

- **Procedimiento N°: PS/00176/2021**

### RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

#### ANTECEDENTES

PRIMERO: **A.A.A.** (en adelante, el reclamante) con fecha 9 de noviembre de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos (en adelante AEPD). La reclamación se dirige contra **CLUB DEPORTIVO AKEKI DE TENERIFE** con NIF **G76613041** (en adelante, el reclamado). Los motivos en que basa la reclamación son la publicación, en la página web del reclamado y de acceso público, del número de DNI, nombre, apellidos, salario neto y retenciones practicadas del reclamante. Junto a la reclamación, aporta capturas de pantalla donde se aprecia la publicación de los datos mencionados.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

En fecha 04/01/2021 se recibió respuesta del reclamado. A tenor de la información preliminar de la que se dispone, se aprecian indicios racionales de una posible vulneración de la normativa en materia de protección de datos, sin perjuicio de lo que se determine en el curso de la instrucción del presente procedimiento.

TERCERO: El 15/04/2020, de conformidad con lo dispuesto en el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: En fecha 28 de junio de 2021, la Directora de la Agencia Española de Protección de Datos acuerda iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 5.1 f) del RGPD, conforme a lo dispuesto en el artículo 83.5 del RGPD, considerada muy grave efectos de prescripción en el artículo 72 apartado 1. i) de la LOPDGDD, y por la presunta infracción 32 del RGPD, conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción en el artículo 73 apartado f) de la LOPDGDD

QUINTO: Notificado el citado acuerdo de inicio y no habiendo presentado alegaciones, a tenor de lo dispuesto en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el acuerdo de inicio puede ser considerado propuesta de resolución. En consecuencia, esta Agencia procede a dictar Resolución.

## HECHOS

PRIMERO: En fecha 9 de noviembre de 2020, el reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, contra el CLUB DEPORTIVO AKEKI DE TENERIFE con NIF G76613041 por la a publicación, en la página web del reclamado y de acceso público, del número de DNI, nombre, apellidos, salario neto y retenciones practicadas del reclamante

SEGUNDO: En fecha 4 de enero de 2021 se recibe respuesta al traslado de la reclamación, de la documentación aportada, el reclamado manifiesta que publicó en la página web el informe de auditoría externa para cumplir con la Ley de Transparencia del Gobierno de Canarias, en donde eran visibles, el DNI, el nombre y la cuantía de las nóminas del reclamante. Y que tras recibir la solicitud del reclamante accedió al tachado del DNI.

## 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 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

### II

El artículo 5.1.f) del RGPD, Principios relativos al tratamiento, señala lo siguiente:

*“1. Los datos personales serán:*

*(...)*

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

El artículo 5 de la LOPDGDD, Deber de confidencialidad, señala lo siguiente:

*“1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.*

*2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.*

*3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento”.*

La documentación obrante en el expediente evidencia que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, en relación con el artículo 5 de la LOPGDD, *deber de confidencialidad*, al publicar en su web, el DNI, el nombre y la cuantía mensual de la nómina.

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

Por tanto, ese deber de confidencialidad es una obligación que incumbe no sólo al responsable y encargado del tratamiento, sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional

### III

En cuanto a la seguridad de los datos personales, el artículo 32 del RGPD “*Seguridad del tratamiento*”, establece que:

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

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

*2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*

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

*4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y*

*tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”.*

Los hechos puestos de manifiesto suponen el quebrantamiento de las medidas técnicas y organizativas al posibilitar la exhibición de documentación del reclamante donde constan sus datos de carácter personal con la consiguiente falta de diligencia por el responsable.

#### IV

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

De la documentación obrante en el expediente se confirma que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad debido a la publicación en su página web de datos personales del reclamante, permitiendo el acceso no autorizado a estos por terceros ajenos.

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

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

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

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

*“(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la*

*confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales”.*

En el presente caso, tal y como consta en los hechos y en el marco del expediente E/09861/2020, la AEPD trasladó al reclamado, la reclamación presentada para su análisis, solicitando la aportación de información relacionada con la incidencia. De la documentación aportada, el reclamado manifiesta que publicó en la página web el informe de auditoría externa para cumplir con la Ley de Transparencia del Gobierno de Canarias, en donde eran visibles, el DNI, el nombre y la cuantía de las nóminas del reclamante. Y que tras recibir la solicitud del reclamante accedió al tachado del DNI.

No obstante, las bases reguladoras de la subvención contenidas en la Orden de 10 de diciembre de 2019, publicada en el BOC el 19/12/2019, en su artículo 16 establece las obligaciones de la persona beneficiaria.

En concreto en el dos. 4. *“Cumplir, en todo momento, lo dispuesto por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE nº 294, de 6.12.18)”.*

Asimismo, el punto tres del referido artículo dispone, *“en cumplimiento del artículo 3.1, letra b) en relación con el artículo 13 de la Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública, se deberá realizar una publicidad activa de las subvenciones obtenidas, derivadas de esta convocatoria, y en concreto en el apartado a) se hace referencia al caso de que se elija la página web de la persona beneficiaria, estableciendo que deberá añadirse en el menú, en la página principal, un icono bajo la denominación de subvenciones, en el que se insertará en formato pdf, la resolución definitiva (de concesión de la subvención)”.*

Por lo tanto y en atención a la normativa referida, debe publicarse únicamente la resolución de concesión de la subvención, careciendo de base legitimadora, para la publicación de los datos personales que figuran en el informe de auditoría externa.

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

De conformidad con lo que antecede, el reclamado es responsable de la infracción del artículo 32 del RGPD, infracción tipificada en el artículo 83.4.a) del RGPD.

De las actuaciones practicadas se constata que las medidas de seguridad, tanto de índole técnica como organizativas, con las que contaba la entidad investigada en

relación con los datos que sometía a tratamiento, no eran las adecuadas al momento de producirse la brecha de seguridad.

La consecuencia de esta falta de medidas de seguridad adecuadas fue la exposición a terceros ajenos de los datos personales de los trabajadores de la investigada. Es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento que, en función de este, debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron. La vulneración del principio de confidencialidad (art 5.1.f) RGPD), la ausencia de medidas de seguridad (art 32 RGPD) adecuadas en función del riesgo, constituyen el elemento de la culpabilidad que requiere la imposición de sanción.

## V

En el presente caso consta la vulneración del artículo 5.1.f) del RGPD, por lo que es de aplicación lo dispuesto en el art. 83.5 del RGPD.

El artículo 83.5 del RGPD 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;”*

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica “Infracciones” determina lo siguiente: *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.*

Establece el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, lo siguiente: *“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:*

*(...)*

- i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.”*

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



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

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

*(...)*

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica *“Infracciones consideradas graves”*, lo siguiente:

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

*(...)*

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

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD y 72.1 i) y 73 apartado f) de la LOPDGDD, arriba transcritos.

## VI

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los *“Principios de la Potestad sancionadora”*, en el artículo 28 la bajo la rúbrica *“Responsabilidad”*, lo siguiente:

*“1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa.”*

## VII

El artículo 58.2 del RGPD, señala lo siguiente:

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

*(...) “*

- a) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento.”

Establece el artículo 76 de la LOPDGDD bajo la rúbrica “Sanciones y medidas correctivas”, lo siguiente: “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.  
(...)

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.”

## VIII

El artículo 70.1 de la LOPDGDD señala los sujetos responsables.

“1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

- a) Los responsables de los tratamientos.”

En el presente caso, atendiendo a la diligencia llevada a cabo por la entidad investigada en lo referente a proceder al tachado de los DNI de sus empleados, así como a la respuesta al requerimiento formulado por la AEPD, justificando su actuación en el cumplimiento de Ley de Transparencia del Gobierno de Canarias, permite considerar una disminución de la culpa en los hechos, por lo que se considera conforme a Derecho, no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento, de conformidad con el artículo 76.3 de la LOPDGDD en relación con el artículo 58.2 b) del RGPD.

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 CLUB DEPORTIVO AKEKI DE TENERIFE, con NIF G76613041, por infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD y del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a CLUB DEPORTIVO AKEKI DE TENERIFE.

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.

938-131120

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