- **Procedimiento Nº: E/10066/2020**

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 TTI FINANCE. S.A.R.L. con número de registro de entrada ******REGISTRO.1*** relativa a exfiltración de datos personales, 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: 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:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

SHELLBROOK INVESTMENT, SL con CIF B86802857

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 14 de diciembre de 2020, se solicitó información a HISPANIA ASSET MANAGEMENT, S.L (en adelante Hispania) la cual puso de manifiesto, en su contestación, que no tiene ningún acuerdo de prestación de servicios con TTI Finance siendo SHELLBROOK INVESTMENT, S.L. (en adelante Shellbrook), empresa matriz del grupo empresarial de Hispania, la que mantiene un contrato de prestación de servicios con GROVE PERFOMANCE MANAGEMENT LIMITED en el que se menciona a TTI Finance como “Legal Owner” o propietario legal de las deudas. En este escrito solicitan que el expediente se dirija a Shellbrook.

2.- Con fecha 28 de enero de 2021 se remite requerimiento de información a Shellbrook y de la respuesta recibida se desprende:

Respecto de la empresa.

- TTI Finance tiene firmado un acuerdo de servicios con GROVE PERFOMANCE MANAGEMENT LIMITED (en adelante, GROVE) para la gestión de determinadas carteras de crédito. Por su parte, GROVE ha suscrito un acuerdo de servicios con la

sociedad Shellbrook para la prestación de diferentes servicios de asesoría y consultoría de créditos en relación con ciertas carteras y portfolios, entre los que se encuentran las carteras de TTI Finance, actuando Shellbrook como subencargado del tratamiento de TTI Finance.

Por otra parte, dichas carteras de TTI Finance que se encuentren ubicadas en España son gestionadas por Hispania a través de Shellbrook. En consecuencia, Hispania también tiene la consideración de subencargado de TTI Finance.

Shellbrook ha aportado contrato entre GROVE como encargado del Tratamiento, y Shellbrook como subencargado del tratamiento (documento 1), y novación de este contrato con fecha 31 de diciembre 2020 entre las partes actualmente implicadas en el servicio (documento 2).

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

Shellbrook ha aportado Informe sobre la brecha de seguridad (documento 3) en el que consta:

- El 03/11/2020 ***Un empleado de la compañía recibe un correo electrónico XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- El día 4/11/2020, ***nada más recibirse el correo en el Departamento Financiero, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- El día 6/11/2020 se comienza el Análisis forense del ordenador afectado

- Comienzan las comunicaciones con el cliente TTI Finance en relación con la brecha.

o El día 6/11/2020 se comunica la brecha. (Anexo III)

o El día 9/11 ***se remite una comunicación (Anexo IV) con la valoración de la brecha y las medidas implantadas, entre otras: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX***.

o El día 10/11/2020 (Anexo V) ***comunicación dando respuestas a las preguntas planteadas por el cliente XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX***.

o El día 11/11/2020 (Anexo VI y Anexo VII) ***comunicación al cliente con objeto de tratar conjuntamente la brecha sufrida XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX***.

o El día 12/11/2020 (Anexo VIII y IX) se envía informe.

o El día 17 (Anexo X) y 23/11/2020 (Anexo XI y XII) remisión de nuevas comunicaciones incluyendo contestaciones a las preguntas efectuadas por el cliente.

- El 17/12/2020 concluye el análisis forense ***sin encontrar XXXXXXXXXXXXXXXXX***.

Respecto de las causas que hicieron posible la brecha

- ***Shellbrook manifiesta XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

Respecto de los datos afectados.

- ***Los datos afectados corresponden a un total de XXXXXXXXXXXXXXXXXXX.***

- ***Los datos personales comprometidos: XXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- ***Dado el volumen y tipo de dato expuesto XXXXXXXXXXXXXXXXXXXXXXXXX.***

- ***La entidad manifiesta que han calculado el riesgo y el resultado obtenido XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- ***Shellbrook manifiesta XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- ***Shellbrook no tiene conocimiento XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

Respecto de las medidas de seguridad implantadas

- ***Con anterioridad a la brecha, Shellbrook XXXXXXXXXXXXXXXXXXXXXXXXXX:***

o Acceso a los sistemas XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Contraseñas custodiadas XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Las cuentas XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o La actividad XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Copias de seguridad XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Puertos XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Las conexiones XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

- ***Con posterioridad a la brecha de seguridad XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

• Shellbrook ha aportado los siguientes documentos:

o Registro XXXXXXXXXX.

o Política de seguridad XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

o Informe de análisis XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

• Shellbrook manifiesta que realiza pruebas anuales XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Respecto de la notificación con posterioridad a las 72 horas.

Como subencargado del tratamiento, la brecha de seguridad se notificó dentro de las 72 horas al encargado del tratamiento con toda la información que en el momento se disponía, y sucesivamente conforme avanzaba el análisis de la brecha.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

SHELLBROOK no había sufrido hasta la fecha ningún incidente 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 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.

De la documentación aportada por la empresa, entre ella el RAT y la Política de seguridad en materia de protección de datos, así como un análisis forense de la brecha y un informe pericial sobre posibles amenazas, ambos realizados por

empresas externas, donde se indica que no hubo vulnerabilidad técnica imprevista y que tampoco se identifican cambios técnicos específicos que pudieran evitar la brecha, pues se trataba de una brecha de tipo social.

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.

La brecha fue posible gracias a un error humano***, un empleado recibe un correo XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

En cuanto al impacto, se han visto afectados XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

La investigada afirma que no tiene conocimiento de que se hayan publicado los datos personales obtenidos a causa de la brecha en Internet, ni de su posible indexación por los buscadores, ni tampoco que los datos obtenidos a través de la brecha hayan sido utilizados por terceros, ***ya que cree que la intención del atacante XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

Para evitar que estos hechos se repitan se ha procedido a recordar a los empleados cuales son los peligros de los correos electrónicos de phishing y se ha implementado la política interna en virtud de la cual***, todos los correos electrónicos recibidos en el entorno de la compañía XXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de mitigar los efectos de la brecha, comunicar al responsable del tratamiento y la rápida adopción de medidas para eliminarla.

Por último, se recomienda elaborar 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.

III

Por lo tanto, se ha acreditado que la actuación del investigado como 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 al investigado SHELLBROOK INVESTMENT, SL

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