Procedimiento Nº: PS/00416/2020

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, el reclamante) con fecha 13/01/2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el AYUNTAMIENTO DE ALBUIXECH con NIF ***P4601400G*** (en adelante, el reclamado). Los motivos en que basa la reclamación son en síntesis:
que a través de la página web del reclamado se puede acceder a datos personales de vecinos como DNI, teléfono, discapacidad, situación económica; aportando varios de los enlaces de la página web que muestran documentos con datos personales.

SEGUNDO: De conformidad con lo previsto en el artículo 65.4 de la LOPDGDD, se dio traslado de su reclamación al reclamado para que procediera a su análisis y diera respuesta en el plazo de un mes sobre la incidencia reclamada. En fecha 03/06/2020, el reclamado, dio respuesta al requerimiento anterior.

TERCERO: El 09/06/2020, tras analizarse la documentación que obraba en el expediente, se dictó resolución por la directora de la AEPD, acordando la no admisión a trámite de la reclamación. La resolución fue notificada al recurrente en fecha 09/06/2020.

CUARTO: En fecha 09/06/2020, el reclamante interpuso recurso potestativo de reposición contra la resolución recaída en el expediente E/02285/2020, mostrando su disconformidad con la resolución impugnada, invocando similares argumentos que los contenidos en su reclamación inicial y exponiendo que el Ayuntamiento no había tomado las medidas correspondientes pues a fecha 09/06/2020, se seguía accediendo a los documentos ya mencionados en la reclamación y junto al recurso se ha aportado nueva documentación relevante a los efectos de lo planteado.

QUINTO: El 06/11/2020, tras las comprobaciones realizadas mediante el acceso a alguno de los enlaces que derivan a páginas con información conteniendo datos personales, se constata que varios de los documentos publicados que contienen información con datos personales no han sido eliminados o anonimizados, resolviéndose el recurso de reposición interpuesto contra la resolución de esta Agencia dictada en fecha 09/06/2020, y acordar la admisión de la reclamación presentada.

SEXTO: El 25/01/2021 la Directora de la AEPD acordó iniciar procedimiento sancionador al reclamado por las presuntas infracciones de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del citado Reglamento.

SEPTIMO: Notificado el acuerdo de inicio, el 12/02/2021 el reclamado solicito copia del expediente y ampliación del plazo que le fue remitida y concedido, respectivamente, por el instructor del procedimiento.

En fecha 18/02/2021 el reclamado presento escrito de alegaciones manifestando. en síntesis: que si bien en un principio se instaló un plugin para bloquear el acceso a los contenidos de la página web del reclamado, el departamento de informatica que trato de solucionar la incidencia en primera instancia fue consciente de que la medida se antojó insuficiente pues aunque no se podía acceder al contenido continuaba siendo posible acceder conociendo la URL de los archivos publicados; que por este motivo se llevó a cabo una migración de la web a otro servidor por lo que todo el contenido al que se podría haber tenido acceso está completamente eliminado y no siendo posible tener acceso desde el momento en que se realizó la migración.

OCTAVO: Con fecha 24/02/2021 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/09211/2020.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado

NOVENO: El 05/04/2021 fue emitida Propuesta de Resolución en el sentido de que se sancionara al reclamado por infracción de los artículos 5.1.f) y 32,1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, con apercibimiento de conformidad con el artículo 77 de la LOPDGDD.

Transcurrido el plazo legalmente señalado el reclamado no había presentado escrito de alegaciones.

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

HECHOS PROBADOS

PRIMERO: 13/01/2020 tiene entrada en la Agencia Española de Protección de Datos escrito del reclamante, manifestando que a través de la página web del reclamado se puede acceder a datos personales de vecinos como DNI, teléfono, discapacidad, situación económica; aportando varios de los enlaces de la página web que muestran documentos con datos personales.

SEGUNDO: El 09/06/2020 se dictó resolución acordando la no admisión a trámite de la reclamación.

TERCERO: El 09/06/2020 el reclamante interpuso recurso potestativo de reposición mostrando su disconformidad con la resolución recaída, exponiendo que el reclamado no había tomado las medidas ya que se podía seguir accediendo a los datos personales contenidos en la información publicada en la web, aportando nueva documentación relevante a efectos de lo planteado, dictándose resolución estimatoria el 06/11/2020.

CUARTO: El reclamado ha señalado que: *"Antes de la recepción del inicio del procedimiento sancionador, concretamente en fecha 01/12/2020, se llevó a cabo una migración de la web www.albuixech.es a otro servidor, por lo que todo el contenido … ya está completamente eliminado y no es posible tener acceso desde el momento en que se realizó la migración"*

También señala que *"En la nueva página web se han adoptado las siguientes medidas de seguridad para evitar que dicha incidencia se vuelva a producir:*
(…).

QUINTO: El reclamado ha aportado impresión de pantalla de la página web donde ya no es posible acceder a contenido alguno y donde figuraba la información conteniendo los datos de carácter personal que dio lugar a la reclamación y que en la actualidad se encuentran eliminados.

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

Los hechos denunciados se concretan que a través de la página web *http//www.albuixech.es/wp-content/uploads/* titularidad del reclamado se podía acceder a datos personales de vecinos como DNI, teléfono, discapacidad, situación económica y que a pesar de que había manifestado dar solución a la incidencia, no se habían tomado las medidas correspondientes ya que se podía seguir accediendo a los datos de los vecinos.

En primer lugar, dicho tratamiento podría ser constitutivo de una infracción del artículo 5, *Principios relativos al tratamiento*, del RGPD que establece que:

> *"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, *Deber de confidencialidad*, de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), señala que:

"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".

III

En segundo lugar, 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".

IV

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, *"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".*

Por otro lado, la LOPDGDD, a efectos de prescripción, en su artículo 72 indica: *"Infracciones consideradas muy graves:*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

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

V

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

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

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

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

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

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

(…)

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".
(…)"

VI

Los hechos probados evidencian el acceso a través de la página web *http//www.albuixech.es/wp-content/uploads* de titularidad del reclamado a los datos de carácter personal de vecinos de la localidad (DNI, teléfono, discapacidad, situación económica, etc.), a pesar de que haber manifestado a esta AEPD que había dado solución a la incidencia, quebrantando y vulnerando las medidas de carácter técnico y organizativas y el deber de confidencialidad de los datos.

Como consta en los antecedentes y acreditado en los hechos probados del procedimiento ha quedado acreditado que dictada resolución de archivo de la reclamación inicial, el reclamante interpuso recurso potestativo de reposición contra la resolución recaída mostrando su disconformidad y exponiendo que el reclamado no había tomado las medidas adecuadas ya que a pesar de lo alegado se continuaba accediendo a los datos de la web municipal, aportando junto al escrito de recurso nueva documentación relevante.

Tras el análisis y comprobaciones realizadas se constató que había documentos publicados conteniendo información con datos de carácter personal que no habían sido eliminados o anonimizados, estimándose el recurso y acordando la admisión de la reclamación presentada.

Por tanto, la actuación de la entidad constituye vulneración de los principios de confidencialidad y de seguridad de los datos, regulados en los artículos 5.1.f) y 32.1 del RGPD, y tipificada en los artículos 83.5.a) y 83.4.a) del RGPD.

No obstante, con la finalidad de aclarar los términos de la incidencia producida y que propició la apertura del presente procedimiento sancionador, el reclamado mediante escrito de 18/02/2021 señalaba que si bien en un principio se instaló un plugin *WP Content Copy Protectión Pro* para bloquear el acceso a los documentos existentes en la página web del Ayuntamiento y llevar a cabo la eliminación de los archivos que contenían datos de carácter personal publicados en la citada página, tras la recepción del acuerdo de apertura de procedimiento el servicio de informatica trato en un primer momento de solucionar la incidencia llegando a la conclusión de que la medida adoptada (instalar un plugin de bloqueo de acceso a la web), se antojaba insuficiente ya que aunque impedía el acceso a los contenidos continuaba siendo posible acceder a los mismos si se conocía la dirección URL de los archivos publicados.

Por ello, se llevó a cabo la migración de la web de la entidad a otro servidor lo que determino que el contenido al que se podría haber tenido acceso con anterioridad a la citada fecha estaba eliminado no siendo posible el acceder al mismo desde el instante en que se realizó la migración.

Con la finalidad de evitar incidencias como la ocurrida, en la nueva página web se adoptaron una serie de medidas técnicas: eliminar el acceso a la carpeta *wp-*

content y de su contenido a través de *.htaccess*; chequear antes de servir los permisos WP mediante la función *is-luger-logged-in*, para recuperar un fichero por una subcarpeta de *wp-content,* etc.

Además, el reclamado ha señalado que asume su responsabilidad como consecuencia de las infracciones cometidas si bien considera que deben tenerse en cuenta los esfuerzos realizados para mejorar las medidas de seguridad con la finalidad de garantizar la seguridad y la confidencialidad de los datos de carácter personal de los que es el responsable y que la infracción no es debido a una inacción o falta de proactividad en el cumplimiento de la normativa sobre protección de datos.

Por otra parte, hay que señalar que el reclamado aporta impresión de pantalla de la página web donde deberían estar el contenido de los datos de carácter personal que provoco la reclamación y que en la actualidad se encuentran eliminados, no siendo posible tener acceso a los mismos.

VII

La LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento,* establece lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

En el supuesto que nos ocupa, de conformidad con las evidencias de las que se dispone y sin perjuicio de lo que resulte de la instrucción, dicha conducta podría constituir, por parte del reclamado la posible infracción a lo dispuesto en el artículo 5.1.f) y 32.1 del RGPD.

Hay que señalar que el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de acudir a la sanción de apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones, cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica.

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 y su adecuación a las exigencias contempladas en los

artículos 5.1.f) y 32.1 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Sin embargo, se considera que la respuesta formulada por el reclamado en escrito de fecha 18/02/2021 ha sido razonable, subsanando la incidencia producida no procediendo instar la adopción de medidas adicionales a las ya tomadas por el reclamado, que es una de las finalidades principales de los procedimientos respecto de aquellas entidades relacionadas en el artículo 77 de la LOPDGDD, habiendo quedado acreditado la suspensión de la web de la entidad donde figuraba la información conteniendo los datos de carácter personal de los vecinos al haber migrado la misma a otro servidor y adoptando una serie de medidas para evitar que se produzcan hechos como los que dieron 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 al AYUNTAMIENTO DE ALBUIXECH, con NIF ***P4601400G***, por una infracción del aartículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD, una sanción de apercibimiento, de conformidad con el artículo 77 de la LOPDGDD.

SEGUNDO: IMPONER al AYUNTAMIENTO DE ALBUIXECH, con NIF ***P4601400G***, por una infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de apercibimiento, de conformidad con el artículo 77 de la LOPDGDD.

TERCERO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE ALBUIXECH, con NIF ***P4601400G***.

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