- **Procedimiento Nº: PS/00461/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a 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 CAIXABANK, S.A. en el que informan a la Agencia Española de Protección de Datos (AEPD) que, con fecha 2 de septiembre de 2019, la unidad de negocio involucrada empezó a detectar comportamientos anómalos en la cartera de clientes de ciertos exempleados, verificando posibles fugas de información por parte de estos, antes de resolver sus contratos con la entidad.

Justificación de notificación tardía:

Manifiestan que desde que se advirtió el incidente se han llevado a cabo diferentes actuaciones internas destinadas a verificar que la brecha se había efectivamente producido, y su alcance. Es cuando se ha concretado y se han definido las acciones a llevar a cabo, incluida la comunicación de la brecha a la AEPD.

SEGUNDO: A la vista de la citada notificación de brecha de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: 17 de enero de 2020.

ENTIDAD INVESTIGADA

CAIXABANK, S.A. con NIF A08663619 y con domicilio en c/ Pintor Sorolla nº2-4,46002, Valencia.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 5 de mayo de 2020 se solicitó información a CAIXABANK, S.A. y de la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos.

A inicios de septiembre de 2019, la unidad de negocio de banca privada de la Entidad detectó comportamientos anómalos en la cartera de clientes de dos exempleados.

Los exempleados A.A.A. y B.B.B. desempeñaban funciones directivas asesorando a clientes en relación con la administración de su patrimonio financiero para conservar y optimizar su rendimiento; y como tal tenían acceso a información personal confidencial y sensible de tales clientes.

Al haber advertido indicios de una posible divulgación ilícita a terceros de datos personales, el área de Auditoría Interna de la Entidad llevó a cabo un análisis que culminó con la emisión en fecha 28 de octubre de 2019 del Informe de Auditoría nº BEXXX, del que aportan la parte que entienden suficiente a efectos del informe de la brecha de seguridad de datos personales. La Entidad detectó que ambos exempleados, antes de causar baja como empleados, el día 29 de julio de 2019, se habían apoderado y habían divulgado a terceros ajenos a la entidad información personal:

A.A.A. reveló a terceros, sin autorización, información confidencial de 187 clientes, que filtró a través de varios correos electrónicos. Según se confirma en el informe de auditoría, el 24 de julio de 2019 se enviaron 6 correos electrónicos, y el día 29 de julio de 2019, se enviaron 19 correos electrónicos. Los correos electrónicos fueron enviados por A.A.A. a su dirección de email particular y a otra dirección de correo electrónico externa de un tercero. Los datos objeto de difusión incluían el DNI de clientes, información de posiciones, rentabilidades y variaciones patrimoniales anuales.

B.B.B., filtró información confidencial a terceros de 32 clientes entre el día 20 de junio y el 28 de julio de 2019, utilizando 18 correos electrónicos. Entre los datos objeto de difusión se incluían el DNI de clientes, rentabilidades y variaciones patrimoniales anuales, así como documentación fiscal.

En fecha 4 de octubre de 2019, la Entidad requirió a través de burofax a los exempleados, advirtiéndoles del carácter ilícito de sus conductas, solicitando que se abstuvieran de utilizar y revelar los datos sustraídos.

En fecha 8 de octubre de 2019 se remitió por parte de la Entidad un burofax a *BANKINTER, S.A.* (donde trabajaban los antiguos empleados de CaixaBank) del que aportan copia, advirtiendo de las actuaciones realizadas por A.A.A. y B.B.B. con el fin de que la Entidad adoptara las medidas preventivas necesarias en relación con los datos personales de los clientes de CaixaBank.

Con fecha 17 de enero de 2020, se notificó a la AEPD la brecha de seguridad.

Con fecha 24 de enero de 2020, la Entidad presentó una querella ante los juzgados de instrucción de Madrid, dado que tales hechos podrían ser constitutivos de delito al

afectar al derecho fundamental a la privacidad de los clientes, el secreto bancario y la protección de secretos comerciales.

Con fecha 14 de febrero de 2020, tras haber presentado la mencionada querella, se realizó notificación adicional a la AEPD, informando de las nuevas medidas adoptadas al respecto por parte de CaixaBank.

Con fecha 4 de febrero, con el objetivo de preservar la confidencialidad de los datos obtenidos de forma irregular por parte de los exempleados, se alcanzó un acuerdo de confidencialidad y no concurrencia. En virtud de dichos acuerdos, los Sres. A.A.A. y B.B.B., se comprometieron a guardar el secreto y mantener la confidencialidad de la información obtenida de manera irregular y, en general, de toda la información sensible y confidencial a la que tuvieron acceso durante la vigencia de su relación laboral como empleados de la Entidad, comprometiéndose a no reproducirla, publicarla, difundirla o comunicarla a terceros. Asimismo, se obligaron a destruir de forma inmediata toda la información, en todos los soportes, compromiso plasmado con la firma del Certificado de Destrucción que se acompaña a cada uno de los acuerdos.

En fecha 19 de marzo de 2020 se comunicó a la AEPD cierre de la brecha de seguridad.

Medidas de minimización del impacto de la brecha.

Envío de burofax a los exempleados solicitando la destrucción de la información.

Envío de burofax a *BANKINTER* advirtiendo de los hechos y solicitando la no utilización de la información.

Presentación de la querella.

Adopción del acuerdo de confidencialidad y certificado de destrucción de la información.

Respecto de los datos afectados.

El número de afectados por la brecha fue en total de 219. La información que se vio afectada fue: DNI, información económico-financiera, información de posiciones, rentabilidades y variaciones patrimoniales anuales.

Las posibles consecuencias para los afectados son la divulgación a terceros de su información personal. En los acuerdos y en los certificados de destrucción de la información, se recoge que todas las copias de los correos electrónicos que contenían datos personales de clientes de la entidad fueron destruidas.

De las investigaciones realizadas no se concluye que los datos personales divulgados hayan sido utilizados por terceros.

La Entidad ha concluido que no procedía la comunicación a los afectados, teniendo en cuenta que se han adoptado medidas apropiadas para evitar que la violación de seguridad tenga implicación en los derechos y libertades de los clientes afectados.

Respecto de las acciones tomadas para la resolución final de la brecha.

Para la resolución de la brecha se llegó a un acuerdo con los exempleados con el objetivo de mantener la confidencialidad de la información de los clientes afectados. En el acuerdo se incluyen obligaciones de destrucción de la información y de confidencialidad. El cumplimiento del acuerdo se ratificó por parte de los empleados mediante la emisión y firma de un certificado de destrucción de la información.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha.

Aportan copia del Registro de Actividades de Tratamiento del área de Banca Privada y Banca Premier, área a la que pertenecían los empleados.

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 consideran que no era necesario realizar un análisis de riesgo ni una evaluación de impacto.

Los empleados están sujetos al cumplimiento del Código de Ética que en su apartado séptimo recoge la obligación de confidencialidad. Asimismo, están obligados al cumplimiento de la norma interna número 137, que se refiere al Código ético, de la cual aportan copia. Concretamente, en el punto 2.1 de la norma 137 se establecen los principios que deben regir la actividad de las personas sujetas al código ético, entre ellos “La confidencialidad de la información que se trata, que se constituye como pilar fundamental sobre el cual se asienta la relación de confianza con los colectivos con los que los empleados se relacionan”.

La normativa interna de la Entidad recoge la preservación de la privacidad de los clientes como pilar fundamental de la actividad desarrollada por los empleados y es de obligado cumplimiento y conocimiento para todos ellos. Adicionalmente se realizan formaciones periódicas que necesariamente deben superar los empleados, por estar vinculadas a su retribución variable.

En el momento en el que un empleado inicia una consulta a través del Terminal Financiero, aparecen dos avisos. El primer aviso recuerda al empleado que para poder consultar clientes no relacionados con la oficina a la que pertenece debe haber una causa justificativa. Concretamente, el empleado debe seleccionar una de las siguientes tres opciones (i) el cliente está presente y ha solicitado expresamente la consulta, (ii) el cliente no está presente pero la consulta está relacionada con un motivo profesional y (iii) la consulta es necesaria para la puesta a disposición de Administraciones Públicas, jueces o Tribunales.

Una vez el empleado selecciona cuál de los tres motivos lo habilita para consultar los datos del cliente, aparece otro control en el que se indica que la consulta requiere confirmación. Se recuerda que la consulta será monitorizada para su tratamiento como posible incumplimiento del Reglamento General de Protección de Datos y el empleado debe confirmar que quiere continuar con la consulta.

Respecto de las medias implementadas con posterioridad la brecha.

Como respuesta a la brecha de seguridad ocurrida, se ha iniciado el proceso para realizar la correspondiente evaluación de impacto.

TERCERO: En fecha 4 de enero de 2021, la Directora de la Agencia Española de Protección de Datos acuerda iniciar procedimiento sancionador a CAIXABANK, S.A. por la presunta infracción del artículo 33 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como leve a efectos de prescripción en el artículo 74.m) de la LOPDGDD.

CUARTO: En fecha 21 de enero de 2021, la investigada presenta alegaciones al acuerdo de inicio, en el que, en síntesis, manifiesta que la notificación de la brecha de seguridad a la AEPD se realizó en el momento en el que se advirtió que era probable que la misma constituyera un riesgo para los derechos y las libertades de las personas afectadas y solicita la anulación del acuerdo de inicio por falta de concurrencia de la infracción prevista en el artículo 33 del RGPD.

HECHOS PROBADOS

PRIMERO: A inicios de septiembre de 2019, la unidad de negocio de banca privada de la Entidad empieza a detectar comportamientos anómalos en la cartera de clientes de ciertos exempleados, verificando posibles fugas de información por parte de estos.

SEGUNDO: El área de Auditoría Interna de la Entidad lleva a cabo un análisis que culmina con la emisión, en fecha 28 de octubre de 2019, del Informe de Auditoría nº BEXXX, por el que se detecta que dos empleados habían obtenido información sensible y confidencial de manera irregular.

TERCERO: En fecha 17 de enero de 2020, CAIXABANK, S.A. notifica a la AEPD la brecha de seguridad.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

El artículo 89.1.d) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) señala lo siguiente:

"Artículo 89. Propuesta de resolución en los procedimientos de carácter sancionador.

1. El órgano instructor resolverá la finalización del procedimiento, con archivo de las actuaciones, sin que sea necesaria la formulación de la propuesta de resolución, cuando en la instrucción procedimiento se ponga de manifiesto que concurre alguna de las siguientes circunstancias:

a) La inexistencia de los hechos que pudieran constituir la infracción.

b) Cuando lo hechos no resulten acreditados.

c) Cuando los hechos probados no constituyan, de modo manifiesto, infracción administrativa.

d) Cuando no exista o no se haya podido identificar a la persona o personas responsables o bien aparezcan exentos de responsabilidad.

e) Cuando se concluyera, en cualquier momento, que ha prescrito la infracción."

El artículo 28.1 de la ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en lo sucesivo LRJSP) señala lo siguiente:

Artículo 28. Responsabilidad.

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

El artículo 70 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, señala lo siguiente:

Artículo 70. Sujetos responsables.

"1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título."

De acuerdo con lo expuesto y a la vista de las alegaciones presentadas, en el sentido de que la notificación de la brecha de seguridad a la AEPD se realizó en el momento en el que se advirtió que era probable que la misma constituyera un riesgo para los derechos y las libertades de las personas, la misma debe ser aceptada y proceder al archivo del procedimiento sancionador, toda vez que el análisis de la entidad para la toma de decisión relacionada con la notificación de brechas de seguridad a la autoridad de control, se efectúa conforme a lo expuesto en la Guía para la gestión y notificación de brechas de seguridad sobre la base de los parámetros que en la misma se indican. Además, hay que señalar que la entidad investigada tenía implementadas medidas de seguridad que, en principio, eran las adecuadas para garantizar que los datos personales no fueran accesibles por terceros y, como consta en los hechos, en cuanto el ataque fue detectado y confirmado por la entidad se adoptaron de manera inmediata una serie de medidas de seguridad adicionales con el fin de minimizar los riesgos y extremando las dificultades para el acceso y extracción de la información.

Por lo tanto, de acuerdo con la legislación aplicable, la Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: ARCHIVAR el presente procedimiento sancionador.

SEGUNDO: NOTIFICAR la presente resolución a CAIXABANK, S.A. con NIF A08663619 y con domicilio en c/ Pintor Sorolla nº2-4,46002, Valencia.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante

escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-131120

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