Procedimiento Nº: PS/00127/2020

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: La reclamación interpuesta Dña. ***A.A.A.*** (en lo sucesivo la reclamante), tiene entrada con fecha 29/04/2019 en la Agencia Española de Protección de Datos. La reclamación se dirige contra IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA UNIPERSONAL, con NIF ***A85850394*** (en adelante, el reclamado). Los motivos en que basa la reclamación son: que el 24/01/2019 la C.G.T (Confederación General del Trabajo) solicitó a la empresa que siguiera una serie de pautas: creación y notificación del preceptivo fichero y obligación de informar debidamente a los trabajadores ante la recogida de las huellas dactilares de los agentes de servicios auxiliares pera un nuevo sistema de fichaje que se implantaría en un futuro próximo. El 27/02/2019 Iberia contesta que se trata de un tratamiento lícito y adecuado, además de medidas para un tratamiento seguro. No obstante, a día de la fecha no se ha facilitado ningún documento a los trabajadores que registran su huella dactilar.

SEGUNDO: La Subdirección General de Inspección de Datos procedió al traslado de la reclamación al reclamado para que informase de sobre los hechos y las medidas tomadas, teniendo conocimiento de los siguientes extremos:

El 18/06/2019, fue trasladada al reclamado la reclamación presentada para el análisis de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.

- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

- Cualquier otra que considere relevante, etc.

El 19/07/20196 el reclamado daba respuesta al requerimiento de información contestando a las cuestiones planteadas y aportaba la siguiente documentación:

- Carta de la CGT de 24/01/2019.

- Respuesta de IBERIA de 29/01/2019.

- Carta de CGT de 18/03/2019.

- Análisis de Impacto en la privacidad sobre el tratamiento en cuestión.

- Comunicación a todos los empleados el 25/05/2018.

- Política de privacidad para empleados de IBERIA.

- Capturas de pantalla de la Intranet y de la app para empleados de la empresa.

Posteriormente, el 12/09/2019 se solicitó al reclamado que aportase el estudio de Evaluación de Impacto; dando respuesta el siguiente día señalando que el citado informe solo podía facilitarse en formato MS Excel, no habiendo sido aceptado como válido en la sede electrónica, razón por la que procedió a presentarlo a través del registro físico de la Agencia.

TERCERO: El 09/10/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada.

CUARTO: Con fecha 30/09/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 13 del RGPD, sancionada conforme a lo dispuesto en el artículo 58.2.b) del RGPD.

QUINTO: Notificado el acuerdo de inicio, el reclamado en fecha 15/10/2010 presento escrito de alegaciones manifestando en síntesis lo siguiente: que se reiteraba en las alegaciones formuladas en escrito de 19/07/2019 y manifestaba que se había elaborado y comunicado al personal nota informativa sobre tratamiento biométrico mediante sistemas de reconocimiento de huella dactilar o de reconocimiento facial para control de accesos.

SEXTO: Con fecha 21/10/2020 se inició un período de práctica de pruebas, acordándose las siguientes

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/05886/2019.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que a ellas acompaña.

SEPTIMO: El 26/02/2020 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la AEPD se sancionara al reclamado por infracción del artículo 13 del RGPD, tipificada en el artículo 83.5.a) del RGPD, con apercibimiento de conformidad con el artículo 58.2.b) del RGPD.

Transcurrido el plazo legalmente señalado al tiempo de la presente Resolución el reclamado no había presentado escrito de alegación alguno.

OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: La reclamante presento escrito de entrada con fecha 29/04/2019 en la Agencia Española de Protección de Datos, manifestando que el 24/01/2019 C.G.T (Confederación General del Trabajo) solicitó a la empresa información sobre la implantación del sistema de acceso y que siguiera una serie de pautas sobre el mismo: creación y modificación del preceptivo fichero y obligación de informar debidamente a los trabajadores ante la recogida de las huellas dactilares de los agentes de servicios auxiliares pera un nuevo sistema de fichaje que se implantará en

un futuro próximo; el 27/02/2019 el reclamado señalaba que era un tratamiento lícito, adecuado y seguro; sin que se haya facilitado documento alguno a los trabajadores que registran su huella dactilar.

SEGUNDO: Consta aportada carta de CGT de 24/01/2019 manifestando su disconformidad con las pautas seguidas por el reclamado ante la recogida de huellas dactilares para la implantación de un nuestro sistema de fichaje en la empresa, sin que en ningún momento se hubiera informado debidamente a los trabajadores ni de la creación y notificación del preceptivo fichero.

TERCERO: Consta la respuesta del reclamado señalando que la sustitución de las tarjetas magnéticas por el uso de la huella digital limitada exclusivamente a la zona de rampa del aeropuerto y los trabajadores que allí trabajen implica un tratamiento licito amparado en el interés público del reclamado, adecuado y seguro de los datos personales sensibles involucrados; que el reclamado ya tiene informado este tipo de tratamiento dentro de su política de privacidad disponible desde mayo de 2018 a través de internet.

CUARTO: El 18/03/2019 CGT señalaba que la información dispuesta por la empresa para informar a sus trabajadores era bastante escasa por lo que entendía que era insuficiente a pesar de que se diga que responde al tratamiento adecuado y a las necesidades del mismo.

QUINTO: El 13/09/2019 el reclamado aportó Evaluación de Impacto del tratamiento llevado a cabo sobre el tratamiento de la huella dactilar para control de accesos.

SEXTO: El 15/10/2020 el reclamado ha aportado comunicación informativa complementaria a los empleados *Nota Informativa sobre los tratamientos de datos biométricos mediante sistemas de reconocimiento de huella dactilar o de reconocimiento facial para el control de accesos*.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD y en los art. 47 y 48.1 de LOPDGDD.

II

La legitimación para el tratamiento de la huella dactilar para el control de los trabajadores por parte del empleador debemos buscarlo en el artículo 9 y 6 del RGPD.

El artículo 9 del RGPD establece en sus apartados 1 y 2.b) 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 las orientaciones sexuales de una persona física.*

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

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 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."

El artículo 6.1.b) del RGPD indica:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

(…)
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."

El reclamado tiene legitimación, fundamentada en la normativa señalada, para efectuar el control laboral de sus trabajadores y siempre que cumpla los requisitos indicados en el Fundamento de Derecho quinto.

III

Los hechos que motivan la reclamación presentada y que son objeto del presente procedimiento se materializan en la solicitud efectuada por el reclamante al reclamado en relación con la implantación de un nuevo sistema de acceso y la obligación de informar debidamente a los trabajadores.

Los hechos reclamados suponen la vulneración de lo señalado en el artículo 13 del RGPD, al no informar debidamente del tratamiento previsto en relación con el control de fichaje por huella dactilar, de conformidad con lo pronunciamientos establecidos en el citado artículo.

Este artículo determina la información que debe facilitarse al interesado en el momento de la recogida de sus datos, estableciendo lo siguiente:

"Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información".

IV

En el presente caso, el reclamante manifiesta dirigirse por escrito al reclamado solicitando que se informara debidamente a los trabajadores ante la recogida de huellas dactilares de cara a la implantación de un nuevo sistema de control horario, sin que se obtuviera respuesta alguna.

No obstante, de la documentación aportada al expediente consta la respuesta ofrecida al reclamante, tal como consta en el antecedente segundo, manifestando que

la sustitución del sistema establecido por el uso de la huella digital limitada exclusivamente a la zona de rampa del aeropuerto y de los trabajadores que allí trabajaban implicaba un tratamiento licito, adecuado y seguro de los datos personales sensibles involucrados y que había informado a través de su política de privacidad a través de la intranet.

En relación con las cuestiones planteadas en el presente caso, en primer lugar hay que señalar que la implantación de un sistema de control horario basado en la huella dactilar por parte del empleador, ha de ser informado a los empleados de manera completa, clara, concisa y, además, la citada información debe ser completada con referencia tanto a las bases legales que den cobertura a dicho tipo de control de acceso, como a la información básica a la que hace referencia en el artículo 13 del RGPD.

En el caso examinado, aunque conta la respuesta del reclamado al escrito presentado por el reclamante señalando que el sistema a implantar era seguro y pertinente, tanto la información transmitida por el reclamado como el sistema empleado para comunicar el sistema de acceso y control horario no es el más adecuado dada la calidad y especialidad de los datos que se solicitaban, pudiendo haber llevado a cabo un mayor esfuerzo en su política de información sobre el tratamiento previsto, formulándolo de una manera mucho más detallada y completa, así como dar respuesta a cierta casuística como los casos de trabajadores que se negaran a proporcionar su huella.

No obstante, hay que señalar que la entidad en las alegaciones al acuerdo de inicio del procedimiento aportó una comunicación complementaria destinada a los empleados *Nota Informativa sobre los tratamientos de datos biométricos mediante sistemas de reconocimiento de huella dactilar o de reconocimiento facial para el control de accesos,* de conformidad con la normativa en materia de protección de datos y, asimismo, consta acreditado la preceptiva evaluación de impacto relativa a la protección de datos regulada en el artículo 35 del RGPD, aportando el documento correspondiente.

En segundo lugar, habría que señalar que la instalación de un sistema de control basado en la recogida y tratamiento de la huella dactilar de los empleados implica el tratamiento de sus datos personales puesto que dato personal es toda aquella información sobre una persona física identificada o identificable de conformidad con el artículo 4.1 del RGPD.

En cuanto a la huella dactilar se trata, además, de datos que deben ser calificados como datos biométricos y de acuerdo con el artículo 4.14 del RGPD tienen esta consideración cuando han sido *“obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”.*

Esto hace que, de conformidad con el artículo 9.1 del RGPD, en el caso presente, se les aplique el régimen específico previsto para las categorías especiales de datos previsto en el artículo 9 del RGPD.

En este sentido, el considerando 51 del RGPD pone de manifiesto el carácter restrictivo con el que se puede admitir el tratamiento de estos datos:

"(51) ... Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las liberta-des fundamentales.

Y el considerando 52 señala que

"(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o con-trol de enfermedades transmisibles y otras amenazas graves para la salud… "

De acuerdo con estas consideraciones el tratamiento de datos biométricos de categorías especiales requerirá, además de la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD, alguna de las excepciones previstas en el artículo 9.2 del RGPD.

El análisis de la base legal de legitimación para realizar este tratamiento viene del artículo 6 del RGPD, relativo a la licitud del tratamiento, que en su apartado 1, letra b) señala: "*El tratamiento será lícito si se cumple al menos una de las siguientes condiciones: (…) 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 éste de medidas precontractuales (…)".*

En virtud de este precepto, el tratamiento sería lícito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Por otra parte, y tal como pone de relieve el considerando 51 del mismo RGPD, en la medida en que los datos biométricos son de categoría especial en los supuestos de identificación biométrica (art. 9.1 RGPD), será necesario que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD que permitirían levantar la

prohibición general del tratamiento de estos tipos de datos establecida en el artículo 9.1.

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será de aplicación cuando "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 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".

En el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores:

"3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

Es innegable la posibilidad de utilización de sistemas basados en datos biométricos para llevar a cabo el control de acceso y horario, aunque tampoco parece que sea o deba ser el único sistema que puede ser usado: así el uso de tarjetas personales, la utilización de códigos personales, la visualización directa del punto de marcaje, etc., que pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas igualmente eficaces para llevar a cabo el control.

En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo y teniendo en cuenta sus implicaciones, tratamiento de datos biométricos dirigidos a identificar de manera univoca a una persona física, sería preceptivo llevar a cabo una evaluación de impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos de conformidad con lo señalado en el artículo 35 RGPD.

En el caso presente, hay que hacer constar que la entidad ha acreditado la preceptiva evaluación de impacto relativa a la protección de datos regulada en el artículo 35 del RGPD, aportando el documento correspondiente, puesto que el 13/09/2019 presentó el documento Evaluación de Impacto del tratamiento llevado a cabo.

V

Por otra parte, los datos biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

Según el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, *"Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior."*

En relación con ellos, el Dictamen precisa que cabe distinguir diversos tipos de tratamientos al señalar que *"Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica."*

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), que ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores.

Sin embargo, debe tenerse en cuenta lo siguiente:

O El trabajador debe ser informado sobre estos tratamientos.

O Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos (Dictamen 3/2012 del Grupo de Trabajo del art. 29).

O Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

O El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.

O Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

O Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

O Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

O Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

VI

El artículo 83.5 b) del RGPD, considera que la infracción de *"los derechos de los interesados a tenor de los artículos 12 a 22",* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento, *"con multas administrativas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía".*

La LOPDGDD en su artículo 71, *Infracciones*, señala que:

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

La LOPDGDD en su artículo 72 indica a efectos de prescripción: *"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:

(…)

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

(…)"

VII

El procedimiento sancionador que nos ocupa evidencia que en la instalación de un nuevo sistema de control de asistencia mediante huella dactilar a implantar había sido llevado a cabo sin informar debidamente con todas las garantías que se señalan en la normativa de protección de datos, en concreto de conformidad con lo señalado en el artículo 13 del RGPD, pudiendo haber incurrido en la vulneración del mismo.

Por tanto, la conducta del reclamado constituiría la vulneración de lo dispuesto en el artículo 13 del RGPD.

Por otra parte, el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla la posibilidad de acudir a la sanción de apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones.

Asimismo, se contempla que la resolución que se dicte establecerá las medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido, la adecuación de la información ofrecida a los usuarios a las exigencias contempladas en el artículo 13 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Ahora bien, hay que señalar que en las alegaciones al acuerdo de inicio del presente procedimiento el reclamado ha aportado copia de la comunicación realizada a todos los trabajadores y que venía a complementar la información aportada con anterioridad *Nota Informativa sobre los tratamientos de datos biométricos mediante sistemas de reconocimiento de huella dactilar o de reconocimiento facial para el control de accesos*, de conformidad con los señalado en el artículo 13 del RGPD, por lo que no procede instar la adopción de medidas adicionales al haber quedado acreditado que el reclamado ha adoptado medidas razonables y evitar que vuelvan a producirse incidencias como la que dio lugar a la reclamación.

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 IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA, con NIF ***A85850394***, por una infracción del artículo 13 del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA, con NIF ***A85850394***.

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.

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