Procedimiento Nº: E/08448/2019
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: Con fecha 31/08/2019 la entidad CAIXABANK, S.A., notificó a esta Agencia una incidencia de seguridad consistente el envío por error de un correo electrónico con múltiples destinatarios sin copia oculta, de tal forma que los receptores pudieron visualizar las direcciones de correo electrónico del resto de destinatarios.

SEGUNDO: Con fecha 10/09/2019, la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación instando a la Subdirección General de Inspección de Datos a que proceda 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 del incidente de seguridad: 27/08/2019

Fecha de comunicación a los afectados: 27/08/2019

Fecha de la notificación del incidente de seguridad: 31/08/2019

ENTIDADES INVESTIGADAS

CAIXABANK, S.A. con NIF A08663619 con domicilio en C/ PINTOR SOROLLA 2-4 - 46002 VALENCIA (VALENCIA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto a los hechos

CAIXABANK, S.A. (en adelante CAIXABANK) ha comunicado a esta Agencia lo siguiente:

"En uno de los trámites habituales para la recuperación de préstamos hipotecarios impagados con antigüedad de 0 a 30 días, el envío de correos electrónicos solicitando el abono de las cuotas pendientes, se cometió un error en el envío de correos del día 27/08/19. En un envío concreto se incluyeron las direcciones de correo electrónico en

el campo para, en lugar de en el campo CCO (copia oculta). Esto motivo que los clientes pudieran ver las direcciones de otros clientes. El texto del correo era genérico, y no incluía información personalizada. El mismo día se envió un correo electrónico de disculpa a todas las direcciones afectadas."

Comunican un total de 398 afectados.

Se ha solicitado a CAIXABANK copia del correo electrónico remitido que dio origen a la brecha de seguridad (correo enviado sin copia oculta), comprobándose que el texto incluido en el mismo consiste en un reclamo de regularización de pago relacionado con un préstamo hipotecario refinanciado por CAIXABANK, no apareciendo en el texto del mensaje datos identificativos de la operación crediticia ni sobre su titular.

Se ha solicitado también a CAIXABANK el listado de los clientes afectados y las direcciones de correo electrónico que quedaron comprometidas, verificándose que las direcciones de correo en ocasiones incluyen nombre, y/o primer apellido, y/o segundo apellido, o una combinación de iniciales y datos de nombre o apellidos, y en muy pocos casos nombre y dos apellidos completos del cliente. En otras ocasiones, la dirección de correo no incluye estos datos del cliente, componiéndose de otros literales no descriptivos de la identidad de la persona.

El correo electrónico fue remitido por IT CORPORATE SOLUTIONS SPAIN, SL (en adelante DXC), en virtud del contrato de prestación de servicios de recobro hipotecario suscrito al efecto.

Cinco de los afectados se pusieron en contacto con la entidad manifestando entender lesionados sus derechos con relación a la protección de sus datos personales. Realizadas búsquedas en el sistema de información de la Subdirección General de Inspección de Datos no se encuentra ninguna reclamación al respecto.

Respecto a las medidas implementadas con anterioridad a la brecha:

CAIXABANK ha aportado copia del **Registro de Actividades de Tratamiento (RAT)**, en el que consta el área de la Entidad en la que figura el tratamiento de datos comprometido (Recuperaciones y Morosidad).

Solicitados el **Análisis de Riesgos** y la **Evaluación de Impacto** que en su caso hayan realizado sobre las actividades de tratamiento involucradas en la brecha de seguridad la entidad ha manifestado lo siguiente:

"Con la entrada en vigor del Reglamento General de Protección de Datos (y por tanto, de la obligación de realizar una Evaluación de Impacto), CaixaBank ha implantado una serie de políticas internas que establecen los criterios y procesos a través de los cuales se llevan a cabo, entre otras cuestiones, las Evaluaciones de Impacto. En este sentido, se ha establecido un plan de trabajo en la Entidad con el objetivo final de realizar una Evaluación de Impacto sobre todas las actividades de tratamiento que se llevan a cabo en la Entidad, priorizando la realización de Evaluaciones de Impacto sobre todas las actividades de tratamiento que se pretenden iniciar, así como respecto de todas las actividades de tratamiento existentes e incluidas en el Registro de Actividades de Tratamiento cuyas características fueran modificadas por cualquier motivo.

En este caso particular, las actividades de tratamiento relacionadas con la recuperación de préstamos no han sufrido ninguna modificación relevante en términos de tipología de datos tratados ni tecnologías intervinientes en los últimos años, por lo que a fecha del incidente todavía no han sido evaluadas.

No obstante, y con ocasión de este incidente, se ha iniciado el proceso de Evaluación de Impacto de la actividad afectada. "

No mencionan el Análisis de Riesgos. No obstante, los representantes de la entidad han indicado que las actividades de tratamiento de datos que se vieron comprometidas se llevaban a cabo con anterioridad a la entrada en vigor del Reglamento General de Protección de Datos y no han sufrido ninguna modificación por lo que no era necesario realizar un Análisis de Riesgos ni una Evaluación de Impacto, y que, no obstante lo anterior, se ha iniciado el proceso para realizar la correspondiente evaluación de impacto.

CAIXABANK ha aportado copia del contrato de prestación de servicios de recobro hipotecario suscrito con DXC, que incluye como cláusula quinta las estipulaciones de protección de datos y seguridad, constando entre otras el compromiso de cumplimiento de las medidas de seguridad así como el de no difundir a terceros los datos personales a que se tenga acceso en el cumplimiento del contrato.

CAIXABANK informa que tienen establecidos, para todas las agencias que colaboran en la prestación del servicio de recobro, una serie de estándares y procesos de actuación que deben regir sus actuaciones para minimizar los riesgos relativos al tratamiento de datos personales. Aportan al efecto el Manual de Gestión Hipotecario que detalla los procedimientos con las agencias colaboradoras para la prestación de los servicios de recobro, así como los protocolos de calidad y la tipología de comunicaciones a realizar. Adicionalmente, los empleados de las agencias colaboradoras asumen una serie de compromisos y estándares en materia de tratamiento de los datos de los clientes que firman de manera individual. Aportan a estos efectos uno de los documentos de adhesión firmado por uno de los empleados que intervienen en la prestación de servicio, que incluye compromiso de confidencialidad.

Respecto a las acciones emprendidas y las medidas implementadas como consecuencia de la brecha:

Los representantes de CAIXABANK han informado que una vez identificada la incidencia, se procedieron a realizar las siguientes acciones inmediatas:

- Se llevó a cabo la comunicación de la incidencia y el envío de un email de disculpa a todos los contratos afectados en la misma fecha de la incidencia;
- Se aplicó la eliminación de los envíos masivos de correos electrónicos por procedimientos manuales;
- Se realizó un recordatorio a las personas del equipo que hasta la fecha se encargaba de realizar las comunicaciones vía email con los clientes.

- Se circuló una comunicación a todo el equipo de gestores para poder informar del hecho y cómo proceder ante cualquier llamada de queja o molestar por parte de algún cliente relacionado con esta incidencia.

Informan así mismo que, sin perjuicio de las acciones inmediatas tomadas en el momento de identificar la incidencia, se ha evaluado el entorno actual de control de las comunicaciones que se dirigen a los clientes y se han implantado las siguientes mejoras:

- Desarrollar una funcionalidad para impedir que en los sistemas (CRM, Buzones, etc.) se puedan incorporar direcciones de mail en el campo “PARA” para envíos masivos.

- Implementar el envío automatizado individualizado de mails. En este sentido, las pruebas de implementación de esta funcionalidad se ejecutaron con éxito a fecha 26 de septiembre de 2019 y se encuentra implantada y en funcionamiento a fecha de la contestación de la entidad a esta Agencia. Aportan documentación gráfica del funcionamiento de la funcionalidad que incluye evidencias de la eliminación de la opción “copia oculta” de los buzones de envío y de del proceso disponible para el envío que implica generar un fichero con todas las direcciones de correo a las que enviar la comunicación.

Finalmente, indican que, en consecuencia, se ha procedido a eliminar del protocolo y procedimiento de recobro los envíos masivos de correos electrónicos.

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 de confidencialidad como consecuencia del envío de un correo electrónico con 398 destinatarios sin copia oculta, informando de la regularización de los préstamos hipotecarios y su refinanciación por CAIXABANK. Dicho texto era genérico y no se incluían datos identificativos de la operación de crédito ni su titular, salvo las direcciones de correo electrónico expuestas.

De las actuaciones de investigación se desprende que CAIXABANK disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias. Estas medidas fueron trasladas a las agencias colaboradoras y trabajadores.

Asimismo, CAIXABANK disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y las agencias colaboradoras en calidad de encargadas, así como el Delegado de Protección de Datos.

Consta también, que con ocasión de la incidencia se ha procedido a realizar la evaluación de impacto sobre los tratamientos afectados e implantar mejoras técnicas y organizativas y eliminar de los procedimientos la posibilidad de envío masivo de correos electrónicos.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que CAIXABANK disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. No obstante se sugiere, a fin de cerrar la brecha de seguridad, se elabore un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. 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, se ha acreditado que la actuación CAIXABANK 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 ***CAIXABANK, S.A. con NIF A08663619, y domicilio en C/ PINTOR SOROLLA 2-4 - 46002 VALENCIA (VALENCIA)***

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