

- Expediente N.º: EXP202209488

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, la parte reclamante), en fecha 20/07/2022, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el AYUNTAMIENTO DE CATOIRA, con NIF **P3601000G** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La reclamante manifiesta que, en fecha 12/07/2022, se presentaron en el Concello de Catoira, mediante Registro Único, más de 400 firmas de particulares en apoyo a una protesta vecinal.

La contestación al escrito fue publicada en el perfil público de Facebook del Concello, en fecha 14/07/2022, constando nombre, apellidos y dirección postal de la reclamante.

Junto a la reclamación aporta el escrito publicado.

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), el 14/09/2022 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 traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, fue recibido en fecha 15 de septiembre de 2022, como consta en el certificado que obra en el expediente.

Transcurrido el plazo establecido el reclamado no presentó escrito respondiendo al requerimiento de la AEPD.

TERCERO: En fecha 20/10/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: En fecha 18/11/2022, se recibe en esta Agencia escrito de respuesta del reclamado al requerimiento de información de 14/09/2022, indicando que tan pronto se tuvo conocimiento de la situación, se procedió a la eliminación de la publicación de documento. Asimismo, aporta escrito remitido a la Valedora do Pobo a través del cual ponía en conocimiento de dicha Institución autonómica los hechos.

QUINTO: Con fecha 08/03/2023, 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 reclamado mediante escrito de 21/03/2023 alegaba, en síntesis: que no era cierto que no se hubiera respondido al requerimiento de la Agencia, si bien la contestación fue extemporánea; que tampoco se había hecho mención al traslado del escrito realizado a la Valedora de Pobo informando de los hechos; que es importante a la hora de determinar la comisión las presuntas infracciones al reclamado, la actuación de la reclamante; que la reclamante no actuaba en nombre propio sino como representante de un grupo numeroso de vecinos y que su negativa a recibir la notificación de la respuesta al escrito presentado impidiendo que las personas que representaba pudieran conocer el contenido de mismo fue uno de los motivos que llevo al reclamado a publicarlo; que como ya se comunicaba a la Valedora de Pobo los datos publicados era de todos conocidos.

SEPTIMO: Con fecha 08/06/2023, el instructor del procedimiento acordó practicar las siguientes pruebas:

Da por reproducidos a efectos probatorios la reclamación interpuesta por la reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y que forman parte del procedimiento AT/03866/2022.

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

Solicitar al reclamado para que aportara la información y/o documentación siguiente:

-Escrito presentado por la reclamante, en representación de la plataforma *“Coaxe libre de Pirotecnia”*, que tuvo entrada en ese Ayuntamiento en fecha 13/07/2022, en el que se solicitaba se les informara sobre el expediente *“resolución estado de tramitación en relación proyecto presentado por la empresa PIROGAL PIROTECNIA SOCIEDAD LIMITADA, almacén pirotécnico que se va a ubicar en el lugar de Coaxe-Dimo Catoira (parcela del polígono núm.21)”*.

-Acuse de recibo relativo a la notificación de la Alcaldía de fecha 14 de julio remitido a la reclamante.

En fecha 22/06/2023 el reclamado dio respuesta a la prueba practicada cuyo contenido obra en el expediente.

OCTAVO: En fecha 11/08/2023 la Directora de la Agencia Española de Protección de Datos dictó resolución acordando nombrar nuevo instructor del procedimiento.

NOVENO: Con fecha fue dictada Propuesta de Resolución en el sentido de que por la Directora de la AEPD se sancionara la reclamado con apercibimiento 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.

Transcurrido el plazo legalmente establecido el reclamado no presento escrito de alegación alguna.

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

HECHOS PROBADOS

PRIMERO. El 20/07/2022 tiene entrada en la AEPD escrito de la reclamante en la que manifiesta que el 12/07/2022 se presenta en el Concello de Catoira a través del Registro Único escrito con más de 400 firmas de particulares en apoyo a una protesta vecinal y el 14/07/2022 la respuesta al escrito presentado es la publicación de en el perfil público del Concello en Facebook donde figuran sus datos personales y privados.

SEGUNDO. Consta aportada impresión de pantalla del perfil público del Concello de Catoira en Facebook donde figura la respuesta al escrito presentado el 12/07/2022 y en el que figuran los datos de carácter personal de la reclamante; también puede observarse el sello del Concello y la fecha de registro de salida.

TERCERO. Consta escrito del reclamado de fecha 21/11/2022, a requerimiento de la AEPD, en el que da traslado del escrito remitido por la Alcaldía al Valedora do Pobo, de fecha 19/09/2022, en relación con el escrito de queja de la reclamante y la publicación del escrito de la Alcaldía en Facebook.

CUARTO. Consta aportado por el reclamado escrito de respuesta dirigido a la reclamante de fecha 14/07/2022, que de conformidad con lo manifestado por el reclamado en escrito de alegaciones *"...la reclamante, de forma totalmente injustificada, se negó a firmar haber recibido el citado escrito"*.

En el citado escrito consta diligencia manuscrita de empleado municipal de fecha 14/07/2022 señalando que la reclamante se negó a su recepción.

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

Los hechos denunciados se materializan en la publicación en la red social Facebook de un escrito del Concello de Catoira, firmado por su Alcalde-Presidente, en el que constan nombre, apellidos y dirección postal de la parte reclamante, con los efectos multiplicadores que el uso de dichos instrumentos puede tener para su visibilidad.

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;

(...)

d) 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;

(...)"

III

Establece el artículo 5.1.f) del RGPD 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»).

(...)"

En relación con este principio, el *Considerando* 39 del referido RGPD señala que:

(39) *"... Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.*

El artículo 4 del RGPD, *Definiciones*, establece en sus apartados 1, 2, 5, 7 y 12:

1) *«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de*

localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione 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;

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 .

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”.

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

1. La documentación obrante en el expediente evidencia que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al permitir el acceso a los datos carácter personal como consecuencia de la publicación del escrito de la parte reclamada en las redes sociales, lo que constituye un tratamiento de datos que, utilizando la infraestructura de dichas redes, da a conocer unos hechos y unos datos que permiten identificar a la parte reclamante a través de la información expuesta, siendo además dicha infraestructura un medio en el que se pueden multiplicar sus efectos al compartir otros usuarios la noticia, vulnerándose los principios de integridad y confidencialidad, ambos establecidos en el citado artículo 5.1.f) del RGPD..

El reclamado en escrito dirigido a este organismo ha reconocido los hechos señalando los motivos que provocaron la publicación en el perfil de la entidad local en Facebook: la reclamante se negó a recibir la notificación de la respuesta a su escrito y que las personas que formaban parte del colectivo que representaba la misma conocieran su contenido, si bien el escrito fue retirado en cuanto se tuvo conocimiento de la situación de la red social.

Hay que señalar que el post o texto publicado por el reclamado constituye un tratamiento de datos, que utilizando la infraestructura de Facebook da a conocer unos hechos y datos que permiten identificar a la reclamante a través del escrito publicado donde figuran su nombre, apellidos y dirección junto con las diversas circunstancias que en el mismo se exponen.

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

Y 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.

2. El reclamado es una entidad que presta una serie de servicios públicos, para los cuales trata datos de carácter personal de sus empleados y ciudadanos.

El reclamado como cualquier otra entidad pública, está obligada al cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos -RGPD-, y de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales -LOPDGDD- con respecto a los tratamientos de datos de carácter personal que realice, entendiendo por dato de carácter personal, *“toda información sobre una persona física identificada o identificable”*.

Realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad y que en virtud del artículo 4.7 del RGPD, es responsable del tratamiento; es el organismo que determina los fines y medios del tratamiento.

Lo que antecede, con independencia de que los datos publicados de la reclamante, como señala el reclamado tanto en su escrito de alegaciones al acuerdo de

inicio, como en el escrito remitido a la Valedora do Pobo “*son conocidos no solo en Coaxe, en cuyo tablón de edictos se publicaron, sino en todo este pequeño municipio de Catoira, donde nos conocemos todos...*”

Si es cierto, como manifiesta el reclamado en este mismo escrito que “*solo buscó, como único objetivo de la publicación del escrito dirigido a la reclamante, que actuaba en nombre de un numeroso colectivo, proteger el derecho de sus miembros a conocer su contenido*”, podría haber procedido eliminando los datos de carácter personal y anonimizando los mismos para que su derecho a la protección de los datos de carácter personal no se viera afectado.

Por tanto, la actuación del reclamado evidencia la vulneración del principio de confidencialidad, de conformidad con lo establecido en el artículo 5.1.f), infracción tipificada en el artículo 83.5.a) del citado Reglamento.

VI

En segundo lugar, se atribuye al reclamado la infracción del 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 ins-*

trucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”.

VII

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:

*(...)
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.”
(...)”*

VIII

1. 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 ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad, derivado de la ausencia de medidas de seguridad adecuadas que propiciaron la publicación en el perfil del Concello en Facebook de la notificación de respuesta al escrito presentado por la reclamante donde son accesibles datos de carácter personal.

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”.

2. En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación la AEPD trasladó al reclamado el 15/09/2022 la reclamación presentada para que procediese a su análisis e informase a esta Agencia de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos; aunque el reclamado manifestaba en escrito de alegaciones al acuerdo de inicio no entender por qué se señalaba que no se había respondido al requerimiento informativo de la AEPD, lo cierto es que tal respuesta se produjo el 18/11/2022 fuera del plazo establecido, cuando ya se había admitido a trámite la reclamación presentada por la reclamante.

Como consta en el Antecedente tercero, la reclamación fue admitida el 20/10/2022, transcurrido el plazo de respuesta y de conformidad con el artículo 65 de la LOPDGDD.

El reclamado tanto en escrito de fecha 21/11/2022 al que adjunta el escrito remitido a la institución *Valedora do Pobo*, informando de los hechos, como en la respuesta a la prueba practicada ha confirmado la publicación y los motivos que provocaron la misma.

No se pone en duda que la publicación del escrito en la red social y por tanto el acceso a la citada información por terceros tenga por objeto dar a conocer la respuesta de la entidad a todos los integrantes de la asociación, pero no se puede olvidar que la revelación en la red social constituye un tratamiento automatizado de datos que permite conocer unos hechos y unos datos que identifican a la reclamante.

Por otra parte, habría que señalar que la búsqueda en internet, del nombre, apellidos y dirección de la afectada puede ofrecer resultados que, combinándolos con los accedidos por terceros, nos permitan el acceso a otras aplicaciones o la creación de perfiles de personalidad, que no tiene por qué haber sido consentida por su titular.

Todos estos hechos ponen de manifiesto que la entidad reclamada no ha respetado de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de los datos, especialmente las dirigidas a impedir el acceso por terceros no interesados, con los efectos multiplicadores que las redes sociales pueden tener para su visibilidad, siendo además el responsable del tratamiento al decidir los fines y los medios de la recogida y del tratamiento de los datos personales utilizados.

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad adecuadas, 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, se estima que el reclamado responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

IX

El artículo 83 “*Condiciones generales para la imposición de multas administrativas*” del RGPD en su apartado 7 establece:

“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.”

Asimismo, el artículo 77 “*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*” de la LOPDGDD dispone lo siguiente:

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

(...)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

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.”

En el caso examinado, el procedimiento sancionador trae causa de que el reclamado, tal y como se expone en los hechos, ha vulnerado la normativa en materia de protección de datos de carácter personal tanto del principio de confidencialidad de los datos como las medidas técnicas y organizativas implantadas.

Dicha conducta constituye por parte del reclamado la infracción a lo dispuesto en los artículos 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.

Adicionalmente, contempla el artículo 58 del RGPD, en su apartado 2 d) 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...”*.

X

Al haberse confirmado la infracción, procede imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *“d) 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”*.

En el presente caso, se requiere al reclamado para que en el plazo de dos meses a partir de la notificación de la presente resolución:

- acredite la adopción de medidas adecuadas para evitar que en el futuro se produzcan incidencias como las que han provocado la apertura del presente procedimiento sancionador evitando incidentes de seguridad como el señalado al posibilitar el acceso a los datos carácter personal de la reclamante como consecuencia de la publicación de sus datos de carácter personal en el perfil público del Concello en Facebook.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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 CATOIRA, con NIF **P3601000G**,

- Por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD, una sanción de apercibimiento.
- Por una infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: ORDENAR al AYUNTAMIENTO DE CATOIRA, para que en el plazo de dos meses desde la notificación de la presente resolución, acredite la adopción de medidas adecuadas para que no vuelvan a producirse incidencias como la que dio lugar al procedimiento sancionador y que los tratamientos efectuados se ajustan a las disposiciones del RGPD.

TERCERO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE CATOIRA.

CUARTO: 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