- **Procedimiento Nº: E/09154/2020**

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: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento CACF BANKIA CONSUMER FINANCE EFC S.A con número de registro de entrada O00007128e2000008432 y fecha de registro 30 de octubre de 2020 relativa a envío de datos personales a destinatario incorrecto, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, así como a trasladar al responsable del tratamiento, la orden de la Directora de la AEPD en la que se le insta a comunicar dicha quiebra a los interesados.

TERCERO: Con fecha 26 de noviembre de 2020 tiene entrada en la Agencia Española de Protección de Datos la reclamación interpuesta por ***A.A.A.*** (en adelante, el reclamante). La reclamación se dirige contra CACF BANKIA CONSUMER FINANCE EFC S.A., con NIF A88147053 (en adelante, el reclamado). El motivo en que basa la reclamación es la sustracción de datos personales importantes. Junto a la reclamación, aporta la comunicación cursada por el responsable en cumplimiento de lo ordenado el 4 de noviembre de 2020, por La Directora de la Agencia Española de Protección de Datos.

CUARTO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), con número de referencia E/00621/2021, se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

QUINTO: Con fecha 2 de marzo de 2021, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante. No siendo ésta objeto de investigación, ya que la única documentación que se aporta, es la comunicación a los afectados ordenada por la Directora de la AEPD.

SEXTO: De la realización de actuaciones previas de investigación, se ha tenido conocimiento de los siguientes extremos:
Fecha de notificación de la brecha de seguridad de datos personales: 30/10/2020 (inicial).

ANTECEDENTES
Como resumen del incidente se notifica inicialmente lo siguiente:

“Datos enviados por error al encargado, el cual nos avisa y tras solicitarle su aislamiento y borrado, nos confirma que se realiza correctamente. Actualmente, investigación interna en curso por posible fuga de datos en el transcurso desde que se enviaron hasta que se detectó la incidencia. Posible fuga interna o del encargado. Mantenemos esta brecha abierta para aportar la información que aflore y las medidas que se vayan tomando”.

El Responsable realiza sucesivas actualizaciones de la información de la brecha, comunicando en fecha 01/11/2020:

“Seguimiento de los archivos tras brecha previa, también comunicada a la AEPD, se detecta publicación en la dark web. Una vez comprobados los archivos se decide notificar y activar los planes de contención, así como avisar al encargado del tratamiento”.

La Directora de la Agencia Española de Protección de Datos ordenó la comunicación a los afectados con fecha 4 de noviembre de 2020. Por su parte, el Responsable ha comunicado a esta Agencia, en las actualizaciones de las notificaciones realizadas a esta Agencia, que ha procedido a enviar a los afectados las correspondientes notificaciones para que tengan conocimiento de los hechos y puedan adoptar las medidas que consideren oportunas para evitar aquellos riesgos que pudieran afectar a su persona. Aportan copia de las notificaciones remitidas, cuatro modelos diferentes según el tipo de cliente.

Con fecha 03/03/3021 se ha incorporado al presente expediente de investigación la reclamación presentada por el reclamante en fecha 26/11/2020 ante esta Agencia. En la reclamación pone de manifiesto que ha recibido un correo electrónico de Soyou notificando de la brecha de seguridad acaecida. Aporta copia de la notificación recibida, de fecha 26/11/2020.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:
CACF BANKIA CONSUMER FINANCE EFC S.A. con NIF A88147053 con domicilio en AVDA. MANOTERAS, N.º 44, 2 D - 28050 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN
1.- Con fecha 13/11/2020 se solicitó información al Responsable. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

Información general de la empresa:
Soyou Bankia es la marca de CACF BANKIA CONSUMER FINANCE EFC, S.A. con la que opera en el mercado de financiación al consumo en España. La entidad es fruto de un proyecto conjunto, iniciado en 2018 para llevar a cabo operaciones comerciales cuyo objetivo es ofrecer financiación a los clientes finales.
Opera desde el inicio de 2020 participada por dos entidades financieras, CREDIT AGRICOLE CONSUMER S.A. y BANKIA S.A., que ostentan, respectivamente, el 51 y el 49% de la titularidad de las acciones.

Respecto de la notificación de brecha.

Los representantes del responsable han manifestado que:
“Del día 07 de octubre al día 12 de octubre 2020, Endesa recibe 13 ficheros procedentes del responsable (SoYou), siendo este último día, el 19 de octubre de 2020 que Endesa advierte de que el fichero que está recibiendo no es el correcto.
Con fecha 20 de octubre 2020 y con base en la información disponible en ese momento, se elabora un análisis del incidente por parte de ***EMPRESA.1** como especialistas en la materia y se determina, siguiendo los criterios establecidos por la AEPD en su Guía sobre Gestión de Brechas de Seguridad, que el incidente, con los datos de los que se disponía en ese momento, no era constitutivo de Brecha de Seguridad que hubiese de ser comunicada a la AEPD.
El día 30 de octubre 2020 se detecta la primera publicación y difusión de datos que provenían del fichero afectado por el incidente interno lo que provoca una nueva reevaluación de los hechos y consecuencias.
Esta vez, debido a la difusión en la Dark Web, y ante el riesgo evidente y potencial para los derechos de los afectados, la evaluación del incidente tiene como resultado que estamos ante una Brecha de Seguridad a notificar, tanto a la Autoridad de Control, como a los interesados.
En consecuencia, se realiza la notificación de Brecha de Seguridad ese mismo día 30 de octubre de 2020, es decir, dentro del preceptivo plazo de 72 horas desde que se determinó la categoría de Brecha de Seguridad del incidente.”

Respecto de la cronología de los hechos

Los representantes del Responsable han manifestado que:
“Como consideraciones previas al relato de los hechos, es conveniente explicar que, el fichero afectado por el incidente que da lugar a la brecha de seguridad se encuentra en el sistema denominado "DataLake", donde se almacenan las bases de datos de forma automática, y al que únicamente tienen acceso la Oficina del Dato (en adelante DMO) y algunas personas muy concretas e identificadas del equipo de IT/Sistemas.
Desde este sistema DataLake se pueden hacer diferentes extracciones, en función de las necesidades que surjan, para ser enviadas a otros departamentos o a terceros en el marco de la relación que les una con SoYou. Para realizar este proceso de extracción, se ha de hacer una programación del dato a extraer, siendo el encargado de esta acción el equipo del Datos de Soyou (DMO).
A continuación, se ejecuta por parte del equipo del DataLake del Grupo Credit Agricole y, una vez ejecutado el fichero, éste se genera y se guarda en la carpeta de la infraestructura del Grupo Credit Agricole.

Extracción y envío de datos a Endesa.

En el marco de la relación de negocio que une a SoYou con Endesa (tienen firmado un contrato de colaboración mediante el cual Endesa (en su calidad de colaborador) actúa como miembro de la Red de Distribución de CACF Bankia), se realizan una serie de comunicaciones de datos que requieren la implementación del proceso anteriormente explicado para extraer datos del DataLake.
La modificación para programar la extracción solicitada por Endesa se realiza el 07 de octubre 2020, por parte del Data Engineer (ingeniero de datos) del departamento DMO, que lo realiza como parte de las funciones encomendadas a su puesto y perfil.
Entre los días 07 de octubre y el día 19 de octubre, Endesa recibe 13 comunicaciones.
El día 19 de octubre, la persona de contacto de Endesa avisa a SoYou de que es posible que la información que estén recibiendo no sólo contenga los datos solicitados por Endesa, sino que también contiene datos correspondientes a terceros ajenos a la relación entre ambas Entidades.
Esta alerta es transmitida de inmediato a los equipos de Seguridad e IT de SoYou y se detiene el proceso automático de envío a Endesa como primera medida de todas las que a continuación se enunciarán.

Investigación preliminar.

El mismo día 19 de octubre por la tarde, comienza el proceso de investigación interna para determinar los hechos y las posibles causas del incidente.
En la mañana del día 19 de octubre, el Data Engineer (presunto responsable del envío de las comunicaciones) había comunicado su deseo de abandonar la compañía en fechas próximas. En concreto, la extinción del contrato sería aproximadamente el 2 de noviembre tras el preceptivo preaviso.
Tras una investigación preliminar, el día 20 de octubre, por la mañana, se identifican a las personas que presuntamente podrían haber provocado el envío erróneo a Endesa, entre ellas, el ya mencionado Data Engineer, y otro miembro del equipo de Data.
El día 22 de octubre del 2020, se "invita" al Data Engineer que había presentado su baja voluntaria a no acudir a su puesto de trabajo hasta la extinción de su contrato con SoYou, Además, se procede a comunicar el despido disciplinario por bajo rendimiento del otro miembro del equipo de Data.

Una vez comunicada esta decisión a los interesados, se procede a depositar en custodia interna sus equipos informáticos, quedando éstos bajo llave en espera de analizarlos con todas las garantías en el marco de la investigación abierta.

Proceso de investigación y monitorización de posibles exfiltraciones.

Con el fin de determinar los detalles exactos de lo sucedido, se inicia el proceso de investigación del incidente para determinar la posible voluntariedad del acto (potencial dolosidad) y si fue una acción desde el interior o en algún punto de la comunicación entre SoYou y Endesa.
Asimismo, con el apoyo y asesoramiento de expertos externos (la entidad ******EMPRESA.1***), se realiza una evaluación del incidente de seguridad para si estaríamos ante Brecha de Seguridad susceptible de ser notificada a la Autoridad de Control (la AFPD en este caso) y a los interesados/afectados.
El resultado de la evaluación, que se realiza siguiendo las pautas de la propia AEPD, arroja como resultado que estaríamos ante un incidente interno sin rango de Brecha

de Seguridad, por lo que la gestión del mismo se continua a llevar a cabo de forma interna.
De forma proactiva, si bien se había determinado que el incidente no alcanzaba rango de Brecha de Seguridad y no hay constancia de un acceso desde el exterior, se decide monitorizar los principales foros de la Dark Web con el objeto de chequear si hubiera habido algún tipo de exfiltración voluntaria de estos ficheros, bien sea en el lado de SoYou, bien sea en el lado de Endesa, o bien sea en el proceso de envío automático del fichero mediante un ataque de "Man in the Middle" en el "SFTP seguro".
La noche del 29 al 30 de octubre de 2020 la monitorización genera la primera alerta sobre una posible publicación de los datos afectados en la Dark Web, siendo la de ese día 29 la primera de las seis publicaciones detectadas.
Se analizan las publicaciones en la Dark Web y, junto con la investigación preliminar, se llega a las siguientes conclusiones:
No puede inferirse un ciberataque externo debido al conocimiento exhaustivo de la plataforma. Para poder exfiltrar los ficheros es necesario conocer el funcionamiento exacto del proceso Batch, cómo se ingestan los ficheros en DataLake, así como la manera de extraerlos.
No puede inferirse una fuga de información por parte de Endesa dado que en fecha 27 de octubre se recibe la confirmación por parte de Endesa (Grupo Enel) de la eliminación del archivo y puesto que las filtraciones posteriores nada tienen que ver con Endesa. De igual modo se infiere un conocimiento exhaustivo del contenido de los ficheros puesto que se han publicado los más sensibles para perjudicar a SoYou.
La extracción de los datos se ha producido antes del 22 de octubre. Los datos publicados corresponden a ficheros generados en las siguientes fechas: 17 de octubre (Fichero de Endesa); 1 de octubre (Fichero RIB); 1 de septiembre (Fichero MIR) 0 1 de Septiembre (Fichero ACTTELECOM).

Excluido un ciberataque o acción dolosa de un hacker, se consolida la opción de que estaríamos ante una supuesta acción voluntaria y dolosa llevada a cabo por personal propio de SoYou. Esta teoría se consolida con el estudio de los mensajes que acompañan las publicaciones en la Dark Web y cuyo detalle se puede consultar en el Documento nº5 del presente escrito.
Dada la tipología, ubicación y complejidad del acceso a la información, se consolida la presunta autoría de las personas identificadas al inicio de la investigación, y sobre quienes se toman medidas disciplinarias, cuyas funciones asignadas permitían acceder a la información afectada y que, además, tendrían un claro conocimiento del contenido de los archivos exfiltrados, así como los conocimientos técnicos necesarios para llevar a cabo una acción de tal calibre.

Categorización como Brecha de Seguridad.

En el momento que se detecta la primera publicación de datos (noche del 29 al 30 de octubre) provenientes del fichero afectado en la Dark Web se realiza internamente y con apoyo de ***EMPRESA.1, una segunda evaluación del incidente teniendo en cuenta los nuevos hechos y, dado que la publicación de datos en la Dark Web podía suponer un riesgo potencial para los derechos de los afectados, se declara el incidente como Brecha de Seguridad, procediendo el mismo día que se detecta la publicación, día 30 de octubre de 2020, a comunicarla debidamente ante la AEPD.

Ante la gravedad de la situación, se presenta denuncia ante la Unidad Central de Ciberdelincuencia, Brigada Central de Seguridad Informática, de la Policía Nacional el 2 de noviembre de 2020.
Asimismo, para garantizar la transparencia del proceso de investigación, se contratan los servicios profesionales de ******EMPRESA.2*** para el análisis forense de los dispositivos electrónicos que se aislaron y así poder averiguar si fueron utilizados por los presuntos autores con el objetivo de identificar si, de la información contenida en éstos, se pudiera desprender que hubieran sido utilizados para llevar a cabo la exfiltración de información que posteriormente fue difundida a través de la Dark Web."
Los representantes del Responsable aportan diversa documentación como apoyo de sus manifestaciones, entre la que se encuentra copia de tres actas notariales, denuncia interpuesta ante la Unidad Central de Ciberdelincuencia, Brigada Central de Seguridad Informática, de la Policía Nacional, y cuatro informes técnicos sobre el incidente elaborados por el equipo de ciberseguridad del Responsable, ******EMPRESA.3, ***EMPRESA.2 y ***EMPRESA.1.***
Los datos fueron publicados en un foro de la dark web por primera vez en la madrugada del 29 al 30/10/2020, el día 3/11/2020 aparece en el blog del mismo foro un mensaje sin nuevos datos publicados, y se detectaron nuevas publicaciones los días 7, 8 y 13 de noviembre de 2020 en el mismo foro.

Respecto de las causas que hicieron posible la brecha:

Los representantes del Responsable han manifestado que:

"Durante el proceso de modificación para programar la extracción de datos solicitada por Endesa, y que se encuentra en el origen del incidente, la persona encargada de esta acción logra utilizar la vía de comunicación con internet para, presuntamente, extraer una copia de forma totalmente irregular, por lo que habría incumplido flagrantemente así sus obligaciones de confidencialidad y deber de secreto aceptados y firmados al incorporarse a SoYou.
Es de subrayar que esta persona, así como el segundo miembro del equipo de Data que presuntamente participa en los hechos, por el puesto que ocupaba en SoYou, disponían de facultades plenas de acceso a la información real y completa (facultades a las que se añadirían sus extensos conocimientos informáticos) lo que propició que pudieran extraer esa copia y utilizarla posteriormente de forma maliciosa en la Dark Web con el único fin, en opinión de la Compañía, de dañar la reputación de ésta poniendo en riesgo los derechos de los interesados al exponer su información personal en la Dark Web."

Medidas de minimización del impacto de la brecha

Los representantes del Responsable manifiestan que han tomado medidas tanto desde el punto de vista técnico como operativas, organizativas e incluso legales (remarcando que los actos cometidos supuestamente por los investigados están tipificados en el ámbito penal). Aportan un listado de 35 acciones tomadas desde el día 19/10/2020 al 24/12/2020 que comprenden entre otras:
- Conminar a uno de los sospechosos a que no acuda más a su puesto de trabajo
- Se crea un grupo de trabajo interno para investigación de hechos y evaluación de riesgos
- Contratación de experto externo: ******EMPRESA.1***

- Monitorización de la dark web
- Despido del otro empleado por su presunta implicación y eliminación de las credenciales de ambos.
- Solicitud de borrado de los datos a Endesa con respuesta de esa entidad confirmado el borrado.
- Análisis forense de los sistemas involucrados.
- Calificación de brecha y notificación a AEPD.
- Denuncia ante Unidad Central de Ciberdelincuencia, Brigada Central de Seguridad Informática, de la Policía Nacional.
- Contratación ******EMPRESA.2.***
- Actualizaciones a AEPD y Policía Nacional.
- Realización de copias ante Notario de los equipos del personal supuestamente involucrado.
- Comunicaciones a clientes, clientes potenciales, y empleados.

Con respecto al borrado de los datos enviados erróneamente a ENDESA aportan copia del correo electrónico del Responsable (SoYou) a Endesa solicitando la supresión de la información y contestación confirmando la misma.

Manifiestan que en la contestación que tanto la investigación policial como el procedimiento judicial abierto contra los presuntos responsables siguen su curso, y sobre el estado del proceso judicial indican que el asunto se encuentra en el Juzgado nº 9 de Plaza Castilla, con número de Diligencias 119/21.

Sobre si tienen conocimiento de la utilización por terceros de los datos personales publicados en la Dark Web, indican que entre las acciones tomadas como reacción al incidente, se abre una línea directa de comunicación y atención para los interesados, no habiendo sido reportado hasta la fecha por ningún cliente ningún caso, por ejemplo, de sustracción de identidad, contratación fraudulenta, phishing, etc.

Subrayan que, por otro lado, los enlaces en la Dark Web a través de los cuales se podrían, hipotéticamente, extraer los datos, se encuentran deshabilitados. Es decir, cuando un usuario de la Dark Web hace click al enlace donde se encuentran los datos, ya no tiene posibilidad de descargarlos. Indican que no ha tenido conocimiento de que le información filtrada haya podido ser utilizada por terceros que accediesen a ella a través de la Dark Web.

Respecto de los datos afectados.

Tipología de los datos afectados por la brecha de seguridad, con los siguientes campos:
- Datos identificativos: nombre, apellidos, DNI, NIE y/o Pasaporte, dirección física y correo electrónico, teléfono de contacto.
- Datos de características personales: fecha y lugar de nacimiento.
- Datos económicos-financieros: número cuenta bancaria (sin IBAN).
- El campo identificado como "KYC-CONOCER A TU CLIENTE, PREV BLANQUEO CAPITALESFINANCIAC TERRORISMO" perteneciente al fichero denominado "MIR report" que contiene información recopilada de clientes, posibles clientes y comercios en cumplimiento de normativa de prevención de blanqueo de capitales y financiación del terrorismo. Los datos que pueden ser recopilados corresponderían a la tipología de datos identificativos, datos económicos-financieros y comprobación de información en listas públicas relacionadas con sanciones internacionales y si se trata de cargos públicos ("personas con responsabilidad pública o PEP's, en inglés").

Sobre las notificaciones a los afectados aportan cuatro modelos de notificaciones y recibos de los envíos realizados.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

Aportan Registro de Actividades de tratamiento (RAT), Análisis de Riesgo (AR) y seis Evaluaciones de Impacto de Datos Personales (EIDP) sobre seis tratamientos afectados. Obran dichos documentos en las presentes actuaciones de inspección.
Aportan listado de las medidas técnicas y organizativas adoptadas para garantizar el nivel de seguridad que se encontraban implementadas en el momento del incidente.
Se ha solicitado al Responsable las siguientes medidas o garantías de protección de datos preexistentes a la ocurrencia de la brecha:
Copia del contrato de colaboración con Endesa donde consten todas las cláusulas y garantías establecidas de protección de datos (incluidas adendas relacionadas, en su caso), así como las finalidades de los tratamientos que realizará Endesa con los datos personales.
Copia de los compromisos de confidencialidad suscritos por el personal supuestamente responsable de la brecha (el aludido ingeniero de datos y el otro técnico del equipo de datos).
Copia de las normas internas establecidas por la entidad, en su caso, con relación a la confidencialidad de los datos personales de los clientes, incluyendo copia de los avisos realizados al personal con relación a dicho tema.
A este respecto, el Responsable aporta copia del contrato firmado con ENDESA ENERGIA, S.A.U (Endesa). En virtud de dicho contrato, el Colaborador (Endesa) se compromete a ofrecer a sus clientes la financiación de sus compras de los bienes y servicios que comercializa en sus establecimientos a través del Responsable,
quedando así el Colaborador integrado en la Red de Distribución del Responsable.
En el Apartado 3 de dicho Contrato se regulan las Normas de Confidencialidad que habrá de aplicarse a toda “Información Confidencial” relacionada con el Contrato, incluida información sobre clientes y no clientes a la que tenga acceso por razón de los servicios de financiación contratados con el Responsable.
Por otro lado, el Apartado 9.5. regula las Obligaciones en materia de protección de datos de carácter personal que aplican al contrato, indicando, entre otras cuestiones, que la finalidad del tratamiento de los datos personales será la gestión de la contratación de los productos del Responsable (incluida la adopción de medidas precontractuales), la prevención del fraude y el cumplimiento de sus obligaciones legales. Con las mismas finalidades se podrán recabar datos sobre solvencia, morosidad u otros indicadores de riesgo crediticio.
La regulación de la relación entre ambas partes bajo la figura del ENCARGO DE TRATAMIENTO es objeto de tratamiento en el Anexo de Protección de Datos incluido a continuación del contrato principal. Se verifica que dicho anexo especifica aspectos sobre las características del tratamiento, incluidas las categorías de datos a tratar, y las obligaciones del encargado, que entre otras destacan: utilizar los datos personales solo para la finalidad estipulada y nunca para fines propios, tratar los datos de acuerdo con las instrucciones del responsable, garantizar la confidencialidad, y que una vez acabada la relación contractual el encargado devolverá al responsable los datos personales, que comportara el borrado total de los datos existentes. También se menciona las garantías relacionadas con la posible ocurrencia de brechas de seguridad.

Aportan copia de los compromisos de confidencialidad firmados por las dos personas que indican que presuntamente han estado en el origen del incidente causante de la Brecha de Seguridad.
Los representantes del responsable manifiestan que:
- La entidad entrega a todo su personal un Código de Conducta que comunica las pautas de comportamiento a seguir por todos los implicados.
- El Código incluye un apartado relativo a los principios éticos a aplicar sobre el uso de los datos de carácter personal de los clientes, proporcionando un marco de referencia a los colaboradores para el tratamiento de este tipo de datos (Apartado 2), así como otro relativo a la Confidencialidad según el cual la confidencialidad y el secreto profesional son los principios fundamentales de la profesión de la banca por lo que deben ser una preocupación permanente para todos y cada uno de los colaboradores, cualquiera que sea el ámbito en el que desempeñan sus funciones (Apartado 22).
- La comunicación del Código de Conducta se realiza, a todo el personal que ha de cumplirlo, vía correo electrónico.
- Asimismo, en la planificación de bienvenida a las nuevas incorporaciones se incluye un apartado relativo a la seguridad y al compliance en general ("Newcomers Onboarding Agenda"). Se adjuntan las correspondientes sesiones realizadas a las dos personas presuntamente involucradas en el incidente (entre otras nuevas incorporaciones).
- Por otro lado, con motivo de eventos o fechas concretas se remite a toda la plantilla información de concienciación en aquellas áreas o escenarios que se han determinado como más sensibles para la empresa como es la confidencialidad o el compliance penal.
Aportan copia del citado Código de Conducta (fecha última revisión Sept.2019), y de los correos electrónicos enviados a los presuntos responsables y el documento "Newcomers Onboarding Agenda" de abril 2019.

Respecto de las medias implementadas con posterioridad la brecha

Los representantes del Responsable manifiestan que con motivo de la investigación de los hechos se ha realizado una revisión exhaustiva de las medidas aplicadas e implantadas, llegando a la conclusión de que el incidente se habría causado, presuntamente, por las acciones individuales de ciertos empleados de la Compañía contraviniendo todas las políticas y procedimientos internos.
Subrayan que se han contratados los servicios de ******EMPRESA.1*** para revisar y mejorar los siguientes aspectos:

-Asesoramiento en protección de datos: redacción de Informes jurídicos en materia de protección de datos.
-Resolución de consultas.
-Control del cumplimiento del RGPD y LOPDGDD: ayuda en el cumplimiento de los principios relativos al tratamiento, apoyo en la identificación de las bases de legitimación del tratamiento y análisis de la normativa sectorial, española y europea de aplicación.
-Asesoramiento en materia de Transferencias internacionales de datos.
-Revisión del Registro de Actividades de Tratamiento.
-Revisión de las cláusulas de información al interesado y en el caso de ser necesario su posterior adaptación.

-Metodología de análisis de riesgos, evaluación de riesgos de los tratamientos, evaluación de los controles implantados y elaboración del plan de tratamiento del riesgo.
-Revisión de los DPIAS elaborados por SoYou y realización de aquellos que sean necesarios.
-Revisión del procedimiento
Aportan copia del contrato de servicios con ***EMPRESA.1***. Indican que adicionalmente se han realizado avisos periódicos lanzados por el CISO de la Compañía, aportando un muestreo de comunicaciones lanzadas a todo el personal por el CISO.

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, debido a la publicación del fichero en la dark web de manera intencionada o dolosa.
De las actuaciones de investigación se desprende, que con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados, ya que aportan Registro de Actividades de tratamiento (RAT), Análisis de Riesgo (AR) y seis Evaluaciones de Impacto de Datos Personales (EIDP) sobre seis tratamientos afectados.
En lo que se refiere a la causa concreta que ha provocado la quiebra de seguridad, acciones individuales de ciertos empleados de la Compañía contraviniendo todas las políticas y procedimientos internos, se ha constatado, tanto la existencia de los compromisos de confidencialidad suscritos por el personal supuestamente responsable de la brecha (el aludido ingeniero de datos y el otro técnico del equipo de datos). Así como la existencia de normas internas a cumplir por el personal en relación a la confidencialidad de los datos personales de los clientes.
También se comprueba un funcionamiento correcto en la relación con el encargado del tratamiento, siendo éste, tal como se muestra en los antecedentes, el que alerta sobre la posible existencia de una brecha de seguridad.

Sobre los protocolos de actuación para afrontar un incidente como el ahora analizado, la rápida identificación y análisis, ha permitido, tras el conocimiento de la publicación en la dark web, considerar como probable el riesgo para las libertades y derechos de las personas físicas, procediendo así a notificar a la AEPD conforme al art 33 del RGPD y en concreto en al apartado 4, facilitando la información de manera gradual, a medida que se iban teniendo conocimiento de los hechos.
En lo que hace referencia a la orden dada por la Directora de la Agencia Española de Protección de Datos, de fecha 4 de noviembre de 2020, relativa a necesidad de comunicar a los afectados la existencia de la mencionada brecha, queda acreditado en la documentación remitida, que el reclamado cumplió con la orden dictada por la Directora.
En cuanto a las medidas posteriores, y pese a que la investigación de los hechos concluye que el incidente habría sido causado, presuntamente, por las acciones individuales de ciertos empleados, se procede a contratar los servicios de una empresa especializada para la revisión y mejora de la seguridad.
Por último y en relación con la reclamación presentada, no se hace necesario realizar ninguna actuación de investigación, ya que la única documentación aportada por el reclamante, es la comunicación realizada por el responsable en cumplimiento de la orden dada por la Directora de AEPD de fecha 4 de noviembre de 2020.

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 al reclamante ***A.A.A.*** con ***NIE ***NIE.1*** y al responsable CACF BANKIA CONSUMER FINANCE EFC S.A. con NIF A88147053 con domicilio en AVDA. MANOTERAS, N.º 44, 2 D - 28050 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.

940-0419

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