- **Expediente Nº: PS/00078/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 08/01/2019, a través del "Sistema de Información del Mercado Interior" (en lo sucesivo IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, se recibió en esta Agencia Española de Protección de Datos (AEPD) una reclamación formulada por ***A.A.A.*** (en lo sucesivo el reclamante), ciudadano holandés, ante la autoridad de protección de datos de Países Bajos (Autoriteit Persoonsgegevens -AP). El traslado de esta reclamación a la AEPD se realiza de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en lo sucesivo Reglamento General de Protección de Datos o RGPD), teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal.

La citada reclamación se formula contra la entidad MARINS PLAYA, S.A. (en lo sucesivo MARINS PLAYA o entidad reclamada), con sede social en España, por los motivos siguientes:

El reclamante indica que en el proceso de registro del hotel le solicitaron el pasaporte, que fue escaneado digitalmente, a pesar de su oposición. El cliente se opone a que dicho documento fuese escaneado completamente alegando que no todos los datos incluidos en el mismo son necesarios, a lo que el empleado del hotel le respondió que dicho escaneo se realizaba siguiendo instrucciones de la policía. Por otro lado, asegura haber visto a los empleados del hotel con la foto del pasaporte en sus tablets.

En relación con la cuestión suscitada por el reclamante, la autoridad remitente preguntó si realmente la ley española obliga a escanear el pasaporte completamente o sólo son necesarios algunos datos para cumplir el proceso de registro.

Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, se han declarado interesadas en el presente procedimiento la autoridad de control que ha comunicado el caso (Países Bajos).

SEGUNDO: A la vista de los hechos expuestos, la Subdirección General de Inspección de Datos procedió a realizar actuaciones para su esclarecimiento, al amparo de los

poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del RGPD. En el marco de estas actuaciones, se dirigió un requerimiento a la entidad reclamada, que informó lo siguiente:

1. Al realizar el registro de entrada del cliente se escanea su pasaporte con el objetivo de pasar a texto la imagen para la incorporación de los campos correspondientes al programa de gestión hotelera.
2. Únicamente se escanea la página en la que se encuentra la identificación del cliente: los datos de identificación del viajero, en los que se comprenden el número, tipo y fecha de expedición del documento de identidad presentado, nombre y apellidos, sexo, la fecha y país de nacimiento, así como la fotografía.
3. No hay instrucciones específicas de las Fuerzas y Cuerpos de Seguridad del Estado sobre el copiado del citado documento, salvo las relativas al envío telemático de la información.
4. La información también se utiliza, contablemente, para generar las correspondientes facturas; sólo puede acceder el personal administrativo de contabilidad.
5. Cuando el cliente se registra se le proporciona una tarjeta magnética que le permite, además del acceso a la habitación, el pago de los consumos con cargo a su cuenta que abonará al finalizar su estancia; en el momento de realizar un consumo, el cliente facilita esa tarjeta al empleado, quien, al pasarla para realizar el cargo, puede comprobar la fotografía del pasaporte. Con ello se pretende verificar la identidad del cliente, a fin de evitar el uso fraudulento de la tarjeta por parte de terceros e impedir causar un grave perjuicio, económico, al cliente. Sólo puede ver la fotografía el empleado que cobra, en la tablet de TPV.
6. La normativa aplicable para la identificación de los clientes en el proceso de registro o alta en el hotel es la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y Orden INT/1922/2003 de 3 de julio.

TERCERO: Tras revisar las contestaciones obtenidas durante la fase previa de investigación, reseñada en el Hecho anterior, esta Agencia consideró que el tratamiento de datos personales objeto de la reclamación se encuentra legitimado por el artículo 6.1.c) del RGPD y es proporcionado y necesario de acuerdo con lo establecido en el artículo 24 de la Ley Orgánica 4/2015 citada, que dispone en su apartado primero: "*Las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, como las de hospedaje… quedarán sujetas a las obligaciones de registro documental e información en los términos que establezcan las disposiciones aplicables".* Y que se detalla en la Orden mencionada (Orden INT/1922/2003 de 3 de julio).

Por otra parte, se tuvo en cuenta que no se constataron los hechos denunciados referidos al escaneo de todas las páginas del pasaporte.

En segundo lugar, se concluyó que el tratamiento de datos personales consistente en el uso de la fotografía obtenido del pasaporte con la finalidad de verificar la identidad del cliente en los consumos que realiza, al realizar cargos en la cuenta de una habitación, y evitar el uso fraudulento de la tarjeta del hotel por parte de terceros distintos al usuario del servicio, está legitimado en el artículo 6.1.f) del RGPD, ya que existe un interés legítimo por parte del hotel en cobrar al verdadero usuario del servicio y para el cliente, ya que se evita que se utilicen las tarjetas de forma fraudulenta y se

carguen en la cuenta de un cliente los consumos efectuados por otros.

En consecuencia, aclaradas las dudas suscitadas, se consideró que no existían indicios de infracción, por lo que, con fecha 28/09/2020, se dictó Proyecto de Resolución de archivo de la reclamación (Draft decisión).

CUARTO: Con fecha 10/11/2020, el Proyecto de Decisión se incorporó al Sistema IMI a fin de que las autoridades interesadas se manifestaran al respecto.

Al término del plazo establecido, formuló objeciones al citado proyecto de archivo la autoridad de protección de datos de Países Bajos (Autoriteit Persoonsgegevens - AP).

En cuanto a los hechos, dicha autoridad de control advierte que el reclamante manifestó que el personal del hotel disponía en su dispositivo de la copia completa de su pasaporte (primera página), incluida su foto, y que ello difiere ligeramente de lo señalado en el Proyecto de Decisión, aunque no cambia la evaluación realizada sobre el mismo.

La AP admite que el tratamiento de los datos personales recogidos en el pasaporte (número, tipo y fecha de emisión del documento de identidad presentado, nombre y apellidos, sexo y la fecha y país de nacimiento, así como la fotografía) sea necesario para el cumplimiento de la legislación nacional y, por tanto, lícito de conformidad con el artículo 6.1.c) del RGPD, pero cuestiona el tratamiento de dichos datos personales en virtud de lo establecido en el artículo 6.1.f) del mismo RGPD, por la existencia de un interés legítimo del hotel responsable en evitar el uso fraudulento de la tarjeta que proporciona a los clientes, la cual sirve para realizar consumos en las instalaciones y también como llave de la habitación; y también del cliente, ya que impide que las tarjetas se utilicen de forma fraudulenta y se le cobren consumos realizados por otros.

Sobre este tratamiento de datos personales basado en el interés legítimo, se refiere la AP al requisito de necesidad, que exige evaluar la proporcionalidad y subsidiariedad del tratamiento, comprobando que tales intereses no puedan lograrse razonablemente de manera efectiva por otros medios menos restrictivos de los derechos y libertades fundamentales de los interesados, en particular los derechos al respeto de la vida privada y a la protección de los datos personales garantizados por los artículos 7 y 8 de la Carta. Y añade que el Tribunal de Justicia de la Unión Europea declaró, además, que el requisito relativo a la necesidad de tratamiento debe examinarse, conjuntamente, con el principio de “minimización de datos” consagrado en el artículo 5.1.c) del RGPD.

En este caso, señala la AP, existen otras formas menos intrusivas para verificar si el titular de la tarjeta magnética es el legítimo titular de la tarjeta en el momento del pago y, así, evitar que dichas tarjetas se utilicen de forma fraudulenta.

Como ejemplo de estas acciones menos intrusivas, indica la posibilidad de que el empleado del hotel, cuando se produce algún consumo, consulte algunos datos de control al cliente, como el apellido o el número de habitación, para verificar si coincide con el titular legítimo de la tarjeta; o exigir la firma de un recibo por el consumo, que también actúa como barrera para terceros. En caso de pérdida de la tarjeta, ésta puede ser bloqueada para impedir su uso fraudulento

La combinación de los escenarios anteriores requiere una cantidad mínima de procesamiento adicional de datos, es menos intrusivo y se ajustan al principio de minimización de datos. Aún así, posibilitan lograr los intereses perseguidos con prácticas comunes en la mayoría de los hoteles.

Frente a ello, la eficacia adicional que proporciona el uso de los datos personales del pasaporte para prevenir fraudes no supera la invasión de la protección de datos.

Entiende que estos datos pueden utilizarse para el fraude de identidad en caso de una violación de datos o el abuso por parte de los empleados del hotel que tienen acceso a los mismos, de modo que no se considera proporcionado su uso para evitar posibles fraudes en el pago de los servicios del hotel.

Según la AP, el tratamiento de todos estos datos es contrario al principio de minimización de datos de conformidad con el artículo 5.1.c. del RGPD, ya que el tratamiento sólo de un nombre y número de habitación es suficiente para minimizar eficazmente el fraude. Además, algunas de las categorías de datos antes mencionadas pueden considerarse categorías especiales de datos personales de conformidad con el artículo 9 del RGPD, sin que pueda aplicarse a este caso ninguna de las excepciones del artículo 9.2 del RGPD.

En resumen, la AP no comparte que el uso de los datos del pasaporte esté permitido en virtud del artículo 6.1.f del RGPD en las circunstancias indicadas. Esto podría conducir al uso de datos de pasaportes por muchos hoteles y proveedores de servicios similares, a una utilización más amplia que podría dar lugar a fraudes de identidad en casos de violaciones de datos o abusos por parte de los empleados del hotel que tienen acceso a los mismos, de modo que, ante el riesgo para las libertades y derechos expresado, no considera proporcionado su uso para evitar posibles fraudes en el pago de los servicios del hotel.

Si un hotel desea procesar los datos del pasaporte con el fin de verificar la identidad de los clientes durante su estancia, añade la AP, el hotel debe invocar otro motivo del artículo 6 del RGPD, como el consentimiento, o volver a la práctica más común, como se ha descrito anteriormente.

QUINTO: Con fecha 11/05/2021, por la Subdirección General de Inspección de Datos se accede a la información disponible sobre la entidad MARINS PLAYA en “Axesor”. ***(…).*** La citada entidad figura de alta en el código de actividad económica correspondiente a “Hoteles y alojamientos similares”.

(…).

SEXTO: Con fecha 03/06/2021, de conformidad con lo establecido en el artículo 64 de la LOPDGDD, apartados 2 (párrafo tercero) y 3, se dictó proyecto de acuerdo de inicio de procedimiento sancionador, motivado por la reclamación recibida a través del Sistema IMI que consta reseñada en el Antecedente Primero. Este proyecto toma en consideración las objeciones reseñadas en el Antecedente Cuarto (proyecto de decisión revisada).

Siguiendo el procedimiento establecido en el artículo 60 del RGPD, con fecha 25/06/2021, el citado proyecto de apertura de procedimiento sancionador fue transmitido a través del Sistema IMI a la autoridad de control interesada, haciéndole saber que, en caso de que no se formulase objeciones en el plazo de dos semanas desde la consulta, se adoptaría el preceptivo acuerdo de apertura de procedimiento sancionador.

La autoridad de control interesada no formuló objeción alguna al proyecto de acuerdo de apertura de procedimiento sancionador adoptado por la AEPD, entendiéndose, por tanto, que existe acuerdo sobre el mismo.

De conformidad con lo establecido en el artículo 64 de la LOPDGDD, el proyecto de acuerdo de inicio de procedimiento sancionador reseñado fue notificado a la entidad reclamada.

SÉPTIMO: Con fecha 15/06/2021, se recibió en esta Agencia escrito presentado por la entidad reclamada en el que solicita el archivo de las actuaciones de acuerdo con las consideraciones siguientes:

1. Describe el procedimiento que siguen en el tratamiento de los datos personales de un cliente desde su llegada al hotel, señalando que se solicita la documentación acreditativa de la identidad de todas las personas mayores de 16 años que se alojan en sus instalaciones, que se somete a un proceso de escaneo para el proceso de registro, el cual completa la ficha de recogida de datos sin guardar en los sistemas informáticos la imagen del documento.

Se trata de un reconocimiento óptico de caracteres conocido con las siglas OCR (*"Optical Character Recognition"*), que posibilita la digitalización de textos (el proceso identifica automáticamente los caracteres de un determinado alfabeto y los almacena en forma de datos). Según la reclamada, este proceso solo se aplica a la página del documento en la que se identifica al viajero, recogiendo los datos personales relativos a número, tipo y fecha de expedición del documento en cuestión (DNI, pasaporte, permiso de conducir, permiso de residencia o carta de identidad), nombre, apellidos, sexo, fecha y país de nacimiento, así como la fotografía. Seguidamente se recaba la firma del viajero en soporte digital, a través de Tablet, en la que se informa sobre la normativa de protección de datos personales; y se le proporciona una tarjeta de acceso a las habitaciones, utilizada también para el uso de los servicios del hotel.

Los datos son tratados por el personal de administración y de servicios (bar y comedor) para el pago de los consumos. Además, son remitidos a las Fuerzas y Cuerpos de Seguridad del Estado, en cumplimiento de la normativa de seguridad ciudadana.

2. Niega que el personal del hotel dispusiera en su dispositivo de la copia completa de la primera página del pasaporte del reclamante, ya que los únicos datos que aparecen en los dispositivos utilizados por el personal de bar y comedor con acceso a TPV son el número de habitación, fecha de salida, nombre y apellido del viajero, fotografía y régimen de alojamiento, necesarios para llevar a cabo el mantenimiento, desarrollo y control negocial, legitimador del tratamiento. A este respecto, destaca que, de los datos disponibles en esos dispositivos, únicamente el nombre, apellidos y fotografía

son tomados del check-in).

3. Teniendo en cuenta los datos que se utilizan para el control de los consumos y evitar el uso fraudulento de las instalaciones, no entiende la reclamada que se cuestione el interés legítimo, especialmente cuando la propia Agencia admite el tratamiento de los datos personales recogidos en el pasaporte para el cumplimiento de la legislación nacional, considerándolo lícito de acuerdo con el artículo 6.1.c) del RGPD.

Sobre las formas menos intrusivas para identificar al cliente a las que se refieren en el acuerdo de apertura, señala que solicitar de forma verbal el número de habitación o el apellido resulta insuficiente y no impide que otra persona pueda oír estos datos y utilizarlos; lo mismo que la firma de un recibo, que el empleado no podría cotejar. Añade que por estos motivos se incluyó la fotografía en los sistemas digitales del personal de bar y comedor, como medio de autenticación, incluso cuando el cliente no está en posesión de la tarjeta por olvido, extravío o sustracción.

En cuanto a los riesgos en caso de una posible violación de datos, advierte que tiene implementados los mecanismos establecidos en el RGPD y que los empleados han suscrito un contrato de confidencialidad.

4. La reclamada no trata categorías especiales de datos personales en ningún momento. Sobre esta cuestión, manifiesta que la imagen del cliente es solo una fotografía de la que no se extraen plantillas biométricas ni se utilizan para reconocimiento facial ni otros medios específicos. Por tanto, a su juicio, el tratamiento que realiza de la obtención de la fotografía que realiza no se ajusta al concepto de tratamiento de categorías especiales de datos (Considerando 51 y artículo 4.15 del RGPD).

En consecuencia, concluye la entidad reclamada que el tratamiento de los datos utilizados para autenticar la identidad de la persona que realiza un gasto no infringe lo dispuesto en el artículo 6.1.f) del RGPD, al resultar necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento (evitar perjuicios y demandas por cobros indebidos), así como del interesado (evitar cobros indebidos).

Aporta una fotografía en la que puede verse el detalle de la información disponible en los dispositivos del personal del hotel sobre una persona en concreto: en el apartado “Datos de la reserva” incluye el número de habitación, número de la reserva, número de personas y fecha de salida; en el apartado “Componentes de la reserva” se indica el nombre y apellidos de la persona, régimen, tipo de VIP y número de visitas, además de la fotografía del cliente.

OCTAVO: Con fecha 19/07/2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad MARINS PLAYA, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD; determinando que la sanción que pudiera corresponder, considerando las evidencias existentes en el momento de la apertura y

sin perjuicio de lo que resulte de la instrucción, ascendería a un total de 30.000 euros (treinta mil euros).

En el mismo acuerdo de apertura del procedimiento se advertía que la infracción imputada, de confirmarse, podrá conllevar la imposición de medidas, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD.

NOVENO: Notificado el citado acuerdo de inicio, la reclamada presentó escrito de fecha 22/07/2021, en el que solicita nuevamente el archivo del procedimiento sancionador.

En este nuevo escrito reproduce literalmente sus alegaciones anteriores, que constan reseñadas en el Antecedente Séptimo. Únicamente añade que el Considerando 47 del RGPD admite el tratamiento de datos personales necesario para la prevención del fraude en base al interés legítimo del responsable y que se considera como fraude un engaño económico llevado a cabo con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado.

DÉCIMO: Con fecha 24/082021, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por reproducidos a efectos probatorios la reclamación interpuesta, los documentos obtenidos y generados por la Subdirección General de Inspección de Datos y los Servicios de Inspección, y el Informe de Actuaciones Previas de Inspección que forma parte del expediente E/01088/2019; y por presentadas las alegaciones formuladas por MARINS PLAYA y la documentación que a ellas acompaña.

Asimismo, se acordó requerir a la entidad la entidad reclamada para que aportase la información y/o documentación siguiente:

"a) Copia del registro de todas las actividades de tratamiento de datos personales de clientes efectuadas bajo la responsabilidad de MARINS PLAYA. Dicho registro, al que se refiere el artículo 30 del RGPD, deberá aportarse en su versión inicial, junto con cualquier adición, modificación o exclusión en el contenido del mismo.

b) Si dispone de ellas, copia de la/s evaluación/es del impacto en la protección de datos personales relativa/s a cualquier tipo de operaciones de tratamiento de datos personales de clientes efectuadas bajo la responsabilidad de MARINS PLAYA que entrañen un alto riesgo para los derechos y libertades de las personas físicas.

Deberá aportarse la versión inicial de esta/s evaluación/es de impacto y, en su caso, el detalle de las modificaciones o actualizaciones que pudieran haberse realizado.

Asimismo, de haberse producido un cambio del riesgo que representen las operaciones de tratamiento y de haberse estimado necesario, deberá aportar el resultado del examen que MARINS PLAYA haya podido realizar para determinar si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos (artículo 35.11 del RGPD).

c) Copia de los documentos en los que conste la evaluación realizada sobre la prevalencia o no de los intereses y derechos fundamentales de los clientes frente a los intereses de MARINS PLAYA, en relación con las operaciones de tratamiento de datos personales de clientes efectuadas bajo la responsabilidad de MARINS PLAYA con las que se pretenda la satisfacción de intereses legítimos perseguidos por la propia entidad MARINS PLAYA o por un tercero.

d) Copia de la información en materia de protección de datos (política de privacidad) facilitada a través de cualquier canal a los clientes de esa entidad, en su versión actual y versiones anteriores vigentes a partir del 25/05/2018, en su caso, con indicación del período de vigencia de cada versión.

Si hubiera adendas o variaciones, u otros avisos de privacidad o informaciones adicionales, relativas al tratamiento de datos personales, se solicita copia de todos los documentos empleados para informar en materia de protección de datos personales distintos a la política de privacidad.

e) Detalle de los canales y procedimientos habilitados para dar a conocer a sus clientes toda la información en materia de protección de datos personales (política de privacidad o cualquier otro documento).

f) Información relativa a los canales, mecanismos y metodología utilizados por esa entidad para recabar la aceptación por parte de sus clientes de la política de privacidad o cualquier otro documento empleado por esa entidad para informar en materia de protección de datos personales; así como para la prestación de los consentimientos previstos en tales documentos, en su caso.

g) Impresiones de pantalla correspondientes a toda la información que conste registrada en su sistema de información relativa al reclamante en el expediente sancionador de referencia.

h) Detalle sobre el programa informático empleado por esa entidad para la toma de los datos de los clientes mediante escaneo de documentos y su conversión a texto".

En respuesta a este requerimiento, se recibió en esta Agencia escrito de la reclamada acompañado de la documentación que seguidamente se indica. En este escrito, dicha entidad manifestó no poder aportar las impresiones de las tablets de bar y comedor con la información sobre el reclamante disponible en estos dispositivos debido a que esta información se suprime en el momento en que el cliente hace el check-out, ni los accesos al wifi, en su caso, que son borrados a los doce meses (Ley 25/2007).

Del contenido de la documentación aportada cabe destacar lo siguiente:

1. Registro de actividades de tratamiento de datos personales de clientes.

. Finalidad: gestión contable, fiscal y administrativa;
. Categoría de interesados: clientes y usuarios;
. Tipos de datos: DNI o NIF, nombre y apellidos, dirección postal o electrónica, teléfono, imagen y firma manual;
. Otro tipo de datos: características personales, circunstancias sociales, información comercial, transacciones de bienes y servicios;
. Cesiones: Fuerzas y Cuerpos de Seguridad.
. Acceso a equipos: se accede mediante usuario y contraseña personalizados.

2. Análisis de riesgo sobre el tratamiento de datos personales de clientes.

Después de analizar la estructura de datos, el cumplimiento normativo, la organización y recursos, así como la seguridad desde el diseño y por defecto, se concluye que *"no existen riesgos en los recursos utilizados"*.

3. Información en materia de protección de datos (política de privacidad) facilitada a

través de la web de la entidad reclamada.

a) Aporta copia de la “Hoja de Registro”, que incluye un apartado relativo al establecimiento y otro a los “datos del viajero” (número de documento de identidad, tipo de documento y fecha de expedición, nombre, apellidos, sexo, fecha de nacimiento, país de nacionalidad, fecha de entrada y firma del viajero). Esta “Hoja” incluye una leyenda informativa en materia de protección de datos personales que detalla, entre otros aspectos, la identidad del responsable, la finalidad para la que serán tratados los datos, la inexistencia de comunicaciones de datos salvo por obligación legal, los derechos del interesado, modo de ejercicio y posibilidad de interponer reclamación ante la AEPD.

Se acompaña una actualización de esta “Hoja Registro” (2019) que contiene una nueva cláusula informativa. En esta se informa sobre la recogida y tratamiento de los datos con la finalidad de prevención, investigación, detección o enjuiciamiento de infracciones penales al amparo de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana; que los datos se conservarán durante tres años y estarán a disposición de las Fuerzas y cuerpos de Seguridad; derechos de los interesados y modo de ejercitarlos y posibilidad de reclamar ante la AEPD.

Por otra parte, la entidad reclamada aporta copia de la política de protección de datos disponible en su web. Se distribuye en dos partes, que denomina *“Política de Privacidad”* y *“Cláusulas de segunda capa”* (esta última parte se encuentra divida en epígrafes: fichero de clientes reserva, facturas/contabilidad, newsletter, usuarios web, empleados, etc.).

El apartado *“Política de Privacidad”* está referido a los datos personales recabados de los clientes *“con el fin de prestarles los servicios contratados consistentes en la reserva de alojamiento en establecimientos hoteleros”*.

En la información de *“Segunda capa”*, epígrafe *“Fichero de clientes reserva”* se informa que la reclamada trata la información que los clientes facilitan *“con el fin de prestarles el servicio y venderle los productos solicitados, realizar la facturación del mismo y gestionar el envío de información y prospección comercial”*.

En esta información, nada se indica sobre la utilización de la fotografía del cliente para el control de los consumos y evitar el uso fraudulento de las instalaciones.

4. Impresión de pantalla correspondiente a la información registrada relativa al reclamante (datos durante el check-in). Se presenta con el rótulo *“Carga de datos de la ficha del cliente”*, e incluye campos relativos a nombre y apellidos, número de documento y fecha de expedición, nacionalidad, fecha de nacimiento, últimas visitas y fotografía. Según esta información, la entrada en el hotel del reclamante tuvo lugar en fecha 27/08/2018.

5. Detalle sobre el programa informático (******PROGRAMA.1”***) empleado para la toma de los datos de los clientes mediante escaneo de documentos y su conversión a texto, facilitado por la empresa desarrolladora del software:

“Procedimiento de captura de datos de los clientes mediante escaneo de documentos.
En el momento de la entrada en el hotel se solicita al cliente su DNI/PASAPORTE para hacer

el escaneo de dicho documento. En este escaneo y mediante un proceso OCR (de la empresa…) se capturan los datos y se integran en la base de datos ya que son necesarios para cumplimentar 2 documentos imprescindibles en el normal funcionamiento del hotel:

1. Rellenar el parte de entrada de viajeros. La recogida y tratamiento de estos datos se hará conforme l Reglamento (UE) 2016/679, de 27 de abril (GDPR) y a Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), con la finalidad de prevención, investigación, detección o enjuiciamiento de infracciones penales, y al amparo de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, artículo 25.1.
2. Emisión de la facturación de los gastos realizados en el hotel.

La imagen con la foto del cliente se captura y se guarda para securizar el proceso de crédito a clientes en los diferentes departamentos ya que facilita al personal del hotel la identificación del cliente que está haciendo uso de la tarjeta del crédito o habitación. De igual forma permite identificar a dicho cliente por parte del personal del hotel a la hora de controlar el acceso al establecimiento".

DECIMOPRIMERO: Con fecha 29/11/2021 se formuló propuesta de resolución en el sentido siguiente:

1. Que por la Directora de la Agencia Española de Protección de Datos se sancione a la entidad MARINS PLAYA, por una infracción del Artículo 6 del RGPD, tipificada en el Artículo 83.5.a) del RGPD y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, con una multa de 30.000 euros (treinta mil euros).

2. Que por la Directora de la Agencia Española de Protección de Datos se imponga a la entidad MARINS PLAYA, S.A., en el plazo que se determine, la adopción de las medidas necesarias para adecuar su actuación a la normativa de protección de datos personales, con el alcance expresado en el Fundamento de Derecho VI de la citada propuesta de resolución.

DECIMOSEGUNDO: Notificada la citada propuesta de resolución, con fecha 15/12/2021 se recibe escrito de la entidad reclamada en el que reitera su petición de archivo del procedimiento, fundamentando su solicitud en las alegaciones siguientes:

1. El reclamante, durante el proceso de registro en el establecimiento hotelero, que tuvo lugar el 27/08/2018, tres meses después de la entrada en vigor del RGPD, facilitó su pasaporte sin mostrar oposición alguna. En ese momento fue informado sobre los extremos que impone el RGPD mediante un documento informativo redactado en español y tenía a su disposición un "display" con una cláusula informativa relativa a los tratamientos de datos que se realizaban. Actualmente, esta información se facilita en los idiomas más frecuentes entre los clientes de la entidad.

2. El Considerando 47 del RGPD recoge de manera expresa que el tratamiento de datos personales estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento, que opera *"ex lege"* cuando el tratamiento obedece a esta finalidad y concurran los parámetros que deben ser tenidos en cuenta para realizar la ponderación, como son que el interesado sea cliente o está al servicio, la realización de un análisis previo y que los tratamientos no se produzcan en circunstancias en las que el interesado no espere que se realice un tratamiento posterior (la perspectiva del interesado).

En este caso, se da el primer aspecto; el segundo fue objeto de análisis cuando se implantó la solución tecnológica para el check-in, concluyéndose la necesidad de informar, limitar el acceso a la imagen exclusivamente a los operadores de cobro por consumo y conservar el dato solo durante la estancia del cliente; además, la identificación por imagen ha sido valorada favorablemente por los clientes, pues han evitado cargos erróneos, especialmente cuando se ofertan estancias de *"todo incluido"*.

3. No existen alternativas que ofrezcan igual garantía minimizando el tratamiento de la información personal.

Reitera que las propuestas de la autoridad de protección de datos de Países Bajos sobre otras prácticas menos intrusivas, como son la consulta al interesado de algunos datos (apellido o número de habitación) o la firma de un recibo, no son efectivas o implican el tratamiento de otros datos, como la firma, que no tienen menor exigencia de protección.

4. La imagen del cliente solo se visualiza por el personal que atiende los pagos por consumo, que suscriben un documento de confidencialidad, no se realiza ningún otro tratamiento de dicha imagen y se elimina al finalizar la estancia del cliente.

5. La argumentación sostenida por la reclamada es la que sostuvo la propia Agencia cuando estimó inicialmente que no existían indicios de infracción.

Con su escrito de alegaciones, MARINS PLAYA aporta copia del documento informativo al que se refiere en sus alegaciones. En este documento se explica el proceso de check-in y el tratamiento de la imagen del documento identificativo mediante un programa de reconocimiento de caracteres. En relación con la fotografía se indica lo siguiente:

"Asimismo, la foto que aparece en el pasaporte o DNI que haya proporcionado para el check-in será registrada en el sistema de gestión hotelera del hotel de destino. La finalidad es permitir al personal del hotel identificarle como un cliente alojado y controlar el cargo de los consumos que realice durante su estancia a su habitación. Esta foto será suprimida en el momento del check-out.

Este tratamiento se basa sobre nuestro interés legítimo en identificar a los clientes alojados para fines de seguridad y de control de cargos. Para la ponderación de este interés respecto a sus derechos y libertades se ha determinado que el tratamiento tenía un impacto limitado en su privacidad, ya que:
- Prexiste una relación contractual y el tratamiento s realicen en conexión con dicha relación;
- Esta medida de seguridad beneficia a los propios clientes al garantizar la correcta imputación de los cargos a su habitación y evitar posibles suplantaciones;
- El acceso a su imagen es restringido al personal del hotel;
- El plazo de conservación de su imagen queda limitado al tiempo de su estancia".

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

1. La entidad MARINS PLAYA está dedicada a la prestación de servicios hoteleros y de alojamientos similares.

2. Para el registro de clientes (check-in), en el momento de la llegada de éstos al hotel, solicita la documentación identificativa y la somete a un proceso de escaneo que posibilita la digitalización de textos (el proceso identifica automáticamente los caracteres de un determinado alfabeto y los almacena en forma de datos), mediante un programa informático de reconocimiento óptico de caracteres (OCR). Este proceso convierte la imagen en texto e incorpora los datos al programa de gestión hotelera, cumplimentando la *"ficha del cliente"* o *"parte de entrada de viajeros"*, con campos relativos a número, tipo y fecha de expedición del documento de identidad presentado, nombre y apellidos, sexo, fecha y país de nacimiento. Este proceso aplicado por la entidad reclamada también incorpora a su base de datos la fotografía del cliente.

En este momento se facilita al cliente una tarjeta magnética que puede utilizar tanto para el acceso a la habitación como para hacer uso de los servicios del hotel.

3. Los datos recabados del cliente por MARINS PLAYA son tratados por el personal de administración y de servicios (bar y comedor); y son remitidos a las Fuerzas y Cuerpos de Seguridad del Estado, en cumplimiento de la normativa de seguridad ciudadana.

El personal de servicios utiliza un dispositivo que tiene incorporada información relativa a los clientes: en el apartado *"Datos de la reserva"* incluye el número de habitación, número de la reserva, número de personas y fecha de salida; en el apartado *"Componentes de la reserva"* se indica el nombre y apellidos de la persona, régimen, tipo de VIP y número de visitas, además de la fotografía del cliente.

La entidad MARINS PLAYA ha manifestado que la imagen con la foto del cliente se utiliza para facilitar al personal del hotel la identificación del cliente que está haciendo uso de la tarjeta del crédito o habitación (en el momento de realizar un consumo, el cliente facilita esa tarjeta al empleado, quien, al pasarla para realizar el cargo, puede comprobar la fotografía), así como para controlar el acceso al establecimiento.

4. El Registro de Actividades de Tratamiento (RAT) aportado por MARINS PLAYA incluye la siguiente información sobre el tratamiento de datos personales de clientes:

. Finalidad: gestión contable, fiscal y administrativa;
. Categoría de interesados: clientes y usuarios;
. Tipos de datos: DNI o NIF, nombre y apellidos, dirección postal o electrónica, teléfono, imagen y firma manual;
. Otro tipo de datos: características personales, circunstancias sociales, información comercial, transacciones de bienes y servicios;
. Cesiones: Fuerzas y Cuerpos de Seguridad.
. Acceso a equipos: se accede mediante usuario y contraseña personalizados.

5. MARINS PLAYA ha manifestado durante la instrucción del procedimiento que después del escaneo del documento identificativo del cliente, realizado durante el

proceso de registro, se recaba la firma del viajero en soporte digital, a través de Tablet, en la que se informa sobre la normativa de protección de datos personales.

MARINS PLAYA ha aportado a las actuaciones copia de la *"Hoja de Registro"*, que incluye un apartado relativo al establecimiento y otro a los "datos del viajero" (nº de documento de identidad, tipo de documento y fecha de expedición, nombre, apellidos, sexo, fecha de nacimiento, país de nacionalidad, fecha de entrada y firma del viajero). Esta *"Hoja"* incluye una leyenda informativa en materia de protección de datos personales que detalla, entre otros aspectos, la identidad del responsable, la finalidad para la que serán tratados los datos, la inexistencia de comunicaciones de datos salvo por obligación legal, los derechos del interesado, modo de ejercicio y posibilidad de interponer reclamación ante la AEPD.

Consta, asimismo, una actualización de esta *"Hoja Registro"* (2019) que contiene una nueva cláusula informativa. En esta se informa sobre la recogida y tratamiento de los datos con la finalidad de prevención, investigación, detección o enjuiciamiento de infracciones penales al amparo de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana; que los datos se conservarán durante tres años y estarán a disposición de las Fuerzas y cuerpos de Seguridad; derechos de los interesados y modo de ejercitarlos y posibilidad de reclamar ante la AEPD.

6. MARINS PLAYA ha aportado a las actuaciones el detalle sobre la información en materia de protección de datos (política de privacidad) que facilita a través de su web. En esta información, nada se indica sobre la utilización de la fotografía del cliente para el control de los consumos y evitar el uso fraudulento de las instalaciones.

7. Los datos personales del reclamante constan registrados en el Sistema de Información de MARINS PLAYA. Se presenta con el rótulo *"Carga de datos de la ficha del cliente"*, e incluye campos relativos a nombre y apellidos, número de documento y fecha de expedición, nacionalidad, fecha de nacimiento, últimas visitas y fotografía. Según esta información, la entrada en el hotel del reclamante tuvo lugar en fecha 27/08/2018.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada Autoridad de Control y, según lo establecido en los artículos 47, 64.2 y 68.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar este procedimiento.

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 RGPD, 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"*.

Los apartados 1) y 2), del artículo 58 el RGPD, enumeran, respectivamente, los poderes de investigación y correctivos que la autoridad de control puede disponer al

efecto, mencionando en el punto 1.d) el de: "*notificar al responsable o encargo del tratamiento las presuntas infracciones del presente Reglamento"*; y en el 2.i) el de: "*imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso".*

El caso examinado está motivado por una reclamación de carácter transfronterizo formulada ante la autoridad de protección de datos de Países Bajos (Autoreit Persoonsgegevens -AP), contra MARINS PLAYA, que tiene sede en España. Dicha sede es el establecimiento principal de la citada entidad, en el sentido de la definición del artículo 4.16 del RGPD. Así, conforme a lo dispuesto en el artículo 56.1 del RGPD, la AEPD es la competente para actuar como autoridad de control principal.

Se tienen en cuenta las siguientes *"definiciones"* establecidas en el artículo 4 del RGPD:

"16) establecimiento principal:
a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal".

"21) autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51".

"22) autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
a.- El responsable o encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
b.- Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o
c.- Se ha presentado una reclamación ante esa autoridad de control".

"23) tratamiento transfronterizo:
a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro,
o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro".

Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, en el presente procedimiento actúa en calidad de *"autoridades de control interesadas"* la autoridad de protección de datos personales de Países Bajos (Autoriteit Persoonsgegevens -AP).

II

El artículo 56.1 del RGPD, relativo a la *"Competencia de la autoridad de control principal"*, establece lo siguiente:

"1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60".

Dicho artículo 60 regula la *"Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas"*:

"1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.
2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.
3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.
4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.
5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.
6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.
7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.
(…)
12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado".

Sobre las cuestiones reguladas en estos preceptos, se tiene en cuenta lo señalado en los Considerandos 124, 125, 126 y 130 del RGPD, en particular lo siguiente:

(124) "…Dicha autoridad (la autoridad principal) debe cooperar con las demás autoridades interesadas…".
(125) "En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones".
(126) "La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas…".
(130) "Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente".

De acuerdo con lo establecido en el artículo 4.24 del RGPD, se entiende por *"objeción pertinente y motivada"* lo siguiente:

"La objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión".

De conformidad con lo establecido en las normas anteriores, en el presente supuesto, referido a una reclamación presentada ante la autoridad de control de un Estado miembro (Países Bajos), en relación con tratamientos en el contexto de las actividades de un establecimiento de un responsable que afectan o es probable que afecten sustancialmente a interesados en más de un Estado miembro (tratamientos de datos transfronterizos), la autoridad de control principal, en este caso la Agencia Española de Protección de Datos, está obligada a cooperar con las demás autoridades interesadas.

La Agencia Española de Protección de Datos, en aplicación de los poderes que le confiere el RGPD, es la competente para adoptar las decisiones concebidas para producir efectos jurídicos, ya sea la imposición de medidas que garanticen el cumplimiento de las normas o la imposición de multas administrativas. No obstante, viene obligada a implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones y tener en cuenta su opinión en la mayor medida. Se establece, asimismo, que la decisión vinculante que deba adoptarse se acuerde conjuntamente.

El artículo 60 del RGPD regula esta cooperación entre la autoridad de control principal y las demás autoridades de control interesadas. El apartado 3 de este artículo establece expresamente que la autoridad de control principal transmitirá a las demás autoridades de control interesadas, sin dilación, un proyecto de decisión para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista, siguiendo para ello el procedimiento previsto en los apartados 4 y siguientes. Las autoridades de control interesadas disponen de un plazo de cuatro semanas para formular objeciones motivadas acerca del proyecto de decisión, entendiéndose que

existe acuerdo sobre dicho proyecto si ninguna autoridad presenta objeciones en el plazo indicado, en cuyo caso todas ellas quedan vinculadas por el repetido proyecto.

En otro caso, es decir, si cualquiera de las autoridades interesadas formula una objeción pertinente y motivada acerca del proyecto de decisión, la autoridad de control principal podrá seguir lo indicado en la objeción, presentando a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado, que se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas. De no seguir lo indicado en la objeción o si se estima que la misma no es pertinente, la autoridad de control principal debe someter el asunto al mecanismo de coherencia contemplado en el artículo 63 del RGPD.

En el presente caso, la AEPD estimó inicialmente que no existían indicios de infracción, por lo que, con fecha 28/09/2020, se dictó Proyecto de Decisión, mediante el que se sometía a la consideración del resto de autoridades de control interesadas el archivo de la reclamación (Draft decisión).

Al término del plazo establecido, formuló objeciones al citado Proyecto de Decisión la autoridad de protección de datos de Países Bajos (Autoriteit Persoonsgegevens -AP), en el sentido expresado en los Antecedentes del presente acto.

Teniendo en cuenta los motivos expuestos en las objeciones formuladas, y de conformidad con lo establecido en el apartado 1 del artículo 60 del RGPD, antes transcrito, que obliga a la autoridad de control principal a cooperar con las demás autoridades, esforzándose por llegar a un consenso, se siguió el procedimiento previsto en el apartado 5 del citado artículo 60, en lugar de acudir al mecanismo de coherencia contemplado en el artículo 63 del RGPD.

Aunque esta Agencia consideró inicialmente que no existían indicios de infracción, una vez analizadas las observaciones u objeciones planteadas por la autoridad de control interesada se pusieron de manifiesto algunas circunstancias que no habían sido suficientemente valoradas en el proyecto de archivo de actuaciones (Draft decisión), que serán expuestas en los Fundamentos de Derecho que siguen.

Por ello, procedía la elaboración de un Proyecto de Decisión Revisado que contemplase la apertura de un procedimiento sancionador a MARINS PLAYA.

Esta actuación es acorde con el procedimiento de cooperación regulado en el artículo 60 del RGPD; y tiene en cuenta lo establecido en el artículo 58.4 del mismo Reglamento, según el cual el ejercicio de los poderes conferidos a la autoridad de control debe respetar las garantías procesales establecidas en el Derecho de la Unión y de los Estados miembros.

Las normas procesales españolas, en concreto, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), establece que los procedimientos de naturaleza sancionadora se iniciarán siempre de oficio por acuerdo del órgano competente, el cual debe contener, entre otras indicaciones, la identificación de la persona o personas presuntamente responsables, los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder

La adopción de este proyecto de acuerdo de inicio de procedimiento sancionador está prevista en el artículo 64 de la LOPDGDD, apartados 2 (párrafo tercero) y 3, estableciéndose la obligación de dar conocimiento formal al interesado. Esta notificación interrumpe la prescripción de la infracción.

El Proyecto de Decisión Revisado elaborado por la AEPD, en forma de proyecto de apertura de procedimiento sancionador, fue sometido a la consideración de la autoridad interesada, a fin de que formulase las objeciones que estimasen pertinentes o prestase su conformidad. Para ello, fue transmitido a través del Sistema IMI a dichas autoridades, haciéndole saber que, en caso de que no formulase objeciones en el plazo de dos semanas desde la consulta, se adoptaría el preceptivo acuerdo de apertura de procedimiento sancionador. La autoridad de control interesada no formuló objeción alguna, por lo que se entendió que existía acuerdo sobre el citado proyecto.

En consecuencia, con fecha 19/07/2021, la AEPD acordó iniciar el presente procedimiento sancionador, de acuerdo con los argumentos y las imputaciones contenidas en el Proyecto de Decisión Revisado.

Por otra parte, en el apartado 4 del citado artículo 64 de la LOPDGDD establece que los plazos de tramitación establecidos en este artículo quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de los Estados miembros conforme con lo establecido en el RGPD, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

III

El artículo 6 del RGPD se refiere a la *"Licitud del tratamiento"* en los términos siguientes:

Artículo 6 del RGPD.
"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:
a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.
La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".

Se tiene en cuenta lo expresado en los considerandos 40 a 45 y 47 del RGPD en relación con lo establecido en los artículos 6 y 7 del RGPD antes reseñados.

En el presente caso, se formula reclamación contra la entidad MARINS PLAYA por realizar, durante el proceso de registro del reclamante en el hotel, un escaneo digital de su pasaporte, de todo el documento, a pesar de la oposición manifestada por el mismo; así como por la utilización de los datos personales contenidos en el citado documento, incluida la fotografía, para el control y facturación de los consumos del cliente durante su estancia.

Las actuaciones desarrolladas han permitido constatar que el proceso de escaneado al que se somete el documento identificativo del cliente a su llegada al hotel no tiene por objeto obtener una imagen digital de todo el documento. Según consta detallado en el Hecho Probado 2, dicho escaneo se realiza utilizando un programa informático

de reconocimiento óptico de caracteres (OCR) que identifica automáticamente los caracteres de un determinado alfabeto y los almacena en forma de datos, es decir, convierte la imagen en texto. Se trata de un programa de apoyo que captura los datos del cliente, los integra en el sistema de información de la entidad y posibilita la cumplimentación de la *"ficha del cliente"* o *"parte de entrada de viajeros"*.

No existe prueba que acredite que la entidad responsable disponga de una imagen completa del documento de identidad de los clientes. Tampoco consta que la imagen escaneada de este documento se incorporase a los dispositivos que utiliza el personal de servicios del hotel (bar y comedor).

Si consta acreditado, en cambio, y así lo ha reconocido la propia entidad MARINS PLAYA, que mediante aquel proceso la citada entidad recaba los datos personales de sus clientes relativos a número, tipo y fecha de expedición del documento de identidad presentado, nombre y apellidos, sexo, la fecha y país de nacimiento, así como la fotografía; y que son remitidos a las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de la normativa de seguridad ciudadana y utilizados para la *"gestión hotelera"*, según los términos empleados por la propia entidad en su respuesta a los Servicios de Inspección de la AEPD.

Esto incluye la utilización de los datos personales por el personal de administración y de servicios. Según la documentación aportada por la entidad reclamada, el personal de servicios utiliza un dispositivo que tiene incorporada información relativa a los clientes, que incluye el número de habitación y de la reserva, número de personas y fecha de salida; nombre y apellidos de la persona, régimen, tipo de VIP y número de visitas, además de la fotografía del cliente, que se comprueba para verificar la identidad del cliente cuando realiza consumos en el hotel; pero no disponen de la imagen escaneada del documento de identidad.

Los datos recabados, salvo la fotografía, resultan necesarios para la ejecución del contrato en el que el interesado es parte y para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Por tanto, el tratamiento de estos datos queda amparado por lo establecido en el artículo 6.1, letras b) y c), del RGPD.

La normativa que regula los libros-registros y partes de entrada de viajeros en establecimientos de hostelería, así como la obligación de comunicar la información contenida en las hojas-registro a las dependencias policiales, está constituida, básicamente, por la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y la Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos.

El artículo 24 de la Ley Orgánica 4/2015 dispone en su apartado primero lo siguiente:

"Las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, como las de hospedaje… quedarán sujetas a las obligaciones de registro documental e información en los términos que establezcan las disposiciones aplicables".

Esta norma, y la Orden mencionada, en la que se detallan aquellas obligaciones, legitima la recogida de los datos personales relativos a número de documento de

identidad, tipo de documento y fecha de expedición, nombre y apellidos, sexo, fecha de nacimiento y país de nacionalidad, fecha de entrada y firma del viajero; los cuales deben incorporarse a la “Hoja-registro” que la entidad responsable del hotel debe trasladar a las Fuerzas y Cuerpos de Seguridad del Estado.

Resta, por tanto, determinar el alcance que debe otorgarse, desde el punto de vista de la protección de datos personales, a la recogida y utilización de las fotografías de los clientes que lleva a cabo MARINS PLAYA.

Sobre esta cuestión, lo primero que debe destacarse es que la información en materia de protección de datos personales que la entidad reclamada facilitaba a los clientes no incluía ningún detalle sobre la recogida y utilización de la fotografía, por lo que eran desconocidas por los interesados. De hecho, ni siquiera el tratamiento de datos a que es sometida la fotografía figura en el Registro de Actividades de Tratamiento.

Debe rechazarse, por tanto, lo manifestado por MARINS PLAYA en su escrito de alegaciones a la propuesta de resolución cuando señala que los clientes eran informados durante el proceso de registro en el establecimiento hotelero. Es cierto que con este escrito de alegaciones ha aportado un documento informativo que sí hace referencia al registro de la fotografía en los sistemas de la entidad, pero no ha acreditado la entrega de este documento a los clientes y tampoco ha justificado cuándo implantó su utilización.

A este respecto, interesa destacar que en la fase de pruebas del procedimiento el instructor requirió expresamente a la entidad reclamada copia de su política de privacidad, en todas sus versiones vigentes a partir de 25/05/2018 y de cualquier aviso de privacidad o informaciones adicionales, además de un detalle sobre los canales habilitados para dar a conocer esta información, y dicha entidad no aportó el documento informativo que ahora aporta con sus alegaciones a la propuesta de resolución.

En relación con las fotografías de los clientes, MARINS PLAYA ha manifestado que dicha imagen se utiliza para facilitar al personal del hotel la identificación del cliente que está haciendo uso de la tarjeta del crédito o habitación (en el momento de realizar un consumo, el cliente facilita esa tarjeta al empleado, quien, al pasarla para realizar el cargo, puede comprobar la fotografía), así como para controlar el acceso al establecimiento. Cuando el cliente se registra, se le proporciona una tarjeta magnética que le permite, además del acceso a la habitación, el pago de los consumos con cargo a su cuenta, que abonará al finalizar su estancia. En el momento de realizar un consumo, el cliente facilita esa tarjeta al empleado, quien, al pasarla por su dispositivo para realizar el cargo, ve la fotografía del cliente.

La recogida y utilización de las fotografías de los clientes no quedan amparadas por las bases jurídicas antes indicadas (ejecución del contrato y cumplimiento de una obligación legal).

Según MARINS PLAYA, se pretende verificar la identidad del cliente a fin de evitar el uso fraudulento de la tarjeta por parte de terceros e impedir causar un grave perjuicio económico al cliente; que no se abonen gastos con una tarjeta extraviada que no corresponda al usuario del servicio. En base a ello, considera la citada entidad que

este tratamiento está amparado por lo dispuesto en el artículo 6.1.f) del RGPD, ya que existe un interés legítimo del responsable en cobrar al verdadero usuario del servicio y del cliente, evitando la utilización de las tarjetas de forma fraudulenta y que se carguen en las cuentas de unos clientes los consumos efectuados por terceros.

Se invoca la existencia de un interés legítimo de la entidad responsable y del propio cliente como base jurídica que presta cobertura al tratamiento de la fotografía de los clientes.

En relación con la base jurídica del interés legítimo, el artículo 6 citado establece:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño...".

El Considerando 47 del RGPD precisa el contenido y alcance de esta base legitimadora del tratamiento:

"(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo".

Los criterios interpretativos que se extraen de este Considerando son, entre otros, (i) que el interés legítimo del responsable prevalezca sobre los intereses o derechos y libertades fundamentales del titular de los datos, a la vista de las expectativas razonables que éste tenga, fundadas en la relación que mantiene con el responsable del tratamiento; (ii) será imprescindible que se efectúe una "*evaluación meticulosa*" de los derechos e interés en juego, también en aquellos supuestos en los que el interesado pueda prever de forma razonable, en el momento y en el contexto de la recogida de datos, que pueda producirse el tratamiento con tal fin; (iii) los intereses y derechos fundamentales del titular de los datos personales podrían prevalecer frente a los intereses legítimos del responsable cuando el tratamiento de los datos se efectúe en circunstancias tales en las que el interesado "*no espere razonablemente*" que se lleve a cabo un tratamiento ulterior de sus datos personales.

MARINS PLAYA no ha justificado este interés legítimo de forma suficiente para permitir la prueba de ponderación entre el interés del responsable y los derechos del interesado, necesaria para determinar la licitud de los tratamientos llevados a cabo. En este caso, además, no consta que la citada entidad haya realizado esa prueba de ponderación y haya informado debidamente al reclamante sobre esta base legitimadora.

Durante la fase de prueba del procedimiento, el instructor solicitó expresamente a la reclamada que aportara *"Copia de los documentos en los que conste la evaluación realizada sobre la prevalencia o no de los intereses y derechos fundamentales de los clientes frente a los intereses de MARINS PLAYA, en relación con las operaciones de tratamiento de datos personales de clientes efectuadas bajo la responsabilidad de MARINS PLAYA con las que se pretenda la satisfacción de intereses legítimos perseguidos por la propia entidad MARINS PLAYA o por un tercero".* Esta entidad respondió a la solicitud de prueba acordada, pero no aportó documentación alguna relativa al tratamiento de datos personales basados en el interés legítimo.

La entidad reclamada no realizó este análisis previo, aunque se refiera al mismo en su escrito de alegaciones a la propuesta, y en ningún momento informa a los clientes sobre esta base jurídica del tratamiento. Sobre el documento informativo aportado con dicho escrito de alegaciones, que contiene una referencia al interés legítimo, nos remitimos a lo indicado anteriormente sobre dicho escrito informativo.

Al faltar la información relativa a la prueba de ponderación, el interesado se ve privado de su derecho a conocer la base jurídica del tratamiento alegada por el responsable, y en concreto, al referirse al interés legítimo, se ve privado de su derecho a conocer cuáles son dichos intereses legítimos alegados por el responsable o de un tercero que justificarían el tratamiento sin tener en cuenta su consentimiento.

Del mismo modo, el interesado se ve privado de su derecho a alegar por qué causas dicho interés legítimo alegado por el responsable podría ser contrarrestado por los derechos o intereses del interesado. No habiéndosele dado oportunidad al interesado de alegarlos frente al responsable, cualquier sopesamiento que realice el responsable sin tener en cuenta las circunstancias que pudiera alegar el interesado a quien no se la ha permitido hacerlo estaría viciado, por ser un acto contrario a una norma imperativa.

Es difícil aceptar que un tratamiento se base en el interés legítimo del responsable cuando ese tratamiento se lleva a cabo de forma oculta.

No cabe, por tanto, invocar esta base jurídica del interés legítimo con ocasión de un trámite administrativo, como el de traslado de la reclamación o el de alegaciones a la apertura del procedimiento sancionador. Aceptarlo sería tanto como admitir un interés legítimo sobrevenido, o a posteriori, respecto del cual no se han respetado las exigencias previstas en la normativa de protección de datos personales y sobre el que no se informa a los interesados.

Aunque el interés legítimo no es aplicable, interesa analizar los términos en que debe llevarse a cabo la ponderación que prevé el artículo 6.1.f) del RGPD entre el legítimo interés del responsable de los datos y la protección de datos de carácter personal del

interesado, es decir, cómo juega dicho interés legítimo, si fuera aplicable.

El TJUE, en su sentencia de 04/05/2017, C-13/16, Rigas Satskime, apartado 28 a 34, determinó cuáles son los requisitos para que un tratamiento pueda resultar lícito sobre la base del interés legítimo. La sentencia TJUE de 29/07/2019, C-40/17, Fashion ID, haciéndose eco de la sentencia citada, recoge dichos requisitos.

28. A tal respecto, el artículo 7, letra f), de la Directiva 95/46 -(actual artículo 6.1.f) del RGPD)- *fija tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento sea necesario para la satisfacción de ese interés legítimo y, tercero, que no prevalezcan los derechos y libertades fundamentales del interesado en la protección de los datos.*

Esta base jurídica requiere la existencia de intereses reales, no especulativos y que, además, sean legítimos. Y no solo la existencia de ese interés legítimo significa que puedan realizarse aquellas operaciones de tratamiento. Es preciso también que estos tratamientos sean necesarios para satisfacer ese interés y considerar la repercusión para el interesado, el nivel de intrusismo en su privacidad y los efectos que pueden repercutirle negativamente.

En cuanto al primero de los requisitos, es decir, que el responsable del tratamiento o terceros persigan un interés legítimo, como es evitar el uso fraudulento de la tarjeta que la reclamada entrega a sus clientes, nos encontramos ante un interés que podría considerarse legítimo en sí mismo, si bien habrá de ser ponderado dicho interés con el de los particulares. Esto es, aunque el responsable tenga dicho interés legítimo, ello no significa, en sí mismo considerado, que pueda simplemente invocarse esta base jurídica como fundamento del tratamiento. La legitimidad de este interés es solo un punto de partida, uno solo de los elementos que deben ponderarse.

En cuanto al segundo de los requisitos, sin embargo, se considera que el tratamiento de datos personales que realiza MARINS PLAYA no es necesario o estrictamente necesario para la satisfacción del interés legítimo alegado (la sentencia citada de 04/05/2017, C-13/16, Rigas Satskime, en su apartado 30, declara "*Por lo que atañe al requisito de que el tratamiento de datos sea necesario, procede recordar que las excepciones y restricciones al principio de protección de los datos de carácter personal deben establecerse sin sobrepasar los límites de lo estrictamente necesario"*).

Este principio, según el cual el tratamiento debe ser estrictamente necesario para la satisfacción del interés legítimo, hay que interpretarlo de conformidad con lo establecido en el artículo 5.1.c) RGPD, que hace referencia al principio de minimización de datos, señalando que los datos personales serán *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*.

De esta forma, deberán preferirse siempre medios menos invasivos para servir a un mismo fin. Necesidad supone aquí que el tratamiento resulte imprescindible para la satisfacción del referido interés, de modo que, si dicho objetivo se puede alcanzar de forma razonable de otra manera que produzca menos impacto o menos intrusiva, el interés legítimo no puede ser invocado.

El término "*necesidad*" que utiliza el artículo 6.1 f) del RGPD tiene a juicio del TJUE un significado propio e independiente en la legislación comunitaria. Se trata de un "*concepto autónomo del Derecho Comunitario"* (STJUE de 16/12/2008, asunto C-524/2006, apartado 52). De otra parte, el Tribunal Europeo de Derechos Humanos (TEDH) ha ofrecido también directrices para interpretar el concepto de necesidad. En su Sentencia de 25/03/1983 precisó que, Sin perjuicio de que el tratamiento de los datos de los reclamantes sea *"útil"*, *"deseable"* o *"razonable"*, como precisó el TEDH en su Sentencia de 25/3/1983, el término *"necesario"* no tiene la flexibilidad que está implícita en esas expresiones.

Cuanto más *"negativo"* o *"incierto"* pueda ser el impacto del tratamiento, más improbable es que el tratamiento en su conjunto pueda considerarse legítimo.

Como puede apreciarse, lo expresado anteriormente se ajusta a la doctrina del Tribunal Constitucional sobre el juicio de proporcionalidad que debe realizarse sobre una medida restrictiva de un derecho fundamental. Según esta doctrina, deberán constatarse tres requisitos: idoneidad (si la medida permite conseguir el objetivo propuesto); necesidad (que no exista otra medida más moderada); proporcionalidad en sentido estricto (más beneficios o ventajas que perjuicios).

En definitiva, dejando aparte el hecho de que el interesado no conoce para qué fines o con qué base jurídica se han recogido sus datos, se entiende que la recogida y utilización de la fotografía de los clientes que MARINS PLAYA realiza supone un tratamiento de datos personales excesivo.

En relación con esta cuestión, sirven todos los argumentos puestos de manifiesto por la autoridad de protección de datos de Países Bajos, reseñados en el Antecedente Cuarto, para cuestionar el tratamiento de dichos datos personales en virtud de lo establecido en el artículo 6.1.f) del mismo RGPD, considerando que existen otras formas menos intrusivas para verificar si el titular de la tarjeta magnética es el legítimo titular de la misma en el momento del pago y, así, evitar que dichas tarjetas se utilicen de forma fraudulenta.

Por otra parte, tampoco consta en las actuaciones que MARINS PAYA haya establecido garantías adicionales que pudieran favorecer la aceptación de esta base jurídica del tratamiento de datos, como la de favorecer el derecho de oposición del interesado o establecer, incluso, mecanismos de exclusión voluntaria.

En definitiva, el interés legítimo invocado por MARINS PLAYA no prevalece frente los derechos y libertades fundamentales de los interesados en la protección de sus datos personales, por lo que no cabe considerar que el tratamiento de datos personales que lleva a cabo esté amparado por el interés legítimo que prevé el artículo 6.1.f) del RGPD.

Y tampoco el interesado presta su consentimiento para dicho tratamiento de datos. De acuerdo con lo expresado en las normas reseñadas, los tratamientos de datos personales objeto de la reclamación requieren la existencia de una base legal que lo legitime, como el consentimiento del interesado prestado válidamente, necesario

cuando no concurra alguna otra base jurídica de la mencionadas en el artículo 6.1 del RGPD o el tratamiento persiga un fin compatible con aquel para el que se recogieron los datos.

El artículo 4 del RGPD define el *"consentimiento"* en los términos siguientes:

"Artículo 4 Definiciones
A efectos del presente Reglamento se entenderá por:
11. «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

En relación con la prestación del consentimiento, debe tenerse lo establecido en el artículo 6 del RGPD, ya citado, y en los artículos 7 del RGPD y 7 de la LOPDGDD.

Artículo 7 *"Condiciones para el consentimiento"* del RGPD:

"1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

Artículo 6 "*Tratamiento basado en el consentimiento del afectado"* de la LOPDGDD:

"1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.
3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual".

El consentimiento se entiende como un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernan, prestada con garantías suficientes para acreditar que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. Y debe darse para todas las actividades de tratamiento realizadas con el mismo o mismos fines, de modo que, cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos

ellos de manera específica e inequívoca, sin que pueda supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de sus datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación negocial. A este respecto, la licitud del tratamiento exige que el interesado sea informado sobre los fines a que están destinados los datos (consentimiento informado).

El consentimiento ha de prestarse libremente. Se entiende que el consentimiento no es libre cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno; o cuando no se le permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato o prestación de servicio sea dependiente del consentimiento, aún cuando éste no sea necesario para dicho cumplimiento. Esto ocurre cuando el consentimiento se incluye como una parte no negociable de las condiciones generales o cuando se impone la obligación de estar de acuerdo con el uso de datos personales adicionales a los estrictamente necesarios.

Sin estas condiciones, la prestación del consentimiento no ofrecería al interesado un verdadero control sobre sus datos personales y el destino de los mismos, y ello haría ilegal la actividad del tratamiento.

El Grupo de Trabajo del Artículo 29 analizó estas cuestiones en su documento *"Directrices sobre el consentimiento en virtud del Reglamente 2016/679"*, revisadas y aprobadas el 10/04/2018; que ha sido actualizado por el Comité Europeo de Protección de Datos el 04/05/2020 mediante el documento *"Directrices 05/2020 sobre el consentimiento con arreglo al Reglamento 2016/679"*. De lo indicado en este documento, interesa ahora destacar algunos aspectos relacionados con la validez del consentimiento, en concreto sobre los elementos "específico", "informado" e "inequívoco":

"3.2. Manifestación de voluntad específica
El artículo 6, apartado 1, letra a), confirma que el consentimiento del interesado para el tratamiento de sus datos debe darse «para uno o varios fines específicos» y que un interesado puede elegir con respecto a cada uno de dichos fines. El requisito de que el consentimiento deba ser «específico» tiene por objeto garantizar un nivel de control y transparencia para el interesado. Este requisito no ha sido modificado por el RGPD y sigue estando estrechamente vinculado con el requisito de consentimiento «informado». Al mismo tiempo, debe interpretarse en línea con el requisito de «disociación» para obtener el consentimiento «libre». En suma, para cumplir con el carácter de «específico» el responsable del tratamiento debe aplicar:

i) la especificación del fin como garantía contra la desviación del uso,
ii) la disociación en las solicitudes de consentimiento, y
iii) una clara separación entre la información relacionada con la obtención del consentimiento para las actividades de tratamiento de datos y la información relativa a otras cuestiones.

Ad. i): De conformidad con el artículo 5, apartado 1, letra b), del RGPD, la obtención del consentimiento válido va siempre precedida de la determinación de un fin específico, explícito y legítimo para la actividad de tratamiento prevista. La necesidad del consentimiento específico en combinación con la noción de limitación de la finalidad que figura en el artículo 5, apartado 1, letra b), funciona como garantía frente a la ampliación o difuminación gradual de los fines para los que se realiza el tratamiento de los datos una vez que un interesado haya dado su

autorización a la recogida inicial de los datos. Este fenómeno, también conocido como desviación del uso, supone un riesgo para los interesados ya que puede dar lugar a un uso imprevisto de los datos personales por parte del responsable del tratamiento o de terceras partes y a la pérdida de control por parte del interesado.
Si el responsable del tratamiento se basa en el artículo 6, apartado 1, letra a), los interesados deberán siempre dar su consentimiento para un fin específico para el tratamiento de los datos. En consonancia con el concepto de limitación de la finalidad, con el artículo 5, apartado 1, letra b), y con el considerando 32, el consentimiento puede abarcar distintas operaciones, siempre que dichas operaciones tengan un mismo fin. Huelga decir que el consentimiento específico solo puede obtenerse cuando se informa expresamente a los interesados sobre los fines previstos para el uso de los datos que les conciernen.
Sin perjuicio de las disposiciones sobre la compatibilidad de los fines, el consentimiento debe ser específico para cada fin. Los interesados darán su consentimiento entendiendo que tienen control sobre sus datos y que estos solo serán tratados para dichos fines específicos. Si un responsable trata datos basándose en el consentimiento y, además, desea tratar dichos datos para otro fin, deberá obtener el consentimiento para ese otro fin, a menos que exista otra base jurídica que refleje mejor la situación…
Ad. ii) Los mecanismos de consentimiento no solo deben estar separados con el fin de cumplir el requisito de consentimiento «libre», sino que también deben cumplir con el de consentimiento «específico». Esto significa que un responsable del tratamiento que busque el consentimiento para varios fines distintos, debe facilitar la posibilidad de optar por cada fin, de manera que los usuarios puedan dar consentimiento específico para fines específicos.
Ad. iii) Finalmente, los responsables del tratamiento deben facilitar, con cada solicitud de consentimiento separada, información específica sobre los datos que se tratarán para cada fin, con el objeto de que los interesados conozcan la repercusión de las diferentes opciones que tienen. De este modo, se permite a los interesados dar un consentimiento específico. Esta cuestión se solapa con el requisito de que los responsables faciliten información clara, tal y como se ha expuesto anteriormente en la sección 3.3".

"3.3. Manifestación de voluntad informada
El RGPD refuerza el requisito de que el consentimiento debe ser informado. De conformidad con el artículo 5 del RGPD, el requisito de transparencia es uno de los principios fundamentales, estrechamente relacionado con los principios de lealtad y licitud. Facilitar información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y, por ejemplo, ejercer su derecho a retirar su consentimiento. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos.
Si no se cumplen los requisitos relativos al consentimiento informado, el consentimiento no será válido y el responsable podrá estar incumpliendo el artículo 6 de RGPD.

3.3.1. Requisitos mínimos de contenido para que el consentimiento sea «informado»
Para que el consentimiento sea informado es necesario comunicar al interesado ciertos elementos que son cruciales para poder elegir. Por tanto, el GT29 opina que se requiere, al menos, la información siguiente para obtener el consentimiento válido:
i) la identidad del responsable del tratamiento,
ii) el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento,
iii) qué (tipo de) datos van a recogerse y utilizarse,
iv) la existencia del derecho a retirar el consentimiento,
v) información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente, e
vi) información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas, tal y como se describen en el artículo 46".

En el supuesto denunciado no existen evidencias sobre la prestación de un consentimiento válido por parte de los clientes de MARINS PLAYA que ampare los tratamientos de datos personales que MARINS PLAYA lleva a cabo con la fotografía de dichos clientes. Esta entidad ni siquiera informa sobre esta utilización de la fotografía, ni ha establecido ningún mecanismo para que los clientes puedan consentir esta utilización mediante un acto afirmativo separado para estas concretas operaciones de tratamiento, las cuales tampoco constan recogidas en el Registro de Actividades de Tratamiento.

En consecuencia, de conformidad con las evidencias expuestas, los citados hechos suponen una vulneración de lo dispuesto en el artículo 6 del RGPD, que da lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

Como puede apreciarse de lo expuesto anteriormente, las conclusiones obtenidas sobre los hechos analizados van más allá de la concreta actuación de MARINS PLAYA respecto de la recogida y tratamiento de datos personales del reclamante, y tienen que ver con el proceso de gestión de datos personales implantado por esta entidad con carácter general. Por tanto, en contra de lo manifestado por esta entidad en su escrito de alegaciones a la propuesta de resolución, resulta irrelevante si el reclamante se opuso o no a la entrega de su pasaporte en el momento del registro en el hotel.

Resulta igualmente irrelevante que la fotografía de los clientes únicamente se visualizara por el personal de servicios. Lo relevante es el tratamiento que se realiza, que conlleva el registro de la fotografía en los sistemas de información de la reclamada, y las circunstancias en que dicho registro se lleva a cabo.

Por último, cabe señalar que las pruebas completadas en el procedimiento permiten rechazar la afirmación realizada por MARINS PLAYA en su escrito de alegaciones a la propuesta de resolución, sobre la conservación de la fotografía únicamente durante la estancia del cliente en el hotel y su eliminación con posterioridad. La propia ficha del reclamante, que fue requerida por el instructor, prueba que en la actualidad su fotografía sigue conservándose en el sistema de información de la reclamada.

IV

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
(…)
b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
(...)
d) 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;
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;".

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en la letra d) anterior es compatible con la sanción consistente en multa administrativa.

V

Los hechos expuestos incumplen lo establecido en el artículo 6 del RGPD, lo que supone la comisión de una infracción tipificada en el apartado 5.a) del artículo 83 del RGPD, que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR 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:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9".

A este respecto, la LOPDGDD, en su artículo 71 establece 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"*.

A efectos del plazo de prescripción, el artículo 72 de la LOPDGDD indica:

"Artículo 72. 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:
(…)
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679".

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos 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, 9 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".

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.
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 indicados, a efectos de fijar el importe de la sanción a imponer en el presente caso, se considera que procede graduar dicha sanción de acuerdo con los siguientes criterios:

Se estiman concurrentes como agravantes los criterios de graduación siguientes:

. Artículo 83.2.a) del RGPD: *"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".

. En relación con la duración de la infracción, consta en las actuaciones que la recogida de datos personales que realiza la reclamada, que incluye la recogida de la fotografía de los clientes, se ha venido produciendo, al menos, desde el 27/08/2018, fecha de entrada en el hotel del reclamante, y se mantiene en la actualidad.
. Número de interesados: la infracción afecta a todos los clientes de la entidad.
. La naturaleza de los perjuicios causados a las personas interesadas, que han visto incrementado el riesgo en su privacidad.

. Artículo 83.2.b) del RGPD: *"b) la intencionalidad o negligencia en la infracción"*.

Es preciso destacar que el procedimiento de recogida de datos personales implantado por MARINS PLAYA supone, desde el punto de vista de los interesados titulares de los datos recabados, la pérdida de la disposición y control sobre sus datos, por cuanto ni siquiera conocen que esa recogida de datos incluye la fotografía que aparece en el documento identificativo facilitado por el cliente a su llegada al hotel.

Estas circunstancias, además de las significadas en el apartado anterior, ponen de manifiesto la actuación negligente de MARINS PLAYA. A este respecto, se tiene en cuenta lo declarado en Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006) que, partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica 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".*

Se trata de una empresa que realiza tratamientos de datos personales de sus clientes de manera sistemática y continua y que debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos.

Además, se considera que ha tenido conocimiento en varias ocasiones, durante la tramitación de la reclamación, sobre la posible irregularidad de su actuación y no ha tomado ninguna medida dirigida a su subsanación.

. Artículo 83.2.d) del RGPD: *"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".*

La entidad imputada no tiene implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, de modo que la infracción no es consecuencia de una anomalía en el funcionamiento de dichos procedimientos sino un defecto del sistema de gestión de los datos

personales diseñado por la responsable.

. Artículo 83.2.g) del RGPD: *"g) las categorías de los datos de carácter personal afectados por la infracción".*

Si bien no se han visto afectadas *"Categorías especiales de datos personales"*, según define el RGPD en el artículo 9, ello no significa que los datos sustraídos no fueran de naturaleza sensible. El dato personal afectado por el tratamiento (la fotografía de los clientes) tiene una naturaleza especialmente sensible, por cuanto permite la pronta identificación de los interesados y aumenta los riesgos sobre su privacidad, especialmente cuando se registra asociado a todos los datos que constan en el documento de identidad del titular, como ocurre en este caso.

. Artículo 76.2.a) de la LOPDGDD: *"a) El carácter continuado de la infracción"*.

El procedimiento de recogida y tratamiento de datos personales implantado por la reclamada se aplica a todos los clientes durante, al menos, el período señalado al referir la duración de la infracción. Se trata de una pluralidad de acciones que siguen la actuación diseñada por MARINS PLAYA, las cuales infringen el mismo precepto.

. Artículo 76.2.b) de la LOPDGDD: *"b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales".*

La alta vinculación de la actividad del infractor con la realización de tratamientos de datos personales, considerando la actividad que desarrolla en el sector hotelero y su volumen de actividad (en el Antecedente Quinto se recogen algunos detalles al respecto).

. Artículo 83.2.k) del RGPD: *"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".*

La condición de mediana empresa y volumen de negocio de MARINS PLAYA (en el Antecedente Quinto se recogen algunos detalles al respecto).

Se considera, asimismo, que concurren como atenuantes las circunstancias siguientes:

. Artículo 83.2.k) del RGPD: *"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".*

Aunque se considera excesiva la recogida del dato personal relativo a la fotografía del cliente y la utilización posterior que se realiza de la misma, se tiene en cuenta la finalidad pretendida por la entidad reclamada, de evitar fraudes en los consumos de servicios, y que no se ha acreditado otro uso distinto de este dato personal.

Considerando los factores expuestos, la valoración que alcanza la multa, por la

Infracción del artículo 6 del RGPD, es de 30.000 euros (treinta mil euros).

Interesa destacar que MARINS PLAYA no ha formulado alegación alguna respecto de la graduación de la sanción en el escrito presentado en respuesta a la propuesta de resolución elaborada por el instructor del procedimiento.

VI

Las infracciones cometidas pueden conllevar la imposición al responsable de 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…".*

En este caso, procede requerir a la entidad responsable para que, en el plazo que se indica en la parte dispositiva, cese en la recogida y tratamiento de la fotografía de sus clientes. En otro caso, deberá adecuar la información en materia de protección de datos que ofrece a los clientes, especialmente la relativa a la recogida y utilización de la fotografía y la base jurídica que fundamenta el tratamiento, estableciendo mecanismos que permitan acreditar que dicha información es accedida por los interesados; y llevar a cabo la necesaria adecuación de las operaciones de tratamiento a las que se refiere el presente acto a las exigencias contempladas en el artículo 6.1 del RGPD, con el alcance expresado en los Fundamentos de Derecho anteriores.

Asimismo, deberá corregir los efectos de la infracción cometida, lo que conlleva la supresión de todas las fotografías recabadas de los clientes en las circunstancias que han determinado la declaración de la infracción que se sanciona en este acto.

Se advierte que no atender los requerimientos de este organismo puede ser considerado como una infracción administrativa grave al *"no cooperar con la Autoridad de control"* ante los requerimientos efectuados, pudiendo ser valorada tal conducta a la hora de la apertura de un procedimiento administrativo sancionador con multa pecuniaria.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la entidad MARINS PLAYA, S.A., con CIF A07158223, por una infracción del Artículo 6 del RGPD, tipificada en el Artículo 83.5.a) del RGPD y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, una multa de 30.000 euros (treinta mil euros).

SEGUNDO: Requerir a la entidad MARINS PLAYA, S.A. para que, en el plazo de un mes, adopte las medidas necesarias para adecuar su actuación a la normativa de protección de datos personales, con el alcance expresado en el Fundamento de

Derecho VI. En el plazo indicado, la citada entidad deberá justificar ante esta Agencia Española de Protección de Datos la atención del presente requerimiento".

TERCERO: NOTIFICAR la presente resolución a la entidad MARINS PLAYA, S.A.

CUARTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-231221

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