- **Expediente N.º: EXP202409760**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento a través de la recepción de una denuncia de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos. Con fecha 11 de julio de 2024, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) para investigar a SOUTH EUROPE GROUND SERVICES, S.L. con NIF ***B70717210*** (en adelante, SOUTH EUROPE) en relación con los siguientes hechos:

La parte denunciante, que afirma actuar en nombre y representación de un sindicato, expone que, en 2019, se implantó por IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA, con ***NIF A85850394***, (en adelante, IBERIA) un sistema de fichaje mediante huella dactilar. En 2021, la empresa habría implantado un nuevo sistema de fichaje para el registro de jornada a través del reconocimiento facial.

Informa la parte denunciante que el sindicato requirió a la empresa para que adoptara políticas internas que cumplieran con los principios de protección de datos desde el diseño y medidas para dar transparencia a las funciones y el tratamiento de los datos personales, permitiendo a los interesados supervisarlo y a su responsable crear y mejorar elementos de seguridad. La parte denunciante indica que la empresa no facilitó la información requerida y no les respondió.

Manifiesta asimismo la parte denunciante que el sindicato presentó reclamación ante la AEPD y, tras la tramitación de expediente sancionador, la Agencia constató que IBERIA, había infringido el artículo 13 del RGPD. Después de varios correos electrónicos remitidos a la encargada de protección de datos de IBERIA, no habrían recibido respuesta.

Afirma que el 16 de mayo de 2024, fruto de subrogación, los trabajadores del servicio de "*handling"* (asistencia a las aeronaves) han pasado a la nueva empresa, la ahora reclamada, SOUTH EUROPE. El 17 de junio, el sindicato solicitó a esta empresa el nombre del DPD, sin haber obtenido respuesta.

La parte denunciante comunica que esa parte de la plantilla continúa efectuando el fichaje de la jornada laboral a través de sus datos biométricos, a fecha de la denuncia.

Aporta:

- Correo electrónico de la sección sindical a IBERIA, solicitando saber cómo va a proceder con la aplicación de la Guía de la AEPD, con fecha de 13 de diciembre de 2023;

- Correo electrónico de la sección sindical a SOUTH EUROPE queriendo saber el nombre de su DPD, con fecha de 17 de junio de 2024.

SEGUNDO: Con fechas de 27/03/2025 y 13/04/2025, se presentaron sendas reclamaciones contra SOUTH EUROPE**,** provenientes de empleados de dicha sociedad, por la implantación del descrito sistema de fichaje mediante datos biométricos. Ambas aportan fotografías del dispositivo de fichaje.

TERCERO. Las citadas reclamaciones fueron admitidas a trámite con fecha, respectivamente, de 31/03/2025 y 14/04/2025

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

1. En relación a la situación actual del tratamiento de datos biométricos como medio para el registro de jornada, manifiesta:

"[…]se pone en conocimiento de la AEPD que SOUTH EUROPE no emplea ni la huella dactilar ni el reconocimiento facial como medio para el registro de jornada de los trabajadores de la Compañía."

2. Asimismo, manifiesta:

"*que SOUTH EUROPE es una sociedad resultante de la escisión acometida por IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A., OPERADORA (en adelante, "IBERIA"), en el marco de la reestructuración organizativa de su unidad de negocio habiéndose otorgado escritura ante Notario en fecha 16 de mayo de 2024.*

Tras la publicación por parte de la Agencia de la Guía sobre tratamientos de control de presencia mediante sistemas biométricos (en adelante, la "Guía"), IBERIA inició un proceso gradual de sustitución de los sistemas biométricos empleados, impulsando la implantación de un nuevo modelo de control horario basado en el uso de tarjetas magnéticas, habiéndose no obstante concluido por parte de la AEPD en el expediente sancionador PS/00127/2020 promovido frente a IBERIA que el uso de las tecnologías biométricas en el contexto analizado se ajustaba a las exigencias legales.

Y es que esta continuidad en el uso de los sistemas biométricos tras la publicación de la Guía encontraba su justificación, por un lado, en la necesidad de no restringir los derechos laborales reconocidos en la legislación vigente, y por otro, en las importantes

cargas económicas que implicaba la instalación de un sistema alternativo, habida cuenta la resolución del proceso de adjudicación de licencias para los servicios de asistencia en tierra anteriormente indicado.

Pues bien, como consecuencia de este proceso de transición societaria y funcional, y hasta que SOUTH pudo operar de manera plenamente autónoma, subsistieron ciertos tratamientos residuales de datos vinculados a estructuras heredadas de la entidad matriz ya que el proceso de distribución, instalación y puesta en funcionamiento de los dispositivos de lectura de tarjetas en los distintos aeropuertos españoles se ha desarrollado de forma escalonada, condicionado por factores logísticos y técnicos específicos de cada centro de trabajo. En este contexto, la situación descrita tuvo su origen en el hecho de que los terminales de fichaje instalados en determinadas ubicaciones requerían tarjetas provistas de chip de proximidad mientras que las tarjetas facilitadas por AENA en ese momento no incorporaban dicha tecnología, lo que impedía su uso operativo efectivo con los dispositivos instalados.

Afirma que desde junio de 2025 todos los dispositivos y el sistema de fichaje con datos biométricos se encuentran “plenamente desactivados”

Y manifiesta:

“[…]SOUTH no ha desarrollado sistema alguno de control horario basado en el tratamiento de datos biométricos, sino que la gestión operativa y técnica fue asumida en su totalidad por IBERIA, quien ya tenía implementado este sistema para el control de presencia con fines laborales de las personas trabajadoras para la realización del registro de jornada para aquellas cuyo centro de trabajo era el aeropuerto, y ello en virtud de lo establecido Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo(en adelante, el “RDL 8/2019”) en relación con lo dispuesto en el Estatuto de los Trabajadores.
[…]
En este contexto, es importante subrayar que los datos biométricos utilizados procedían exclusivamente de personas trabajadoras que ya prestaban servicios en la entidad matriz y que, como consecuencia de la segregación acaecida el 16 de mayo de 2024, pasaron a formar parte de SOUTH sin que se produjera un nuevo tratamiento de recogida de datos.”

4. De sus manifestaciones se extraen las siguientes que pueden tener relación con la información proporcionada a los trabajadores:

“[…]el sistema implementado ha sido puramente transitorio, y dado que desde SOUTH ha abogado en todo momento por su supresión a los efectos de cumplir con las directrices de esta Agencia, desde el escrupuloso respeto de la normativa vigente en materia de protección de datos y, concretamente, según lo dispuesto por el artículo 13 del RGPD con relación al artículo 5 del texto europeo, la Compañía facilitó la información relativa al tratamiento de datos de carácter biométrico en su política de privacidad garantizando así que toda persona trabajadora fuera debidamente informada respecto de cualquier tratamiento que, aun siendo residual y en vías de supresión, pudiera tener lugar de manera transitoria.[…]”

. En relación a la evaluación de impacto manifiesta:

"[…] la EIPD que sustentaba dicho tratamiento en cuestión, fue la realizada por IBERIA y aportada con el escrito de contestación al requerimiento de información con número de referencia EXP202405962."

9. En relación al levantamiento de la prohibición del art. 9 RGPD y a la base de legitimación, manifiestan:

"[…] en tanto en cuanto el sistema de biometría no se utiliza en la actualidad por parte de SOUTH y su uso fue estrictamente excepcional como consecuencia del período vivido, habiéndose validado su adecuación a Derecho por medio del PS/00127/2020, puesto que este se basaba en mecanismos de verificación biométrica tipo 1:1, es decir, una comparación uno a uno entre el dato facilitado por el trabajador y su correspondiente plantilla previamente registrada, por lo que, al no permitir una identificación indiscriminada dentro de una base de datos, el tratamiento no se consideraba constitutivo de una operación sobre datos de categorías especiales.

3. En relación a la forma de fichaje que se utilizaba, manifiesta:

"En relación con la cuestión planteada, se informa a esta Agencia que, tanto en el contexto de IBERIA como, en su fase inicial, en SOUTH, el sistema de control horario implementado mediante tecnologías biométricas permitía la identificación del trabajador exclusivamente a través de una de las dos modalidades habilitadas en los terminales instalados, esto es, huella dactilar o reconocimiento facial, sin que fuera necesario –ni posible– presentar simultáneamente una tarjeta de identificación asociada al trabajador para realizar el fichaje.

Esto se debía a que los terminales biométricos utilizados no disponían de capacidad técnica para la lectura de tarjetas, por lo que el uso de tarjetas físicas no formaba parte del procedimiento de registro de jornada en dicho sistema.
No obstante, cabe destacar que esta situación cambió con la progresiva implantación del nuevo sistema de fichaje basado en tarjetas con chip de proximidad, que comenzó a desplegarse una vez iniciada la transición hacia medios alternativos al tratamiento de datos biométricos, y cuyos terminales sí incorporan la capacidad técnica necesaria para la lectura y registro mediante dicho soporte físico."

4. En relación al número de trabajadores afectados por el tratamiento biométrico justo antes y justo después de la segregación, manifiesta:

> *"Por otro lado, desde el inicio de la actividad operativa de SOUTH, en junio de 2024, la compañía optó por implantar el nuevo sistema de fichaje basado exclusivamente en el uso de tarjetas físicas con chip de proximidad. Este proceso de implantación se llevó a cabo de manera escalonada, conforme a la disponibilidad de los terminales y las particularidades técnicas de cada centro de trabajo, pero con el objetivo claro de sustituir completamente el sistema biométrico heredado de la etapa anterior. En consecuencia, durante la primera etapa de actividad de SOUTH, pudieron subsistir ciertos fichajes mediante sistemas biométricos en aeropuertos concretos, pero siempre con carácter transitorio y limitado.*

No obstante lo anterior, a día de hoy puede afirmarse con absoluta certeza que la totalidad del personal de SOUTH registra su jornada laboral exclusivamente mediante el uso de tarjetas personalizadas, vinculadas individualmente al perfil de cada trabajador. No existe ningún sistema alternativo de fichaje actualmente activo, ni tampoco se contempla el uso de tecnologías biométricas para esta finalidad en ninguno de los centros gestionados por la Compañía. Por tanto, tal y como se informó a esta Agencia a través del Escrito de fecha 4 de julio de 2025, ocho mil quinientos treinta y dos (8.532) trabajadores, a través del número de tarjeta debidamente asignado, se encuentran dados de alta en el sistema de fichaje."

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

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

II
Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de

la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo

89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

III

Evaluación de impacto relativa a la protección de datos

La evaluación de impacto relativa a la protección de datos se regula en el artículo 35 del RGPD en los siguientes términos:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de

datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

IV
Conclusión

De los resultados de las actuaciones previas de investigación que constan en el expediente puede concluirse lo siguiente:

SOUTH EUROPE es una sociedad resultante de la escisión acometida por IBERIA en el marco de la reestructuración organizativa de su unidad de negocio habiéndose otorgado escritura ante Notario en fecha 16 de mayo de 2024.

Tras la publicación por parte de la Agencia de la Guía sobre tratamientos de control de presencia mediante sistemas biométricos (en adelante, la “Guía”), IBERIA inició un proceso gradual de sustitución de los sistemas biométricos empleados, impulsando la implantación de un nuevo modelo de control horario basado en el uso de tarjetas magnéticas.

SOUTH EUROPE justifica la continuidad en el uso de los sistemas biométricos tras la publicación de la Guía en la necesidad de de no restringir los derechos laborales reconocidos en la legislación vigente, , a la vez que planificó un calendario de abandono paulatino del sistema en todas sus instalaciones en España.

Como consecuencia de este proceso de transición societaria, y hasta que SOUTH EUROPE pudo operar de manera plenamente autónoma, subsistieron ciertos tratamientos residuales de datos vinculados a estructuras heredadas de la entidad matriz ya que el proceso de distribución, instalación y puesta en funcionamiento de los dispositivos de lectura de tarjetas en los distintos aeropuertos españoles se ha desarrollado de forma escalonada, condicionado por factores logísticos y técnicos específicos de cada centro de trabajo. En este contexto, la situación descrita tuvo su origen en el hecho de que los terminales de fichaje instalados en determinadas ubicaciones requerían tarjetas provistas de chip de proximidad mientras que las tarjetas facilitadas por AENA en ese momento no incorporaban dicha tecnología, lo que impedía su uso operativo efectivo con los dispositivos instalados.

SOUTH EUROPE afirma haber facilitado la información relativa al tratamiento de datos de carácter biométrico en su política de privacidad.

En relación a la evaluación de impacto, manifiesta que, dada la transitoriedad del tratamiento y el abandono progresivo del mismo, la EIPD que sustentaba dicho tratamiento en cuestión, fue la ya realizada por IBERIA.

SOUTH EUROPE ha facilitado una detallada información sobre la fecha en que cada una de sus instalaciones ha desactivado los sistemas y dispositivos de fichajes mediante huella dactilar o reconocimiento facial. Afirma que desde junio de 2025 todos los dispositivos y el sistema de fichaje con datos biométricos se encuentran “plenamente desactivados”.

Se ha de significar, por su importancia, que SOUTH EUROPE adoptó medidas para el cumplimiento de la normativa aplicable de manera diligente, tomando la decisión de

suprimir el sistema de fichaje en cuestión, y por iniciativa propia, muchos meses antes de que recibiera de esta AEPD requerimiento de información alguno.

Como ya se ha indicado el mero inicio de actuaciones de investigación por parte de esta Agencia no implica la imputación de una infracción en materia de protección de datos o la imposición de medidas correctivas por parte de la AEPD, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

A mayor abundamiento, señalar que la Sentencia del Tribunal de Justicia de 24 de septiembre de 2024, en el asunto C 768/21, se pronunció en relación con un caso de brecha de datos personales en el que una autoridad de control (el Comisionado para la Protección de Datos y la Libertad de Información del Estado Federado de Hesse, Alemania) no impuso una multa en atención a las circunstancias del caso concreto. En la sentencia se afirma lo siguiente en relación con este punto (el subrayado es de esta Agencia):

> *"41 En consecuencia, no puede deducirse ni del artículo 58, apartado 2, del RGPD ni del artículo 83 de este la existencia de una obligación a cargo de la autoridad de control de adoptar, en todos los casos, cuando constate una violación de la seguridad de datos personales, una medida correctora, en particular una multa administrativa, siendo su obligación, en tales circunstancias, reaccionar adecuadamente para subsanar la deficiencia constatada. En estas circunstancias, como señaló el Abogado General en el punto 81 de sus conclusiones, el autor de una reclamación cuyos derechos han sido vulnerados no dispone de un derecho subjetivo a que la autoridad de control imponga una multa administrativa al responsable del tratamiento.*
>
> *43 A este respecto, no se excluye que, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, la autoridad de control pueda abstenerse de adoptar una medida correctora aunque se haya constatado una violación de la seguridad de datos personales. Tal puede ser el caso, en particular, cuando la violación constatada no haya persistido, por ejemplo cuando el responsable del tratamiento, que, en principio, había aplicado medidas técnicas y organizativas apropiadas en el sentido del artículo 24 del RGPD, haya adoptado, tan pronto como haya tenido conocimiento de dicha violación, las medidas adecuadas y necesarias para que la violación finalice y no vuelva a producirse, habida cuenta de las obligaciones que le incumben, en particular, en virtud de los artículos 5, apartado 2, y 24 del mencionado Reglamento."*

El TJUE incide, por tanto, en el margen de apreciación que tienen las autoridades de control para, en el ejercicio de sus funciones, desarrollar y optar entre los poderes atribuidos por el artículo 58 del RGPD, teniendo en cuenta las circunstancias del caso concreto, así como velando por el pleno respeto del RGPD. La consigna que debe regir siempre la actuación de una autoridad de control es asegurar un nivel alto de protección de los datos personales.

Así, cabe que, aun cuando se hubiera constatado o se tuvieran indicios de que se ha producido una vulneración en materia de protección de datos, las autoridades de

control se abstengan de ejercitar sus poderes correctivos cuando esta presunta infracción hubiera sido subsanada y se garantice la conformidad de los tratamientos de datos personales con el RGPD.

Lo señalado por el TJUE en la sentencia antes citada, refuerza la idea de proporcionalidad de actuación de las autoridades de control que se recoge, con anterioridad a que fuera dictada la mencionada sentencia, en los artículos 65.4 y 65.6 de la LOPDGDD, por los que se permite a la AEPD, en atención a las circunstancias del caso concreto, la inadmisión a trámite o el archivo de reclamaciones, cuando, tras el traslado de las mismas al responsable del tratamiento, este demostrara haber adoptado medidas para el cumplimiento de la normativa aplicable.

En el presente caso, en atención a las circunstancias acontecidas, se considera que, con carácter excepcional y en atención a las circunstancias del caso concreto, no procede la imposición de una medida correctiva.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, por la Presidencia de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **SOUTH EUROPE GROUND SERVICES, S.L.** con NIF ***B70717210***, y a las partes reclamantes.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia 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.

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos