

- -Expediente N.º: EXP202100354

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, la parte reclamante) con fecha 14/06/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AYUNTAMIENTO DE SALINAS DE PISUERGA con NIF *P3415800F* (en adelante, el reclamado). Los motivos en que basa la reclamación son los siguientes: el reclamante manifiesta que el reclamado ha dado a un tercero acceso al expediente administrativo en el que se regula una obra de construcción impulsada por el reclamante; dicha persona, miembro del Consejo ciudadano del municipio, señaló en reunión del mismo que el reclamante debía ceñirse en la ejecución de su proyecto a lo dispuesto en la memoria presentada y aprobada; el reclamante señala que cómo puede conocer esa persona los detalles del expediente, manifestando que en el Registro no consta ninguna solicitud formal de acceso al mismo, por lo que entiende que ha accedido a la información de manera irregular; también señala que se ha publicado el acta de la reunión del Consejo ciudadano en la página de *facebook* y en ella figuran su nombre y apellidos sin su consentimiento.

Y aporta:

- Acta de reunión del Consejo Ciudadano celebrada el ***FECHA.1.
- Fotografía de la página de Facebook en la que se aprecia la publicación de la mencionada acta de reunión del Consejo Ciudadano.

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 a la parte reclamada, 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.

El reclamado en escrito remitido a esta Agencia con fecha 22/07/2021 ha señalado lo siguiente:

“En relación con “la memoria presentada y aprobada” cabe informar que la persona, miembro del Consejo Ciudadano que hizo esa observación, nunca ha tenido acceso a ese expediente desde este ayuntamiento.

Desconocemos como lo sabe, pero es fácil imaginar que tratándose de un pueblo y de una obra de tan escasa entidad e importancia y siendo la persona vecina del reclamante, en cualquier momento o lugar ha podido oírlo.

En relación al acta del Consejo Ciudadano, en la que aparece el nombre del reclamante, cabe indicar que la publicación del acta es un ejercicio de transparencia de lo público y que en ningún caso se puede entender que hay afectación al honor o a la integración moral del reclamante y mucho menos atentado a su dignidad, ni menoscabo de derechos fundamentales.

En el futuro, este ayuntamiento, que seguirá en su ejercicio de transparencia, omitirá cualquier nombre que pueda herir sensibilidades."

TERCERO: Con fecha 23/07/2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

Con fechas 30, 31/08/2021 y 30/09/2021, el reclamado ha aportado la siguiente información:

Respecto al procedimiento de registro y consulta de la información y documentación que obra en los expedientes administrativos de solicitudes de obra presentadas por los ciudadanos, existen dos procedimientos, uno externo y otro interno.

A nivel externo al ayuntamiento, para poder consultar un expediente administrativo, el interesado, previamente debe realizar una solicitud a través de la oficina de registro presencial o a través de la oficina de registro en la sede electrónica del Ayuntamiento. Una vez autorizada la solicitud de consulta, se le facilita en las dependencias municipales de manera presencial la consulta al expediente. En ningún momento se facilita copia del expediente.

A nivel interno, la consulta se realiza a través de la herramienta gestor de expedientes Gestiona, los usuarios dados de alta para realizar la consulta son la secretaria del ayuntamiento, auxiliar administrativa y el alcalde. Además, los expedientes también están archivados en carpetas los cuales pueden ser consultados de manera presencial por los miembros de la corporación y personal del ayuntamiento. Tanto personal como la corporación tienen firmado el compromiso de confidencialidad.

El acceso a la herramienta se realiza a través de certificado electrónico o nombre y contraseña y dispone de un registro de accesos.

No se realizan registros de los accesos a los expedientes en papel por parte de la corporación ni de los empleados públicos

- Se aporta copia de los registros de accesos realizados al expediente automatizado correspondientes a las fechas desde el 06/02/2019 hasta el 25/08/2021, de lo que se desprende que todos los accesos al expediente han sido realizados por dos usuarios que según manifestaciones del representante del Ayuntamiento son personal con acceso autorizado y el acceso forma parte de sus funciones en el desempeño de su puesto de trabajo.
- Aporta copia del registro de actividad del tratamiento denominado “REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN”.
- Respecto a las medidas de seguridad manifiestan que el gestor de expedientes utilizado es la herramienta de administración electrónica Gestiona, certificada de conformidad con el Esquema Nacional de Seguridad con categoría ALTA, con el certificado AENOR de prestador de Servicios de confianza cualificados, certificación ISO 27001 de Seguridad de la Información y con el cumplimiento del RGPD.

Así mismo manifiesta que todos los trabajadores tienen firmado un compromiso de confidencialidad.

- Aporta copia del análisis de riesgos que contempla el tratamiento “Gestión administrativa de expedientes de disciplina urbanística”.

El informe de análisis de riesgo recoge las amenazas identificadas a las que los datos personales están expuestos, así como las vulnerabilidades que pueden aprovechar dichas amenazas para tener éxito. Se ha estimado también el daño que podrían producir las distintas amenazas en caso de que se materializasen, así como la probabilidad de su ocurrencia. Con estos datos se ha realizado una estimación del nivel de riesgo y se han tomado las decisiones pertinentes para gestionar estos riesgos implantando medidas de seguridad que eliminen o reduzcan aquellos riesgos que se ha decidido gestionar.

Respecto a las medidas de seguridad recogidas en el análisis de riesgo relativas a los soportes y documentos establece que:

- o Los dispositivos de almacenamiento de los soportes y documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros medios que realicen la misma función.
- o Solo los usuarios autorizados deberán disponer de las llaves y medios que facilitan la apertura de dichos dispositivos.
- o Cuando las características físicas no permitan adoptar esta medida, se deberán adoptar las medidas necesarias para impedir el acceso de personas no autorizadas.

- o En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

Respecto a las medidas de seguridad recogidas en el análisis de riesgo relativas a control de accesos establece, entre otras, que:

- o El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.
- o Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Dichos mecanismos, en el caso de soportes informáticos, podrán consistir en la asignación de contraseñas para el acceso a los mismos, u otros dispositivos más sofisticados: biométricos, llaves USB, etc.; y en el caso de documentos en papel, en la entrega de llaves que facilitan la apertura de los dispositivos de almacenamiento donde se recopila la información.

QUINTO: Con fecha 18/02/2022, la Directora de la Agencia Española de Protección de Datos 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 RGPD.

SEXTO: Notificado el acuerdo de inicio el 09/03/2022, el reclamado presento escrito de alegaciones manifestando que como ya indicó en su día, nunca se dio a nadie acceso a ningún expediente que no lo hubiera solicitado por el conducto reglamentario; que el miembro del consejo ciudadano citado nunca había solicitado el expediente mencionado y nunca había tenido acceso al mismo; que fue publicado en Facebook un acta del consejo ciudadano en aras de la transparencia de las actuaciones públicas y en ella figura información con nombres y apellidos que, en ningún caso afecta a la dignidad ni revela ningún secreto, pues lo publicado es público y notorio, ni puede considerarse lesivo a los intereses o al honor de nadie; que cuando el responsable de la Diputación de Palencia para la protección de datos solicitó que se retirara el dato al que nos referimos y fue retirado de manera inmediata; que entiende que no cabe iniciar proceso sancionador.

SEPTIMO: Con fecha 16/03/2022, se acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por la reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que acompaña.

OCTAVO: El 12/07/2022 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la AEPD se sancionara al reclamado por infracción 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 una sanción de apercibimiento.

Transcurrido el plazo establecido para presentar alegaciones el reclamado, no había presentado escrito alguno.

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

HECHOS PROBADOS

PRIMERO. El 14/06/2021 tiene entrada en la Agencia Española de Protección de Datos escrito del reclamante manifestando que el reclamado ha dado a un tercero acceso al expediente administrativo en el que se regula una obra de construcción impulsada por el reclamante; dicha persona, miembro del Consejo ciudadano del municipio, señaló en una reunión del mismo que el reclamante debía ceñirse en la ejecución de su proyecto a lo dispuesto en la memoria presentada y aprobada; el reclamante se pregunta cómo puede conocer dicha persona los detalles del expediente, si en el Registro no consta ninguna solicitud formal de acceso al mismo, por lo que entiende que ha accedido a la información de manera irregular; asimismo, manifiesta que se ha publicado el acta de la reunión del Consejo ciudadano en la página de facebook y en ella figura su nombre y apellidos sin su consentimiento.

SEGUNDO. Consta aportada Acta de reunión del Consejo Ciudadano celebrada el ***FECHA.1 en cuyo apartado, Ruegos y Preguntas figura lo señalado por el reclamante en su escrito.

TERCERO. El reclamado en escrito de 21/06/2021 ha manifestado que *“la persona, miembro del Consejo Ciudadano que hizo esa observación, nunca ha tenido acceso a ese expediente desde este ayuntamiento.*

Desconocemos como lo sabe, pero es fácil imaginar que tratándose de un pueblo y de una obra de tan escasa entidad e importancia y siendo la persona vecina del reclamante, en cualquier momento o lugar ha podido oírlo.

En relación al acta del Consejo Ciudadano, en la que aparece el nombre del reclamante, cabe indicar que la publicación del acta es un ejercicio de transparencia de lo público y que en ningún caso se puede entender que hay afectación al honor o a la integración moral del reclamante y mucho menos atentado a su dignidad, ni menoscabo de derechos fundamentales.

En el futuro, este ayuntamiento, que seguirá en su ejercicio de transparencia, omitirá cualquier nombre que pueda herir sensibilidades”.

CUARTO. Consta aportada impresión de pantalla de la página de Facebook en la que se figura la publicación del acta de reunión del Consejo Ciudadano.

QUINTO. El reclamado en escrito de 08/03/2022 ha manifestado que *“Ciertamente se publicó en Facebook un acta del consejo ciudadano en aras a la transparencia de las actuaciones públicas. En dicha acta aparecía una información con nombres y apellidos que, en ningún caso afecta a la dignidad ni revela ningún secreto, pues lo publicado es público y notorio, ni puede considerarse lesivo a los intereses o al honor de nadie.*

A mayor abundamiento, cuando el responsable de la Diputación de Palencia para la protección de datos solicitó a este ayuntamiento que se retirara el dato al que nos referimos, fue retirado de manera inmediata”.

SEXTO. Consta aportada copia del Análisis de Riesgos; figura el tratamiento *“Gestión administrativa de expedientes de disciplina urbanística”.*

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora 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

En el presente caso, los hechos puestos de manifiesto por el reclamante se materializan en que el reclamado habría posibilitado a un tercero el acceso al expediente administrativo en el que se regula una obra impulsada por el reclamante, así como la difusión de sus datos personales en la página de *Facebook* del reclamado.

El artículo 58 del RGPD, *Poderes*, señala:

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

(...)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(...).”

El RGPD establece en el artículo 5 los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de “*integridad y confidencialidad*”.

El artículo señala 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»).

(...)

III

La documentación obrante en el expediente ofrece indicios de 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 proceder a la publicación de sus datos en la página de Facebook del reclamado.

Como así figura en los hechos probados consta aportada impresión de pantalla de la página de Facebook en la que se encuentra publicada el acta de la reunión del Consejo Ciudadano, donde se contienen los datos de carácter personal del reclamante.

El deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos, así como evitar que se realicen filtraciones de los datos o cesiones de los mismos a terceros sin la existencia de una base legal que lo legitime.

No obstante, el reclamado en escrito de 22/07/2021 ha señalado que: *“En relación al acta del Consejo Ciudadano, en la que aparece el nombre del reclamante, cabe indicar que la publicación del acta es un ejercicio de transparencia de lo público y que en ningún caso se puede entender que hay afectación al honor o a la integración moral del reclamante y mucho menos atentado a su dignidad, ni menoscabo de derechos fundamentales.*

En el futuro, este ayuntamiento, que seguirá en su ejercicio de transparencia, omitirá cualquier nombre que pueda herir sensibilidades.”

Y posteriormente en escrito de 08/03/2022 señalaba sobre la misma cuestión que *“Ciertamente se publicó en Facebook un acta del consejo ciudadano en aras a la transparencia de las actuaciones públicas. En dicha acta aparecía una información con nombres y apellidos que, en ningún caso afecta a la dignidad ni revela ningún secreto, pues lo publicado es público y notorio, ni puede considerarse lesivo a los intereses o al honor de nadie.*

A mayor abundamiento, cuando el responsable de la Diputación de Palencia para la protección de datos solicitó a este ayuntamiento que se retirara el dato al que nos referimos, fue retirado de manera inmediata”.

No obstante, se estima que el reclamado sería responsable de la infracción del artículo 5.1.f) del RGPD, infracción tipificada en su artículo 83.5.a) del citado reglamento.

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.

Por otro lado, la LOPDGDD en su artículo 71, *Infracciones*, establece que:

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

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:

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

V

En segundo lugar, hay que señalar que la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD.

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”.

VI

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 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”.
(...)”

VII

El RGPD define las violaciones de seguridad de los datos personales como “todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alte-

ración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.

La documentación obrante en el expediente ofrece indicios de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad al posibilitarse el acceso al expediente administrativo en el que se regula una obra de construcción impulsada por el reclamante; el tercero, miembro del Consejo ciudadano del municipio, señaló en reunión del citado Consejo y que posteriormente fue subido a Facebook, que el reclamante debía ceñirse en la ejecución de su proyecto a lo dispuesto en la memoria presentada y aprobada por la entidad local, sin que exista en el Registro de la institución solicitud de acceso, lo que puede suponer infracción de las medidas técnicas y organizativas.

Hay que señalar que el RGPD 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”.

Figura en los hechos y en el marco del expediente de investigaciones previas, que la AEPD trasladó al reclamado la reclamación presentada para que procediese a su análisis e informase del incidente y de las acciones llevadas a cabo, señalando en escrito de 22/07/2021 que el tercero, miembro del Consejo Ciudadano, al que se refiere el reclamante nunca ha tenido acceso al expediente administrativo.

En escrito de alegaciones al acuerdo de inicio del procedimiento sancionador de 09/03/2022, el reclamado reitera e insiste en sus manifestaciones señalando que *“Este Ayuntamiento como ya indicó en su día, nunca ha dado acceso a ningún expediente a nadie que no lo haya solicitado por el conducto reglamentario. En el caso que nos ocupa, el miembro del consejo ciudadano citado nunca ha solicitado el expediente mencionado y nunca ha tenido acceso al mismo”.*

Es cierto que el reclamado ha informado sobre el procedimiento implantado de registro y consulta a la información y documentación que obra en los expedientes administrativos, aportando copia de los accesos realizados al expediente desde el 06/02/2019 hasta el 25/08/2021, deduciéndose que los mismos fueron realizados por personal del reclamado con acceso autorizado; además hay que señalar que todos los trabajadores tienen firmado un compromiso de confidencialidad y consta la copia del informe de análisis de riesgos donde figura el tratamiento *“Gestión administrativa de expedientes de disciplina urbanística”.*

Sin embargo, también es cierto que en la respuesta ofrecida a la AEPD también señalaba que: *“No se realizan registros de los accesos a los expedientes en papel por parte de la corporación ni de los empleados públicos”*, por lo que se podría haber provocado un acceso no consentido.

En este sentido, la responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto, 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 e impedir el acceso a los mismos.

Por tanto, de conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del artículo 32.1 del RGPD, infracción tipificada en su artículo 83.4.a).

VIII

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, el presente procedimiento sancionador viene motivado en base a la presunción de que el reclamado habría incurrido en vulneración de la normativa sobre protección de datos, artículos 5.1.f) y 32.1 del RGPD.

Hay que señalar que la LOPDGDD contempla en su artículo 77 la sanción de apercibimiento en relación con los tratamientos de datos personales que no se adecúen a sus previsiones. A este respecto, el artículo 83.7 del RGPD contempla que “*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*”.

En este mismo sentido, el artículo 58 del RGPD, en su apartado 2 d) señala que cada autoridad de control podrá “*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...*”.

Como se señalaba con anterioridad ha quedado acreditado que el reclamado ha incumplido la normativa de protección de datos, artículos 5.1.f) y 32.1 del RGPD, al publicar en *facebook* los datos de carácter personal del reclamante y posibilitar el acceso al expediente administrativo, vulnerando las medidas técnicas y organizativas.

Se hace necesario señalar que de no corregir dichas deficiencias adoptando las medidas adecuadas a lo señalado en los artículos 5.1.f) y 32.1 del RGPD o bien reiterar la conducta puesta de manifiesto en la reclamación y que es causa del presente procedimiento, así como no informar a esta AEPD de las medidas adoptadas podría dar lugar al ejercicio de posibles actuaciones ante el responsable del tratamiento a fin de que se apliquen de manera efectiva las medidas apropiadas para garantizar y no comprometer la confidencialidad de los datos de carácter personal y el derecho a la intimidad de las personas.

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 SALINAS DE PISUERGA, con NIF *P3415800F*, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: IMPONER al AYUNTAMIENTO DE SALINAS DE PISUERGA, con NIF *P3415800F*, por una infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de apercibimiento

TERCERO: REQUERIR al AYUNTAMIENTO DE SALINAS DE PISUERGA, para que en el plazo de un mes desde la notificación de esta resolución, acredite la adopción de medidas técnicas y organizativas necesarias y pertinentes de conformidad con la normativa en materia de protección de datos de carácter personal a fin de evitar que en el futuro vuelvan a producirse incidencias como las que han dado lugar a la reclamación corrigiendo los efectos de su posible infracción, adecuando el tratamiento de los datos de carácter personal a las exigencias contempladas en los artículos 5.1.f) y 32.1 del RGPD.

CUARTO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE SALINAS DE PISUERGA.

QUINTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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