- **Procedimiento Nº: E/03109/2021**

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 del escrito presentado por **IBERIA LINEAS AEREAS DE ESPAÑA SA OPERADORA,** (en adelante IBERIA), con número de registro de entrada ******REGISTRO.1***, relativo a un ciberincidente del prestador de servicios ******PRESTADOR.1*** (en adelante ***XXXX***), 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, teniendo conocimiento de los siguientes extremos:

Resumen de la notificación:
XXXX, empresa suiza prestadora de servicios tecnológicos para aerolíneas, se ha visto afectada por un ciberataque que podría afectar a un gran número de aerolíneas de transporte de pasajeros. **IBERIA** manifiesta que no es el responsable de los datos respecto del tratamiento realizado por ***XXXX*** y no tiene una relación comercial con ***XXXX.*** No obstante, la interconexión de los vuelos internacionales es tal que se ha comprobado que puede haber datos afectados que tuvieran su origen primario en **IBERIA**. ***XXXX*** opera sistemas de servicio a los pasajeros (Passenger Servicing Systems, o "PSS") para varias aerolíneas del sector, aunque, como se ha mencionado anteriormente, no para la entidad investigada.
Aunque el incidente todavía está siendo investigado por ***XXXX***, según la información compartida con **IBERIA** en este momento, los componentes del entorno operativo del servicio PSS de ***XXXX*** en Estados Unidos, habrían sido objeto de un ataque de seguridad que habría provocado una violación de seguridad de datos personales que afectaría a datos de viajeros frecuentes ("Frequent Flyers").
Según la información recibida, **IBERIA** entiende que el ciberataque habría sido detectado por ***XXXX*** el 8 de febrero de 2021, y que al día siguiente lo clasificó como un incidente de seguridad y contrató a varias empresas para investigar, monitorizar los sistemas y poner en marcha el plan de contención. El día 11 de febrero de 2021 habría sido el último día en que se observó actividad en los sistemas de ***XXXX*** por parte de los atacantes. Consideran que no es una brecha de seguridad que afecte a los sistemas de **IBERIA** o a los de sus encargados de tratamiento; sin embargo, fruto de la naturaleza interconectada de las aerolíneas y de sus respectivos programas de viajeros frecuentes, se cree que parte de los datos comprometidos corresponderían a miembros de los programas Iberia Plus y British Airways Executive Club (BAEC) previamente compartidos con otras aerolíneas ***XXXXXXXX*** para permitir a estas últimas ofrecer beneficios recíprocos a miembros de programas de viajeros frecuentes

de otras aerolíneas ***XXXXXXXX***. En concreto, ***XXXX*** ha notificado a la entidad investigada que los datos comprometidos incluían 449.325 cuentas Iberia Plus, con las siguientes tipologías de datos:

Documentación aportada:

ENTIDAD INVESTIGADA: Durante las presentes actuaciones se ha investigado la siguiente entidad: **IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA** con **CIF** A85850394 con domicilio en C/ MARTÍNEZ VILLERGAS, 49 - 28027 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN
Con fecha 4 de marzo de 2021 se solicitó información a **IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA**. De la respuesta recibida se desprende lo siguiente: ***XXXX*** comunicó la brecha en primera instancia a International Consolidated Airlines Group, S.A. ("IAG"), sociedad de cabecera del Grupo IAG al que pertenece **IBERIA**, el sábado día ******FECHA.1***, e inmediatamente IAG informó a la entidad investigada de la comunicación recibida desde ***XXXX***.
En dicha comunicación ***XXXX*** informaba de que no es proveedor de **IBERIA** en relación con la gestión de los ficheros de información de viajeros frecuentes propios o de terceras aerolíneas, pero sí lo es de otras aerolíneas con los que la entidad investigada tiene acuerdos para el reconocimiento recíproco de niveles de estatus de viajeros frecuentes, como ocurre en el marco de las aerolíneas pertenecientes a la alianza ***XXXXXXXX*** y con las que a tales efectos intercambia la información necesaria relativa a dichos viajeros. Dicha comunicación de datos está informada a los interesados en la política de protección de datos de clientes y pasajeros de **IBERIA**, disponible en ******URL.1***, apartado "¿Con quién compartimos tus datos personales?" y está basada en el cumplimiento de la relación contractual que nos une a nuestros pasajeros miembros del programa Iberia Plus que, identificándose como tales, tengan reserva en vuelos operados por otras aerolíneas de la alianza ***XXXXXXXX***, o que lleven a cabo reservas de vuelos directamente con esas aerolíneas identificándose como miembros del Programa Iberia Plus al objeto de disfrutar de los beneficios que a tales efectos les correspondan. La información disponible, por remisión, en la web ******URL.2*** muestra cuáles son las ventajas y beneficios para los miembros del programa Iberia Plus de volar con aerolíneas de la alianza ***XXXXXXXX***, incluyendo la generación de puntos de fidelización (avios, en el caso de Iberia Plus), así como beneficios adicionales dependiendo del nivel del pasajero dentro del programa de fidelización de que se trate: facturación preferente, fast track en acceso a zona de embarque y/o en embarque, acceso a salas VIP, franquicia adicional de equipaje, preferencia en lista de espera, etc…
El intercambio de esta información entre **IBERIA** y cada una de las demás aerolíneas ***XXXXXXXX*** se lleva a cabo de forma segura. La pasarela para el intercambio de dicha información es ***XXXXXXXX***.

Respecto a las categorías de los datos afectados:
XXXX notificó que sólo se habían visto afectados por esta brecha los nombres de clientes Iberia Plus, sus números de viajeros frecuentes, su nivel de estatus dentro del programa y algunas de sus preferencias, como los asientos. Desde **IBERIA** entienden que la base legitimadora para el tratamiento de datos por parte de ***XXXX,*** es su condición de encargado del tratamiento respecto de dichos datos, en nombre de la

aerolínea receptora de dicha información para la que se encuentre prestando los servicios correspondientes de gestión de los ficheros de información de viajeros frecuentes de terceras aerolíneas.
De acuerdo con la información facilitada por ***XXXX***, el número de miembros Iberia Plus afectados sería de unos cuatrocientos cincuenta mil (450.000).
Aportan copia de la comunicación remitida por correo electrónico a principios del mes de marzo de 2021 a los miembros del programa Iberia Plus que se vieron afectados por la brecha de seguridad de ***XXXX***. En ella, además de informar acerca del incidente, de los datos de los interesados que se habrían visto comprometidos, así como de sus posibles consecuencias, se les advertía de que como medida de precaución ******MEDIDA.1***.

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 artículo 4 apartado 12 del 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."*

Asimismo, el artículo 4 apartado 7 del RGPD define al "responsable del tratamiento" como la "*persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".*

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.

III

De la documentación aportada por la entidad investigada en el curso de estas actuaciones de investigación se desprende que **IBERIA LINEAS AEREAS DE ESPAÑA SA OPERADORA** no es responsable del tratamiento de datos personales que realiza ***XXXX,*** dado que no es quien define los medios ni los fines del tratamiento que realiza esta última, ni tiene relación directa con la empresa global de tecnología de la informa-

ción ***XXXX,*** que es la que ha sufrido el ciberataque, por lo que no se puede considerar que haya sufrido ningún incidente de seguridad, ni tenga responsabilidad alguna en lo sucedido en ***XXXX***.

No constan reclamaciones ante esta AEPD por parte de posibles clientes afectados

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 **IBERIA LINEAS AEREAS DE ESPAÑA SA OPERADORA**

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