre de 2019 dentro del Plan Anual de Auditoras de la entidad para detectar posibles riesgos.

  En el Plan Anual de auditorías se revisan, entre otros controles, las informaciones que se generan tras descompilar las *Apps*, por este motivo se detectó el 4 de noviembre el incidente mencionado.

- Banco Mediolanum ha aportado la siguiente documentación:
    - Registro de actividad de tratamiento de Clientes y Gestión de Agentes
    - Evaluación de Impacto y Análisis de Riesgo de la App.
    - Guía de Seguridad del desarrollo
    - Decálogo seguro
    - Actualización del ciclo de vida desarrollo
    - Procedimiento para la notificación de brechas de seguridad

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 brecha 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, la brecha de seguridad notificada a la AEPD por Banco Mediolanum calificada como brecha de confidencialidad al existir la posibilidad de acceso a los a los datos del cliente por terceros ajenos, se debió a un error por parte del encargado del tratamiento cuando procedía a corregir una incidencia puntual a un cliente en relación con el mal funcionamiento del servicio Bizum que facilitaba la aplicación del Banco.

El contenido de la información a la que se podría haber accedido como consecuencia de la brecha de seguridad se refiere a nombre-apellidos, código IBAN y dos códigos PAN (número que aparece en el anverso de la tarjeta de pago) de tarjetas bancarias canceladas de un cliente y teléfonos de los contactos de la agenda del cliente.

Cabe señalar que la brecha de seguridad fue detectada por la Auditoría programada para noviembre de 2019 dentro del Plan Anual de Auditoras de la entidad para detectar

posibles riesgos sobrevenidos. Dos días después de la detección de la brecha de seguridad, ya estaba corregida la *App* y disponible en producción.

No consta que haya habido tratamientos posteriores de los datos del afectado causados por la brecha de seguridad y no constan reclamaciones al respecto ante esta AEPD.

Asimismo, consta que Banco Mediolanum disponía de Registro de actividad de tratamiento de Clientes y Gestión de Agentes, Evaluación de Impacto y Análisis de Riesgo de la App, Guía de Seguridad del desarrollo, Decálogo seguro, Actualización del ciclo de vida desarrollo y Procedimiento para la notificación de brechas de seguridad

En consecuencia, se aprecia un nivel de diligencia proporcional y razonable en la actuación de la entidad investigada como responsable del tratamiento al disponer de medidas técnicas y organizativas de seguridad previas al incidente sobrevenido, así como en la corrección de la disfuncionalidad detectada en la aplicación que ofrecía el servicio de pago Bizum.

Señalar, por último, la necesidad de realizar un informe final tras el seguimiento y cierre sobre la brecha y su impacto. Dicho informe final es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros.

III

Por lo tanto, consta que la actuación de Banco Mediolanum, como responsable del tratamiento, ha sido diligente y proporcional con la normativa sobre protección de datos personales analizada en los párrafos anteriores al detectar, minimizar el impacto y corregir la brecha de seguridad notificada.

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 BANCO MEDIOLANUM, S.A. con NIF A58640582 y con domicilio en Avenida Diagonal 668, 08034 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