

- **Expediente N.º: PS/00158/2021**

### RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

#### ANTECEDENTES

PRIMERO: En fecha 18 de noviembre de 2020, **D.ª A.A.A.** (en adelante, la parte reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos, contra el AYUNTAMIENTO DE ARNUERO, con NIF P3900600B, (en adelante, la parte reclamada).

La reclamante expone que el hijo de un vecino del municipio de Arnúero presentó una denuncia contra ella, aportando junto a esa denuncia, un correo electrónico que ella misma envió al Ayuntamiento el \*\*\*FECHA.1. Manifiesta que el Ayuntamiento proporcionó a esta persona copia de su escrito en el que constaban sus datos personales sin haberlos ocultado y que no se adoptaron las medidas necesarias para garantizar el cumplimiento de la normativa de protección de datos. En dicho correo electrónico se podía ver su nombre, apellidos, DNI, domicilio, teléfono móvil y dirección de correo electrónico.

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 LOPDGD), se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

En fecha 22 de febrero de 2021, se recibe escrito de respuesta del reclamado en el que pone de manifiesto que se cursa oficio a la empresa \*\*\*EMPRESA.1., con la cual el Ayuntamiento tenía contratada, a tal fecha, el asesoramiento en materia de protección de datos de carácter personal, y expone que:

- Hasta el día 25 de enero, no se produce la emisión de informe por parte de \*\*\*EMPRESA.1 y ello sólo tras diversas gestiones telefónicas. El indicado informe recibe nº entrada 2021-E-RC-XXX, también de 25 de enero, habiendo sido cursado a este Ayuntamiento por correo electrónico, junto con otro que se solicitaba a la indicada empresa, acerca del escrito interpuesto por un tercero ante este Ayuntamiento.

- Considerando insuficientes los términos del informe relativo a la reclamación, el día 29 de enero de 2021, se remite nueva comunicación por correo electrónico a la representación de \*\*\*EMPRESA.1, instando mayor concreción y alcance sobre las cuestiones que habían sido consultadas, dado que se consideraba que lo planteado desde la AEPD, lo hacía preciso antes de adoptar cualquier resolución.

- En relación con el informe adicional así solicitado, hasta la fecha de emisión del presente, no se tiene noticia alguna. Todo lo cual se pone en conocimiento, a los

efectos de que sea tenido en cuenta en la tramitación de las actuaciones con s./ref. E/ 10291/2020, indicando que han sido circunstancias totalmente ajenas a la voluntad municipal, las que han impedido dar cumplida respuesta a lo requerido, especialmente en lo relativo a los apartados mediante los que se requiere “la decisión adoptada a propósito de esta reclamación” y el “informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia”, dado que se estima la necesidad de que todo ello reciba un adecuado respaldo técnico-jurídico.

TERCERO: En fecha 8 de abril de 2021, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: En fecha 26 de noviembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 y 83.4 del RGPD, respectivamente.

Notificado el acuerdo de inicio, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que había procedido a implantar las medidas correctoras adecuadas para evitar la repetición de hechos similares en el futuro y solicitaba el archivo del procedimiento sancionador.

QUINTO: En fecha 27 de enero de 2022 se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se imponga al AYUNTAMIENTO DE ARNUERO, con NIF P3900600B, por una infracción del artículo 5.1. f) del RGPD, conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 i) de la LOPDGDD y por infracción del artículo 32 del RGPD, conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción den el artículo 73 apartado f) de la LOPDGDD, una sanción de apercibimiento. >>

SEXTO: La parte reclamada no ha presentado alegaciones a la Propuesta de Resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

#### HECHOS PROBADOS

PRIMERO: Consta que en fecha 18 de noviembre de 2020, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, toda vez que la parte reclamada proporcionó a un tercero, copia de su escrito en el que constaban sus datos personales sin haberlos ocultado.

SEGUNDO: Se verifica que se trata de un correo electrónico en el que se puede visualizar nombre, apellidos, DNI, domicilio, teléfono móvil y dirección de correo

electrónico de la reclamante, por lo que terceros ajenos tuvieron acceso no autorizado a dichos datos.

TERCERO: La parte reclamada expone que ha procedido a implantar las medidas correctoras adecuadas para evitar la repetición de hechos similares en el futuro. La documentación aportada se encuentra incorporada al expediente.

### FUNDAMENTOS DE DERECHO

PRIMERO: 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 y 48.1 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.”*

SEGUNDO: Establece el artículo 5.1.f) del RGPD lo siguiente:

“Artículo 5 Principios relativos al tratamiento:

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:

*“[...]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”.*

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado vulneró el artículo 5 “Principios relativos al tratamiento” del RGPD, apartado 1.f), al revelar información y datos de carácter personal a terceros.

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

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

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

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

*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”.*

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”.*

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

La falta de medidas de seguridad queda acreditada, además de por el resultado de revelación de información, conteniendo datos personales, por el hecho de que el Ayuntamiento en su contestación a esta Agencia, se compromete a la adopción de numerosas medidas de seguridad básicas, antes inexistentes. Por ejemplo “Establecer una Política de uso del sistema de información del Ayuntamiento.”

CUARTO: El artículo 83.5 del RGPD dispone lo siguiente:

*“5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

- a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;”*

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica “Infracciones” determina lo siguiente: *Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.*

A efectos del plazo de prescripción de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente: *“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

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

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

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

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

(...)

A efectos del plazo de prescripción de las infracciones, el artículo 73 de la LOPDGDD, bajo la rúbrica *“Infracciones consideradas graves”*, establece lo siguiente:

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

(...)

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

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD.

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

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



La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

SEXTO: El artículo 58.2 del RGPD dispone: *“Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

*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;”*

La imposición de esta última medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

SÉPTIMO: El artículo 83.7 del RGPD añade:

*“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.”*

El ordenamiento jurídico español ha optado por no sancionar con la imposición de multa administrativa a las entidades públicas sino con apercibimiento, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6. de la LOPDGDD:

*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.*

*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."*

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: SANCIONAR CON APERCIBIMIENTO al AYUNTAMIENTO DE ARNUERO, con NIF P3900600B, por una infracción del artículo 5.1. f) del RGPD y del artículo 32 del RGPD, tipificadas en los artículos 83.5 del RGPD y 83.4 del RGPD, respectivamente.

SEGUNDO: REQUERIR al AYUNTAMIENTO DE ARNUERO, que implante las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares.

TERCERO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE ARNUERO.

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.

938-150222

Mar España Martí

Directora de la Agencia Española de Protección de Datos