- **Expediente N.º: EXP202303565**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 6 de mayo de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***PILLOW HOTELS, S.L.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202303565

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 07/02/2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra PILLOW HOTELS, S.L., con NIF ***B66964255*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: la reclamante manifiesta haber realizado una reserva en el alojamiento bilbaíno *"Irala, by Pillow"*, a través de booking.com. Señala que unos días antes del viaje recibió un mensaje de WhatsApp en el que una persona que se identificaba como directora del hotel se dirigía a ella por su nombre y apellidos y le pedía la confirmación de la reserva, facilitándole un enlace fraudulento para que introdujera los datos de su tarjeta, cosa que no hizo. Dice que contactó con el hotel para confirmar el fraude y que le comunicaron que ya eran conocedores de otros caso similares.

Se aportan capturas de pantalla de la conversación de WhatsApp en la que se produce la suplantación del alojamiento e intento de estafa.

SEGUNDO: 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), el 22/03/2023 se dio traslado de dicha reclamación a la parte reclamada, 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.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 02/04/2023, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 04/04/2023. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

TERCERO: Con fecha 07/05/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Las presentes actuaciones de investigación se han enfocado en los puntos que a continuación se van a desarrollar.

Punto 1: Respecto de la empresa investigada.

La parte reclamada es una sociedad limitada de nacionalidad española. Según los datos obrantes en AXESOR para el ejercicio de 2022 se trata de una PYME, con 13 empleados y un volumen de ventas al inferior a un millón de euros. No se han encontrado en Sigrid expedientes anteriores al presente con relación a brechas de esta entidad.

La entidad MD MANAGEMENT, S.L., actúa como la matriz del grupo al que pertenece la parte reclamada, tratándose de una empresa de un único empleado y un volumen de ventas de inferior a un millón de euros, según AXESOR para el ejercicio 2022. No se han encontrado tampoco en Sigrid expedientes anteriores al presente con relación a brechas de esta entidad.

La entidad RAPINFORMES ON LINE, S.L., ha actuado como representante.

Punto 2: Constatación de los hechos reclamados.

Como punto de partida, se ha procedido a tratar de verificar los hechos reclamados y los detalles del incidente. Para ello se han hecho requerimientos a la parte reclamada, a la parte reclamante y al proveedor de la plataforma de reservas *Booking.com*.

2.1. Cronología de los hechos.

El orden cronológico de los sucesos, obtenido a partir de la información aportada, es el siguiente:

- La parte reclamante realizó una reserva el día 05/01/2023 en el alojamiento de la parte reclamada. La reserva fue realizada a través de la plataforma del proveedor externo *Booking.com*. La parte reclamante recibió un correo electrónico ese día, de *Booking.com*, con la confirmación de su reserva y los datos básicos. La reserva era para las fechas del 8 al 10/02/2023.
- Según manifiesta *Booking.com*, en relación con la cuenta de la parte reclamada en su plataforma, "*el primer intento malicioso se produjo el 20/01/2023*". No se ha podido profundizar sobre el ataque concreto sufrido, aunque se indica que se trataría de *phishing* con el objeto de obtener las credenciales de acceso.

Consultando el registro de brechas que dispone la División de Innovación Tecnológica de la AEPD, no se ha localizado ninguna notificación de brecha específica de *Booking.com*, si bien constan antecedentes en esas fechas de casos similares donde establecimientos hoteleros se han visto afectados por la vulneración de su cuenta en la plataforma debido a ataques de *phishing*.

Adicionalmente, se ha consultado la información disponible en IMI (Sistema de Información del Mercado Interior). No se ha localizado ninguna entrada relativa a esta brecha, si bien consta una entrada previa de tipología similar, en las que España figura como autoridad de control interesada (entrada nº ******ENTRADA.1***).

- La parte reclamada indica que el día 30/01/2023 solicitó a su departamento de informática que modificaran las contraseñas de los correos electrónicos.
- El 03/02/2023 se produjo el intento de fraude y suplantación del alojamiento, objeto de la reclamación presentada. En las capturas de pantalla aportadas por la parte reclamante se puede constatar el intento de estafa mediante la tipología descrita en la reclamación: una persona que manifiesta ser la directora del hotel solicita la confirmación de la reserva y envía un enlace a una pasarela de pago (******URL.1***). El número desde el que se contactó a la parte reclamante fue el ******TELEFONO.1***. Según manifiesta la parte reclamada, también se empleó el número ******TELEFONO.2*** para estos fines.
- La parte reclamante contactó con el alojamiento el mismo día 3 de febrero. Manifiesta que llamó por teléfono y envió un correo electrónico alertando del incidente ocurrido. Se aporta copia de la conversación por correo. La parte reclamada respondió el 3 febrero, solicitando capturas de pantalla del presunto fraude, que a su vez fueron enviadas.
- La parte reclamante manifiesta que una vez llegó al alojamiento, que se puede deducir por lo expuesto anteriormente que sería el 08/02/2023, la persona que le atendió en la recepción le comunicó que "*sabían que se había producido la filtración y estaban investigando el origen*".
- Según manifiesta *Booking.com*, en marzo de 2023 la cuenta del alojamiento en su plataforma se encontraba comprometida por motivos de seguridad.
- Posteriormente, la parte reclamante recibió el 07/03/2023 un correo electrónico de *Booking.com* en relación con su reserva. Se aporta copia del mismo. En

este correo se indica que algunos clientes estaban recibiendo llamadas o correos sospechosos tratando de suplantarles tanto a ellos, *Booking.com*, como a los alojamientos que utilizan la plataforma. Se incluyen en el correo una serie de recomendaciones de seguridad para prevenir estafas, así como enlaces en caso de haber sido víctima de algún tipo de fraude de esta naturaleza.

- Tras solicitudes posteriores de información a la parte reclamada, se remitió información que indicaba que una segunda brecha e intento de fraude de similares características se había producido en agosto de 2023. Analizando la información remitida, dicha brecha se pudo producir el día 17 de agosto y, en base a las manifestaciones aportadas por la parte reclamada, ocurrió debido a la vulneración de las credenciales de acceso de su cuenta a la plataforma de *Booking.com*.

Punto 3. Funcionamiento del sistema de reservas.

Para poder profundizar sobre el incidente, se ha tratado de estudiar y comprender el funcionamiento de las reservas, desde que un cliente la realiza a través de la plataforma de *Booking.com* hasta que los datos llegan al hotel. Al haberse producido el incidente antes de haberse realizado la estancia, la filtración ha debido de ocurrir en alguno de los elementos que intervienen en la gestión de reservas.

La parte reclamada manifiesta que cuando un cliente realiza una reserva reciben en el buzón de recepción un correo electrónico en el que figuran los datos del cliente, entre los que se encuentran su nombre, apellidos, datos de contacto (número de teléfono) y fechas de en las que se producirá la estancia. Aportan un correo de ejemplo. En dicho correo se observa que proviene de *WuBook **(***EMAIL.1)***. Se trata de una plataforma para la gestión de reservas, pudiendo actuar de intermediaria entre *Booking.com* y el alojamiento.

En relación con *WuBook*, se ha aportado el contrato de suscripción a dicho servicio. Este contrato está suscrito entre MasterYield S.L. y la parte reclamante en modalidad de alquiler de soffware, formando parte del conjunto de servicios ofrecidos por el sistema de gestión hotelera MasterYield PMS.

No ha sido posible profundizar sobre el uso que realiza la parte reclamada de esta plataforma, por la información disponible sobre este proveedor en Internet, el uso esperable es que fuera empleado para la gestión de las reservas integrándose con los datos registrados en *Booking.com* como portal externo para los clientes. No ha sido posible verificar qué medidas de seguridad existentes hay ni los periodos de conservación de la información alojada allí.

Por parte de *Booking.com*, la información manifestada sobre el funcionamiento de las reservas es la siguiente: Una vez que un cliente ha realizado una reserva en su plataforma, se procesan sus datos por parte de *Booking.com* y del proveedor de alojamiento, así como potencialmente su proveedor de conectividad. *Booking.com* transfiere los datos más relevantes al alojamiento, pudiendo variar en función del tipo de reserva. Según se indica, comprenderían el nombre del cliente, datos de contacto, datos de pago, nombres de los acompañantes y preferencias que pudieran haber especificado al realizar la reserva. En determinados casos, se aporta información

adicional relativa al histórico del cliente: si se ha alojado previamente en ese alojamiento, reservas completadas y cancelaciones, avisos de mala conducta y reseñas emitidas.

No se concreta el canal de transferencia de esta información. En cualquier caso, por la información aportada por *Booking.com*, que se desarrollará posteriormente, esta información sería accesible desde su plataforma empleando la cuenta de usuario que dispone el alojamiento. No consta que el alojamiento disponga de una infraestructura propia donde se almacene la información, más allá del correo electrónico corporativo. Por las manifestaciones realizadas, la gestión de reservas es realizada mediante estas dos herramientas: la plataforma de *Booking.com* y el correo electrónico.

Punto 4: Análisis de las brechas.

4.1. Origen de la primera brecha.

No ha sido posible determinar el origen exacto de la brecha. La parte reclamada manifiesta desconocerlo. Según indican "*se me ocurrió cambiar la clave del mail de recepción y dejó de pasar, así que habrá sido algún link fraudulento que algún recepcionista abrió*", por lo que podría tratarse de un caso de *phishing*.

Se ha solicitado colaboración a *Booking.com* para tratar de esclarecer los hechos, a través de la filial que disponen en España. *Booking.com B.V.,* empresa matriz del grupo *Booking.com* está registrada y tiene su sede social en Holanda. Tal como se indica en la información legal de su portal, la gestión de la plataforma corresponde de manera exclusiva a esa entidad: "*Booking.com B.V. (la empresa que está detrás de Booking.com™) está registrada y tiene su sede social en Ámsterdam, Países Bajos, desde donde ofrece un servicio de reservas de alojamiento online a través de su sitio web (…) Las empresas filiales no ofrecen el Servicio y no poseen, operan o administran el Sitio web ni ningún otro sitio web*".

Manifiestan que ninguno de sus sistemas se ha visto comprometido y trasladan la responsabilidad de los incidentes a los alojamientos, indicando que son con frecuencia víctimas de ataques de *phishing*. Como resultado de estos ataques, se produce un acceso no autorizado a la cuenta del alojamiento en la plataforma de *Booking.com*, desde donde se puede consultar la información de los clientes que tienen allí reservas.

Booking.com indica en su respuesta que es una práctica frecuente que los alojamientos se vean vulnerados por ataques de tipo *phishing,* consiguiendo los atacantes sus credenciales y disponiendo de la capacidad para poder actuar en su nombre. Mencionan que tienen constancia de diferentes métodos que emplean los atacantes: "*los atacantes envían un "enlace de phishing" con la solicitud de hacer clic en él. Booking.com tiene conocimiento de que algunos proveedores de alojamiento hicieron clic en este enlace y descargaron un archivo malicioso que infectó su dispositivo con malware. Este malware permitió a los atacantes acceder al ordenador del proveedor de alojamiento*". Una vez obtenidas las credenciales de su plataforma, los atacantes tendrían acceso a los datos de los clientes y podrían contactarles por otros canales, como sería *WhatsApp*.

Manifiestan que desconocen el volumen exacto de personas afectadas, al ser incidentes ajenos a ellos. Señalan que "*hemos recibido informes de 11.244 reservas afectadas en España durante este año 2023*". No ha sido posible profundizar sobre la tipología de incidentes a los que se refieren, si es particular para este alojamiento investigado o de forma general para todos los alojamientos de España que hacen uso de su plataforma.

En relación con este caso concreto, *Booking.com***,** como se ha señalado en la cronología, manifiesta que el primer incidente de seguridad con la cuenta de la parte reclamada tuvo lugar el 20/01/2023. No se aportan más detalles al respecto sobre qué tipo de incidente fue. Manifiestan que "*se confirmó que la cuenta del alojamiento estaba comprometida en marzo de 2023*", pero no se ha ampliado tampoco la información sobre este aspecto.

El incidente reclamado tuvo lugar entre estos dos hechos, por lo que se puede presuponer que hubo una relación directa y el origen de la brecha pudo ser una vulneración y acceso indebido a la cuenta del alojamiento o a su correo electrónico corporativo, teniendo en cuenta que además el cambio de contraseña de, al menos el correo electrónico, solventó el incidente, según manifiesta la parte reclamada.

4.2. Origen de la segunda brecha.

Como se ha indicado, se produjo una segunda brecha de características similares en el mes de agosto de 2023. No es posible determinar el origen de la misma, pero en este caso por las manifestaciones aportadas se focalizaría en la cuenta corporativa del alojamiento en la plataforma de *Booking.com*.

La contraseña a esta plataforma se vería comprometida y presumiblemente fue explotada para obtener la información de los clientes. La parte reclamada manifiesta lo siguiente a este respecto: *"cambiamos varias veces la contraseña de Booking, la mayoría de las cuales el propio Booking nos echaba de la web y nos pedía establecer de nuevo una contraseña, no sé si por el propio Booking o porque el hacker quería retomar el control. Estuvimos así varias horas, y no fueron menos de 7 u 8 veces las que cambié la contraseña"*

La parte reclamada traslada la responsabilidad de esta segunda brecha a *Booking.com.* Aportan una comunicación de *Booking.com* en la que esta entidad manifiesta que ha ocurrido una brecha de seguridad relativa a la cuenta del alojamiento en su plataforma (*Extranet*): "*we have followed up on your report of suspicious activity on your Extranet Account, we regret to inform you that our Security team has confirmed a breach has occurred*". Por el contenido del mensaje no se puede determinar el origen de esta brecha, si realmente se debe a un incidente de *Booking.com* como manifiesta el alojamiento o no.

4.3. Volumen de personas afectadas.

La parte reclamada ha manifestado que un total de 24 personas pudieron resultar afectadas por la primera brecha, objeto inicial de esta investigación. Aportan un documento Excel con los clientes que tenían reserva en esas fechas, entre los que se encuentra la parte reclamante.

Respecto al segundo incidente, ocurrido en agosto de 2023, la parte reclamada no ha facilitado la cifra de clientes afectados por la brecha. Por la información aportada se trataría de varias decenas: "*todas las rsvas (decenas por no decir más)*"

4.4. Tipología de los datos afectados.

Los datos afectados han sido, como mínimo, nombre, apellidos, datos de contacto (teléfono, correo electrónico) y fechas de la reserva. Al no haberse podido determinar el punto en el que se ha producido la brecha, no es posible concretar esta información.

La parte reclamante manifiesta los siguientes: "*Nombre y apellidos, fecha de la estancia, tipo de habitación, importe, etc.*".

Partiendo de la hipótesis de que la cuenta del alojamiento en la plataforma de *Booking.com* se hubiera visto vulnerada, tal como se ha analizado previamente, los datos afectados podrían haber sido mayores. Según indica *Booking.com*, en caso de haberse visto afectada esta cuenta, los potenciales atacantes podrían tener acceso a:

- Nombre y apellido.
- Número de teléfono.
- Alias de dirección de correo electrónico.
- Número de reserva.
- Primera y última fecha de reserva.

Según el Registro de Actividades de Tratamiento facilitado, relativo al tratamiento que atañe a los clientes, el total de los datos implicados serían:

- DNI o NIF
- Nombre y apellidos
- Dirección postal o electrónica
- Teléfono
- Firma manual
- Características personales
- Circunstancias sociales
- Información comercial
- Económicos, financieros y de seguro
- Transacciones de bienes y servicios

Punto 5: Comunicación informativa del incidente.

Tras las averiguaciones realizadas, se ha tratado de confirmar las comunicaciones realizadas por la parte reclamante informando sobre la brecha ocurrida, tanto a los clientes afectados como el motivo de no haber informado a esta Agencia.

No es posible acreditar que se haya realizado ninguna comunicación proactiva a los clientes afectados por el incidente de enero/febrero de 2023, entre los que se encontraba la parte reclamante. Manifiestan que a los clientes que les llamaron por esta cuestión fueron avisados.

Según se indica en el documento de registro de incidentes de seguridad aportado, se determinó que no era necesario notificar ni a la Autoridad de Control ni a

los interesados: "*Es improbable que la brecha de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas, por lo que conforme a los artículos 33.1 y 34.1 del RGPD no es obligatorio notificarla a la autoridad de control ni comunicarla a los interesados*".

Para el incidente de agosto de 2023 la parte reclamada sí manifiesta que contactaron con los clientes. Se aporta captura de pantalla de uno de los mensajes enviados, el 17/08/23 a través de la mensajería de *Booking.com*, en los que la parte reclamada informaba del incidente y alertaba de la práctica fraudulenta. En dicho mensaje se comenta por parte del alojamiento: "*our account has been hacked*". No se puede constatar que se informase a todos los potenciales afectados ni que se realizase la comunicación en tiempo.

No consta en la página web del hotel ninguna publicación de carácter general alertando de estos incidentes, en caso de haberse realizado la comunicación por ese medio.

Con respecto a la comunicación de estas brechas a esta Agencia, no consta ninguna notificación al respecto.

Punto 6: Medidas de seguridad implantadas.

6.1. Medidas previas a la brecha.

En el marco del traslado se ha aportado la siguiente documentación, enfocada desde el punto de vista del normativo:

- Registro de Actividades de Tratamiento.
- Registro de violaciones de seguridad.
- Análisis de riesgos.
- Medidas técnicas y organizativas.
- Informe de cumplimiento normativo.

Esta documentación contiene los logos de la empresa matriz, MD MANAGEMENT, S.L y la representante, RAPINFORMES ON LINE, S.L., no figurando la parte reclamada (PILLOW HOTELS, S.L.) El nombre fiscal del responsable según se indica es: MD MANAGEMENT 2010 S.L.

Las medidas previas, según manifiesta la parte reclamada en el documento de registro de violaciones de seguridad, eran las siguientes:

- Políticas de protección de datos y seguridad.
- Actualización de sistemas.
- Actualización de software.
- Actualización de equipos.
- Registro de brechas de seguridad.
- Auditorías periódicas.
- Sistema de copias de seguridad.

No se aporta acreditación documental de las mismas ni mayor concreción.

En el análisis de riesgos se trata el correo electrónico corporativo. Se indica que no existe un control ni registro de accesos no autorizado a la aplicación y se estima un riesgo bajo. No se hace mención a la gestión de la cuenta en la plataforma de *Booking.com* en este análisis. No se considera que existan riesgos de *phishing*.

Las medidas propuestas, tal como se detalla en la documentación aportada, se encuentran orientadas al correo electrónico y se enfocan en comprobar que se envían cifrados los mensajes. Se indica que existen sistemas *antiphishing*.

6.1.1. Formación a los empleados.

Se han solicitado las acciones de formación, previas a la brecha, en materia de ciberseguridad y protección de datos.

Se han aportado certificados de diciembre de 2022 por la realización de un curso denominado "*Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*", para un total de 5 personas que la parte reclamada manifiesta que son trabajadores suyos. Se complementa esta información una presentación de una formación en protección de datos elaborada por RAPINFORMES ON LINE, S.L.

Respecto a los empleados, se aporta el registro de la Seguridad Social donde se les vincula a la empresa. En dicho registro figura otra relación de trabajadores, coincidiendo 4 de estas 5 personas, mientras que figuran algunas otras para las que no se ha aportado certificado de formación. Dicho registro figura como razón social VA OPCO SOCIEDAD LIMITADA. Se señala que, según AXESOR, su plantilla en 2022 fue de 13 trabajadores. No se ha aportado información del puesto de trabajo que ocupan estas personas, en particular si son las que atienden de forma exclusiva el buzón de correo y la cuenta de la plataforma de *Booking.com.*

6.2. Medidas adoptadas con posterioridad.

Las medidas para subsanar la primera brecha, según manifiesta la parte reclamada en el registro de violaciones de seguridad aportado, fueron las siguientes:

- Políticas de protección de datos y seguridad.
- Actualización de sistemas.
- Actualización de software.
- Actualización de equipos.
- Auditorías periódicas.
- Sistema de copias de seguridad.
- Actualización del registro de brechas de seguridad con los detalles relativos a esta brecha de datos personales.

No se ha aportado acreditación sobre su efectiva realización. Se destaca que, a excepción de la actualización del registro de brechas, el resto de las medidas también constaban como medidas de seguridad previas.

Respecto al registro de violaciones de seguridad: Cuenta con un único registro, relativo a la brecha objeto de la reclamación. Se indica como fecha de la brecha y de detección el 20/04/2023 (en esta fecha se dio respuesta al traslado). Como datos afectados únicamente figura el número de teléfono y no consta número de interesados. Se indica en la descripción del incidente "…d*ice que contactó con el hotel*

para confirmar el fraude y que le comunicaron que ya eran conocedores de otros caso similares."

Según se indica en este registro, la brecha se dio por resuelta el 21/07/2023.

Complementariamente a la información aportada en el mencionado documento, según las manifestaciones realizadas se tomaron más medidas con posterioridad de carácter operativo, principalmente el cambio de credenciales.

Para la primera brecha, la parte reclamada manifiesta que el 30/01/2023 su departamento de informática modificó las contraseñas de los correos electrónicos y, tras haber cambiado la clave de acceso al correo de recepción, el incidente quedó solventado. Respecto al motivo de este cambio, manifiestan: "*Accedieron al mail de la empresa y se procedió al cambió la contraseña*", sin aportar más detalle. Cabe destacar que el intento de fraude a la parte reclamante se produjo después, el 03/02/2023, y fue en esta fecha cuando se puso en contacto con el alojamiento. No se confirma si se modificó la contraseña de su cuenta para la plataforma de Booking.com en este primer caso.

Manifiestan que avisaron a su gestoría, a *Booking.com*, a su departamento comercial e intentaron poner denuncia en la Ertzaintza. No se aporta documentación al respecto.

Con relación al segundo incidente informado, las acciones tomadas han sido similares. La parte reclamada manifiesta que se modificó la contraseña de la plataforma de *Booking.com* en repetidas ocasiones: "*cambiamos varias veces la contraseña de* Booking*, (…) Estuvimos así varias horas, y no fueron menos de 7 u 8 veces las que cambié la contraseña*".

Adicionalmente, manifiestan para este segundo incidente haber realizado un análisis de sus equipos informáticos y correo electrónico, sin que se detectase ningún *malware*.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las*

disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Primera obligación incumplida: infracción del artículo 5.1.f) del RGPD

De conformidad con lo establecido en el artículo 4.1 del RGPD, consta la realización de tratamiento de datos personales, toda vez que la parte reclamada realiza, entre otros, la recogida y conservación de datos personales, preferentemente de clientes suyos.

La entidad realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y los medios relacionados con el tratamiento de los datos de carácter personal, en virtud del artículo 4.7 del RGPD.

Además, el responsable del tratamiento se debe encargar también de aplicar las medidas técnicas y organizativas que garanticen la seguridad de los datos personales al llevar a cabo el tratamiento. Y ser capaz de demostrar el cumplimiento RGPD y de la LOPDGDD.

En el presente caso los hechos se materializan en el acceso a los datos de carácter personal por terceros, como consecuencia de brecha de seguridad derivado de la realización de una reserva por la parte reclamante en establecimiento de la parte reclamada, lo que podría suponer la vulneración de la normativa en materia de protección de datos.

El artículo 5.1.f) *"Principios relativos al tratamiento"* del RGPD establece:

"1. Los datos personales serán:

(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."
(…)"

La documentación obrante en el expediente ofrece indicios evidentes de que la entidad, podría haber vulnerado el artículo 5.1.f) del RGPD, principios relativos al tratamiento, al no garantizar debidamente la confidencialidad de los datos de carácter personal como consecuencia de la quiebra de seguridad producida.

Este deber de confidencialidad, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de datos no consentidas por los titulares de los mismos.

Consta que la parte reclamante recibió el 03/02/2023, a través de la red social *WhatsApp*, un mensaje supuestamente del alojamiento donde había realizado una

reserva para ser disfrutada entre 8 al 10/02/2023; en el citado mensaje una persona que manifiesta ser la directora del alojamiento le solicita la confirmación de la reserva y envía un enlace a una pasarela de pago: ****URL.1,* en el que se le piden datos bancarios, negándose a aportarlos. En el mensaje figura identificada la parte reclamante a través de: nombre y apellidos y número de teléfono.

En el mensaje de *WhatsApp* recibido figura lo siguiente:

*****TELEFONO.1*
Hola, parte reclamante
Me llamo ***B.B.B.***
Reservaste nuestros pisos en
Booking.com
Soy el Director de parte reclamada
Estamos deseando conocerte
Pero debes saber que tengo que finalizar
tu reserva
Por favor, hágame saber si su reserva esta
actualizada para que pueda confirmarla
Parte reclamada ***B.B.B.***

Confirmada la reserva por la parte reclamante, recibe un segundo mensaje:

***TELEFONO.1
De acuerdo,
Por favor, siga este enlace web para confirmar su reserva
*****URL.2*
Tu pago se procesará según los términos de tu acuerdo con
Booking.com
Tienes una opción de cancelación
gratuita.
Asi que no te preocupes por la
cancelación.
Gracias por tu comprensión

La parte reclamante remitió correo electrónico a la parte reclamada comunicando el incidente:

"He recibido un mensaje de WhatsApp haciéndose pasar por ustedes (adjunto capturas de pantalla). Conocían mi nombre completo y mi teléfono, lo que indica que ustedes tienen una brecha de seguridad.

Les ruego que, por una parte, denuncien a quien les suplanta la identidad y, de forma más importante, se aseguren de que tratan los datos de sus clientes de manera segura. Por favor manténganme informada de sus acciones al respecto".

Aunque se desconoce cuál ha podido ser el origen de la brecha, la parte reclamada reconoce que el origen que motivó el mensaje dirigido a la parte reclamante pudo estar ocasionado por una actuación negligente por su parte *"se me ocurrió cambiar la clave del mail de recepción y dejó de pasar, así que habrá sido algún link fraudulento que algún recepcionista abrió",* ocasionando una vulneración de sus

cuentas *"Accedieron al mail de la empresa"* y la plataforma *Booking.com* ha señalado que en marzo de 2023 la cuenta del alojamiento se encontraba comprometida por motivos de seguridad.

Asimismo, según la parte reclamante la recepción del alojamiento le comunicó que *"sabían que se había producido la filtración y estaban investigando el origen".*

El número de personas afectadas por esta primera brecha asciende a un total de 24 personas, aportándose documento conteniendo el listado de clientes afectados que tenían reserva en esas fechas, entre los que se encuentra la parte reclamante.

Posteriormente, en el mes de agosto de 2023, se produce una segunda brecha de seguridad de características similares, de la cual tampoco ha sido posible determinar su origen.

En este incidente de seguridad aunque no se ha facilitado el número de clientes afectados, por la información aportada se desprende que se trataría de un número bastante elevado, *"todas las rsvas (decenas por no decir más)".*

Por otra parte, en cuanto a los datos afectados lo estarían como mínimo: *nombre, apellidos y datos de contacto* (teléfono, correo electrónico).

A la luz de lo que antecede y sin perjuicio del resultado de la instrucción del presente procedimiento, se considera que la parte reclamada podría haber vulnerado el principio de confidencialidad de los datos, consagrado en el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.5.a) del RGPD.

III
Tipificación por la infracción del artículo 5.1.f) del RGPD

De conformidad con las evidencias de las que se dispone y sin perjuicio de lo que resulte de la instrucción, se considera que la parte reclamada no garantizó debidamente la confidencialidad e integridad de los datos de carácter personal.

La infracción que se le atribuye a la entidad se encuentra tipificada en el artículo 83.5 a) del RGPD, que considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento, *"con multas administrativas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".*

La LOPDGDD en su artículo 71, Infracciones, señala que: "Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

Y en su artículo 72, considera a efectos de prescripción, que son: *"Infracciones consideradas muy graves:*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que

supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)
a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
(…)"

IV
Propuesta de sanción por la infracción del artículo 5.1.f) del RGPD

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece que:

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

- De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción a imponer en el presente caso por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD de la que se responsabiliza a la parte reclamada, en una valoración inicial, se estiman concurrentes los siguientes factores:

La naturaleza, gravedad y duración de la infracción; los hechos puestos de manifiesto afectan a un principio básico relativo al tratamiento de los datos de carácter personal, como es el de la confidencialidad e integridad de los mismos, que la norma sanciona con la mayor gravedad; en el presente caso se ha posibilitado, como consecuencia del incidente de seguridad, el acceso a los datos de carácter personal de la parte reclamante por la parte reclamada, que no estaba autorizado con los perjuicios que ello puede conllevar.

La intencionalidad o negligencia en la infracción. Se observa grave falta de diligencia en el cumplimiento de las obligaciones que le impone la normativa de protección de datos, permitiendo que ciber-delincuentes accedieran a los datos de carácter personal vulnerando la confidencialidad e integridad hasta en dos ocasiones con motivo de las brechas acreditadas; en este sentido puede citarse la SAN de 17/10/2007, que si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...).el Tribunal Supremo viene entendiendo que existe*

imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto" (artículo 83.2, b) del RGPD).

La actividad de la entidad presuntamente infractora se encuentra vinculada con el tratamiento de datos de carácter personal tanto de clientes como de terceros. En la actividad de la entidad reclamada es imprescindible el tratamiento de datos de carácter personal por lo que, dado su objeto de negocio la transcendencia de la conducta objeto de la presente reclamación es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

El volumen de negocio de la parte reclamada; se trata de una pequeña empresa con una cifra de negocio en el ejercicio 2.022 de 844.498 € (artículo 83.2, k) del RGPD).

A efectos de decidir sobre la imposición de la multa y su cuantía, de conformidad con las evidencias de que se dispone y sin perjuicio de lo que resulte de la instrucción del procedimiento, teniendo en cuenta los criterios del artículo 83.2 del RGPD con respecto a la infracción cometida, vulneración del artículo 5.1.f) del RGPD, se considera fijar una sanción de 3.000 euros.

V

Segunda obligación incumplida: infracción del artículo 32.1 del RGPD

El artículo 32 del RGPD "Seguridad del tratamiento", establece que:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

La documentación obrante en el expediente evidencia la vulneración del artículo 32.1 del RGPD, como consecuencia de la falta de medidas técnicas y organizativas apropiadas a fin de garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad al riesgo se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En el presente caso, se evidencia que las medidas de seguridad que la parte reclamada tenía implantadas en relación con los datos que sometía a tratamiento no eran las pertinentes ni adecuadas para garantizar la seguridad de los datos personales en el momento de producirse los citados incidentes (quiebras).

Como señala igualmente el Considerando 39:

"…Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Según la parte reclamada se adoptaron medidas para subsanar esta primera brecha; sin embargo, no consta acreditado que se hubieran adoptado éstas, si exceptuamos el registro de brechas, pues las enumeradas ya figuraban previamente al incidente de la brecha y por el resultado acontecido no fueron ni efectivas ni suficientes. Y en cuanto al registro de brechas solo consta el de la primera de ellas, no así la segunda y en la descripción del incidente se indica, refiriéndose a la parte reclamante, *"dice que contacto con el hotel para confirmar el fraude y que le comunicaron que ya eran conocedores de otros casos similares".*

En el documento de análisis de riesgos tampoco se contempla el control ni el registro de acceso no autorizado a la aplicación y tampoco se contempla la gestión de la cuenta en la plataforma de *Booking.com*, no considerándose riesgos de *phishing*.

En cuanto al segundo incidente, de características similares se produce en el mes de agosto de 2023. La parte reclamada ha manifestado: *"cambiamos varias veces la contraseña de Booking, la mayoría de las cuales el propio Booking nos echaba de la web y nos pedía establecer de nuevo una contraseña, no sé si por el propio Booking o porque el hacker quería retomar el control. Estuvimos así varias horas, y no fueron menos de 7 u 8 veces las que cambié la contraseña".*

Hay que señalar que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos ya que no es posible asegurar el citado derecho si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo que sean adecuadas.

La adecuación del nivel de seguridad al riesgo debe ser evaluada por el responsable y reconsiderada periódicamente en función de los resultados obtenidos, teniendo en cuenta para ello -entre otros factores- los riesgos que pueda presentar el tratamiento como consecuencia de la comunicación no autorizada de dichos datos. Las medidas técnicas y organizativas de seguridad que deben de aplicarse son las pertinentes para responder al riesgo existente, valorando, entre otros factores, el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento y los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Uno de los requerimientos que establece el RGPD para responsables y encargados del tratamiento que realizan actividades de tratamiento con datos personales es la necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información con el fin de establecer las medidas de seguridad y control orientadas a cumplir los principios de protección desde el diseño y por defecto que garanticen los derechos y libertades de las personas.

La responsabilidad de la parte reclamante viene determinada por las brechas de datos personales puestas de manifiesto, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. En este sentido, las medidas no eran apropiadas, independientemente de la brecha de datos personales producida.

Esa falta de medidas de seguridad que provoca la infracción del artículo 32.1 constituye una infracción en si misma considerada e independientemente de los incidentes de seguridad detectados, brechas de datos personales producidas.

Como precisa la STS de 15/02/2022: *"En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia" o "de comportamiento".*

En su Fundamento segundo dice: *"(…) la cuestión que reviste interés casacional consiste en determinar si las infracciones de la Ley de Protección de Datos por fallos de las medidas de seguridad (…) deben examinarse en atención al resultado y, (…) con independencia de los medios y medidas de prevención que hubiera podido adoptar.*

(…)"

Y en su Fundamento tercero: *"La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.*

(…)”

Por tanto, de conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32.1, infracción tipificada en su artículo 83.4.a) del RGPD.

VI
Tipificación de la infracción del articulo 32.1 RGPD

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

“4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43.
(…)”

La LOPDGDD en su artículo 71, *Infracciones*, señala que: *“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.*

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de *“Infracciones consideradas graves”:*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)
f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.
(…)”

VII
Propuesta de sanción por incumplimiento del articulo 32.1 RGPD

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece que:

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

- De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción a imponer en el presente caso por la infracción tipificada en el artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD de la que se responsabiliza al reclamado, en una valoración inicial, se estiman concurrentes los siguientes factores:

La naturaleza y gravedad de la infracción; los hechos puestos de manifiesto afectan a un elemento esencial del tratamiento de los datos de carácter personal, como es el de la seguridad de los mismos; hay que considerar que las medidas implantadas no eran las idóneas para garantizar un nivel de seguridad adecuado al riesgo; medidas que no eran las apropiadas y que son claves a la hora de garantizar el derecho fundamental a la protección de datos, cuya infracción la norma sanciona con gravedad.

El número de personas afectadas ya que según la parte reclamada el número de afectados puede haber sido de 24, por la primera de las quiebras y, la segunda, de características muy similares y ocurrida el 17/08/2023 aunque no se ha podido determinar el número de clientes afectados, de la información aportada se desprende que se trataría de un número bastante elevado, *"todas las rsvas (decenas por no decir más)".*

Nivel de perjuicios y daños sufridos: aunque no conste acreditado que se hubieran producido perjuicios a la reclamante, lo que no obsta para que al resto de afectados por las brechas hayan podido sufrir algún tipo de daños y perjuicios (artículo 83.2.a) del RGPD).

La intencionalidad o negligencia en la infracción. Se observa una grave falta de diligencia en el cumplimiento de las obligaciones que le impone la normativa en materia de protección de datos, pues a las inadecuadas medidas implantadas; a este respecto se puede citar la SAN de 17/10/2007 que si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...).el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto."*

La actividad de la entidad presuntamente infractora se encuentra vinculada con el tratamiento de datos de carácter personal tanto de clientes como de terceros. En la actividad de la entidad reclamada es imprescindible el tratamiento de datos de carácter personal por lo que, dado su objeto y volumen de negocio la transcendencia de la conducta objeto de la presente reclamación es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

A efectos de decidir sobre la imposición de la multa y su cuantía, de conformidad con las evidencias de que se dispone y sin perjuicio de lo que resulte de la instrucción del procedimiento, teniendo en cuenta los criterios del artículo 83.2 del RGPD con respecto a la infracción cometida, vulneración del artículo 32.1 del RGPD, se considera fijar una sanción de 2.000 euros.

VIII

Tercera obligación incumplida: infracción del artículo 33.1 del RGPD

El artículo 33 del RGPD, *Notificación de una violación de la seguridad de los datos personales a la autoridad de control,* establece que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

La obligación de notificar a la autoridad de control las brechas o quiebras que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

En este sentido el considerando 87 estable que:

"Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento".

Por su parte, esta Agencia ha indicado lo siguiente en su Guía para la notificación de brechas de datos personales (v. junio de 2021), en su el apartado IV, señala:

"La notificación de una brecha de datos personales a la Autoridad de Control conforme al artículo 33 del RGPD corresponde al responsable del tratamiento. El responsable puede autorizar una persona física, representante o entidad que ejerza su representación para que realice la notificación de la brecha de datos personales ante la Autoridad de Control.

El encargado del tratamiento que ha sido objeto de la brecha de datos personales únicamente podrá notificar en nombre del responsable si así lo tiene establecido en un contrato o vínculo legal de similar índole. En todo caso, el responsable de tratamiento debe ser previamente informado sobre la ocurrencia de la brecha de datos personales y todos los detalles relevantes como establece el artículo 33.2 del RGPD".

Hay que señalar que una vez que se tuvo conocimiento de la brecha de seguridad, el RGPD establece que el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

El RGPD también establece los casos en los que una brecha de datos personales se debe comunicar al afectado, en concreto cuando sea probable que la brecha los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Tanto la notificación a la autoridad de control competente como la comunicación al afectado son obligaciones del responsable del tratamiento, aunque puede delegar la ejecución de las mismas en otras figuras, como el encargado del tratamiento siempre que ello estuviera previsto en el correspondiente contrato de encargo.

Por tanto, el responsable tenía la obligación de notificar a la autoridad de control las quiebras de datos personales producidas, de lo que se desprende que la conducta del reclamado supone la vulneración del 33.1 del RGPD, infracción tipificada en su artículo 83.4.a) del mismo texto legal.

IX

Tipificación de la infracción del articulo 33.1 RGPD

La vulneración del artículo 33 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43.
(…)"

La LOPDGDD en su artículo 71, *Infracciones,* señala que: *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves:*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)
r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.
(…)"

X

Propuesta sanción por incumplimiento del articulo 33.1 RGPD

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece que:

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

- De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción a imponer en el presente caso por la infracción tipificada en el artículo 33.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD de la que se responsabiliza a la parte reclamada, en una valoración inicial, se estiman concurrentes los siguientes factores:

La intencionalidad o negligencia en la infracción. Se una grave falta de diligencia en el cumplimiento de las obligaciones que le impone la normativa en materia de protección de datos; a este respecto se puede citar la SAN de 17/10/2007 que si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...).el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto.",*

La actividad de la entidad presuntamente infractora se encuentra vinculada con el tratamiento de datos de carácter personal tanto de clientes como de terceros. En la actividad de la entidad reclamada es imprescindible el tratamiento de datos de carácter personal por lo que, dado su objeto y volumen de negocio la transcendencia de la conducta objeto de la presente reclamación es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

A efectos de decidir sobre la imposición de la multa y su cuantía, de conformidad con las evidencias de que se dispone y sin perjuicio de lo que resulte de la instrucción del procedimiento, teniendo en cuenta los criterios del artículo 83.2 del RGPD con respecto a la infracción cometida, vulneración del artículo 33.1 del RGPD, se considera adecuado fijar una sanción de 2.000 euros.

XI
Adopción de medidas

De confirmarse las infracciones, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Por tanto, se consideraría procedente ordenar que el reclamado en el plazo de seis meses a partir de la firmeza de la resolución sancionadora que, en todo caso, se dictare para que adecúe los tratamientos objeto del presente procedimiento a la normativa aplicable. En el texto de este acuerdo se establecen cuáles han sido los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD. Se señala como medidas a adoptar: la implantación de aquellas medidas de carácter técnico y organizativas que garanticen la seguridad de los datos e imposibiliten el acceso a los mismos por terceros de conformidad con lo señalado en los artículos 5.1.f) y 32.1 del RGPD, así como establecer de manera fehaciente aquellas que aseguren el cumplimiento de lo establecido en el artículo 33 .1 del RGPD.

Se advierte que no atender la orden impuesta por este organismo podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

` Por lo tanto, a tenor de lo anteriormente expuesto,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a PILLOW HOTELS, S.L., con NIF ***B66964255***,

- Por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD.
- Por la presunta infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD.
- Por la presunta infracción del artículo 33.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD.

SEGUNDO: NOMBRAR Instructor a ***R.R.R.*** y Secretaria a ***S.S.S.***, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los

artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO. INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que integran el expediente.

CUARTO. QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre y artículo 58.2.b) del RGPD, las sanciónes que pudieran corresponder por la vulneración de los artículos 5.1.f), 32.1 y 33.1 del RGPD sería de 3.000 €, 2.000 € y 2.000 € (tres mil euros, dos mil euros, dos mil euros) respectivamente, sin perjuicio de lo que resulte de la instrucción.

QUINTO. NOTIFICAR el presente Acuerdo a PILLOW HOTELS, S.L., con NIF ***B66964255***, indicándole expresamente su derecho a la audiencia en el procedimiento y otorgándole un plazo de DIEZ DÍAS HÁBILES para que formule las alegaciones y proponga las pruebas que considere procedentes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, en caso de que la sanción a imponer fuese de multa, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción total quedaría establecida en 5.600 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción total quedaría establecida en 5.600 euros y su pago implicará la terminación del procedimiento, sin perjuicio de las medidas que en su caso se impongan.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción total quedaría establecido en 4.200 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (5.600 o 4.200 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

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

>>

SEGUNDO**:** En fecha 16 de mayo de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **4200 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

CUARTO: En el Acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá “ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…”.

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el Acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202303565**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a ***PILLOW HOTELS, S.L.*** para que en el plazo de 6 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del Acuerdo de inicio transcrito en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a ***PILLOW HOTELS, S.L.***.

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, los interesados podrán interponer 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.

1259-16012024

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