

- **Expediente N.º: EXP202310781 (PS/000372/2023)**

## RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

### ANTECEDENTES

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento con fecha 21 de julio de 2023 a través de denuncia interpuesta por **FACUA CASTILLA Y LEON - CONSUMIDORES EN ACCIÓN** (en adelante, la parte denunciante) de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos. La denuncia se dirige contra **AYUNTAMIENTO DE RENEDO DE ESGUEVA** con NIF **P4713400B** (en adelante, **AYUNTAMIENTO**) en relación con los siguientes hechos:

La parte denunciante manifiesta que el **AYUNTAMIENTO** ha publicado en su cuenta oficial de Facebook, el 28 de junio de 2023, el resultado del sorteo para ser miembro de las mesas electorales. Los listados publicados incluyen nombres y dos apellidos de cada miembro (vocales y suplentes) y nivel de estudios.

Junto a la denuncia se aporta capturas de pantalla de la publicación del **AYUNTAMIENTO** en Facebook, el 28 de junio de 2023, del resultado del sorteo para ser miembro de las mesas electorales.

SEGUNDO: Con fecha 30 de enero de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **AYUNTAMIENTO**, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, y por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, en el que se le indicaba que tenía un plazo de diez días para presentar alegaciones.

Este acuerdo de inicio, que se notificó al **AYUNTAMIENTO** con fecha 30 de enero de 2024, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en, como consta en el acuse de recibo que obra en el expediente.

TERCERO: Con fecha 8 de febrero de 2024, se recibe en esta Agencia, en tiempo y forma, escrito del **AYUNTAMIENTO** en el que aduce alegaciones al acuerdo de inicio en el que, en síntesis, manifestaba que:

*“1. Se ha procedido a la retirada inmediata de las publicaciones en la cuenta oficial de Facebook de este Ayuntamiento que han sido objeto de denuncia.*

*2.Dichas publicaciones se realizaron ante la insistencia y numerosas peticiones de vecinos dado que muchos de ellos se encontraban en periodo vacacional dificultando su notificación.”*

CUARTO: Con fecha 16 de febrero de 2024 se formuló propuesta de resolución, proponiendo que por la Directora de la AEPD se declare que el AYUNTAMIENTO DE RENEDO DE ESGUEVA, con NIF P4713400B, ha infringido lo dispuesto en el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.5 del RGPD, así como lo dispuesto en el artículo 32 del RGPD, infracción tipificada en el artículo 83.4 del RGPD.

Esta propuesta de resolución, que se notificó al AYUNTAMIENTO conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 16 de febrero de 2024, como consta en el acuse de recibo que obra en el expediente.

QUINTO: Con fecha 29 de febrero de 2024, se recibe en esta Agencia, en tiempo y forma, escrito del AYUNTAMIENTO en el que aduce alegaciones a la propuesta de resolución en el que, en síntesis, manifestaba que:

*“1. Este Ayuntamiento ha realizado las tareas indispensables para garantizar el cumplimiento de la normativa de Protección de datos, adjuntando al presente informe del Delegado de Protección de Datos en dicho sentido.*

*2.Este Ayuntamiento está muy concienciado respecto al cumplimiento de dicha normativa y se tomarán cuantas medidas sean necesarias para tal fin.”*

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

### HECHOS PROBADOS

PRIMERO: Con fecha 28 de junio de 2023, el Ayuntamiento de Renedo de Esgueva publicó en su cuenta oficial la red social Facebook, el resultado del sorteo para ser miembro de las mesas electorales (páginas 7 a 12 del expediente). Los listados publicados incluyen nombres y dos apellidos de cada miembro (vocales y suplentes), nivel de estudios y datos de la mesa asignada.

### FUNDAMENTOS DE DERECHO

#### I

#### Competencia

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 Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el **AYUNTAMIENTO**, para el cumplimiento con la normativa relativa al régimen electoral, realiza una actividad de tratamiento, como es la designación de los miembros de las mesas electorales, en la cual son objeto de tratamiento, entre otros, los siguientes datos personales de personas físicas: nombre, apellidos y nivel de estudios, entendiendo por dato de carácter personal: *"toda información sobre una persona física identificada o identificable"*.

El **AYUNTAMIENTO** realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD, que define al «responsable del tratamiento» o «responsable» como: *"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"*.

Se considera persona física identificable aquella 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.

Asimismo, debe entenderse por 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"*

Por su parte, el artículo 4 apartado 12 del RGPD define, de un modo amplio, 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.”*

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en el artículo 32 del RGPD, que reglamentan la seguridad del tratamiento.

### III

Contestación a las alegaciones al acuerdo de inicio y a las alegaciones a la propuesta de resolución

A) Con relación a las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por la parte reclamada en su escrito:

*“1. Se ha procedido a la retirada inmediata de las publicaciones en la cuenta oficial de Facebook de este Ayuntamiento que han sido objeto de denuncia.”*

El haber procedido a la retirada de la publicación del anuncio que ha motivado la incoación del presente procedimiento no implica una variación de la responsabilidad respecto a los hechos reclamados.

*“2. Dichas publicaciones se realizaron ante la insistencia y numerosas peticiones de vecinos dado que muchos de ellos se encontraban en periodo vacacional dificultando su notificación.”*

Tal y como se razonó en el acuerdo de inicio, según expone la Junta Electoral Central en su Acuerdo 663/2011 el carácter público del sorteo para la designación de los miembros de Mesa previsto en el artículo 26.2 Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (en adelante, LOREG), no determina la necesidad de la publicidad de los datos resultado de los mismos, especialmente teniendo en cuenta que no son definitivos, dado que podrían estar sometidos a excusa. La comunicación de la designación como miembro de Mesa electoral debe ser objeto de notificación, la cual se realizará conforme al modelo oficial correspondiente. En cualquier caso, toda medida adoptada para proporcionar información acerca del resultado del sorteo a los ciudadanos designados, con objeto de facilitar su participación como miembros de las mesas electorales, deberá respetar el principio de confidencialidad previsto en el artículo 5.1.f) del RGPD.

Por todo lo expuesto, se desestiman las alegaciones.

B) Con relación a las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas:

- *“El AYUNTAMIENTO ha realizado las tareas indispensables para garantizar el cumplimiento de la normativa de Protección de datos... está muy concienciado respecto al cumplimiento de dicha normativa y se tomarán cuantas medidas sean necesarias para tal fin.”*

Se valora positivamente las medidas adoptadas por el AYUNTAMIENTO en orden a procurar el debido cumplimiento por parte de sus empleados de la normativa de protección de datos, sin que estas desvirtúen la responsabilidad del AYUNTAMIENTO en la comisión de los hechos objeto del presente procedimiento.

Por todo lo expuesto, se desestiman las alegaciones.

#### IV

#### Integridad y confidencialidad

El artículo 5 del RGPD, bajo el título *“Principios relativos al tratamiento”*, establece en su apartado 1.f) 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 el presente caso, queda acreditado que el **AYUNTAMIENTO** publicó en su cuenta oficial de Facebook, el 28 de junio de 2023, los listados de personas que habían sido designadas para ser miembro de las mesas electorales, como resultado del correspondiente sorteo entre las personas censadas en el municipio. En estos listados publicados se incluyen nombres y dos apellidos de cada miembro (vocales y suplentes) y nivel de estudios, datos personales a los cuales tuvieron acceso terceras personas no autorizadas. El principio de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos personales no consentidas por los titulares de estos.

El Acuerdo 663/2011 de la Junta Electoral Central establece lo siguiente respecto a la publicación de la composición de las mesas electorales:

*“1º) La LOREG establece el carácter público del sorteo para la designación de los miembros de Mesa en el artículo 26.2 LOREG, pero no la publicidad de los datos resultado de los mismos, especialmente teniendo en cuenta que no son definitivos dado que podrían estar sometidos a excusa. Esta Presidencia no acierta a comprender la justificación de una publicidad de tal carácter, con la única excepción de que sea el interesado el que pueda comprobar, introduciendo sus datos personales, si ha resultado designado miembro de una mesa electoral, del mismo modo que sucede con la posibilidad de comprobación por el interesado de sus datos censales.*

*2º) Dicha publicación no podrá en ningún caso sustituir el acto de notificación de la designación. Es doctrina de esta Junta que la notificación se realizará en el modelo oficial aprobado por Real Decreto (Ac. 17 de Junio de 1987). El modelo oficial se contiene en el anexo 7. C .7.4ª del Real Decreto 605/1999 de 16 de abril por el que se establece la regulación complementaria de los procesos electorales.”*

De acuerdo con lo expuesto por la Junta Electoral Central, no existe causa que justifique la publicidad del resultado del sorteo para la designación de los miembros de las mesas, pese al carácter público del mismo. Recordemos que, según el artículo 19 de la LOREG, las consultas resueltas por la Junta Electoral Central tienen carácter vinculante.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable al **AYUNTAMIENTO**, por vulneración del artículo 5.1.f) del RGPD.

## V

### Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

El artículo 83.5.a) del RGPD tipifica como infracción la vulneración de las disposiciones siguientes:

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

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72 de la LOPDGDD, que califica de muy grave la siguiente conducta:

*“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. (...)”*

## VI

### Declaración de infracción

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:*

*a) [...]*

*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 declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*

*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.”*

Por lo tanto, este precepto establece que los procedimientos que tengan causa en infracciones en materia de protección de datos personales cometidas por las categorías de responsables o encargados del tratamiento enumerados en su apartado 1 se resolverán declarando la infracción.

Confirmado que la conducta efectuada por el AYUNTAMIENTO constituye una vulneración del artículo 5.1.f) del RGPD, corresponde declarar que se ha cometido una infracción por parte de la AYUNTAMIENTO.

## VII Seguridad del tratamiento

El Artículo 32.1, “*Seguridad del tratamiento*”, del RGPD establece:

*“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.*
- (...)”.*

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”.*

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

*“Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.”*

La responsabilidad del **AYUNTAMIENTO** viene determinada por la falta de medidas de seguridad apropiadas, 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, con objeto de asegurar que los

datos personales de los ciudadanos que formen parte de las mesas electorales de su municipio no queden al acceso de terceros no autorizados.

En este sentido, el Considerando 74 del RGPD establece que:

*“Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.”*

Trasladando estas consideraciones al caso concreto, se puede concluir que, en el momento de realizarse la denuncia, el **AYUNTAMIENTO** no disponía de las medidas de seguridad razonables en función de los posibles riesgos estimados.

No consta ninguna medida específica de carácter técnico u organizativo destinada a evitar la comunicación a un tercero no autorizado de los datos personales de los ciudadanos obrantes en la base de datos del **AYUNTAMIENTO**, teniendo en cuenta que desde el año 2011 existía un acuerdo de la Junta Electoral Central afirmando que la publicación de los datos personales de miembros de las mesas electorales no era una medida amparada por la normativa del régimen electoral general.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable al **AYUNTAMIENTO**, por vulneración del artículo 32 del RGPD.

## VIII

### Tipificación y calificación de la infracción del artículo 32 del RGPD

El artículo 83.4.a) del RGPD tipifica como infracción la vulneración de las disposiciones siguientes:

*“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, la infracción imputada prescribe a los dos años, conforme al artículo 73.f) de la LOPDGDD, que califica de grave la siguiente conducta:

*“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.  
(...)*

## IX

### Declaración de infracción

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:*

*a) (...)*

*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 declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*

*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."*

De este modo, este precepto establece que los procedimientos que tengan causa en infracciones en materia de protección de datos personales cometidas por las categorías de responsables o encargados del tratamiento enumerados en su apartado 1 se resolverán declarando la infracción.

Confirmado que la conducta efectuada por el AYUNTAMIENTO constituye una vulneración del artículo 32 del RGPD, corresponde declarar que se ha cometido una infracción por parte de la AYUNTAMIENTO.

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:** DECLARAR que **AYUNTAMIENTO DE RENEDO DE ESGUEVA**, con NIF P4713400B, ha infringido lo dispuesto en el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.5 del RGPD, y lo dispuesto en el artículo 32 del RGPD, infracción tipificada en el artículo 83.4 del RGPD.

**SEGUNDO:** NOTIFICAR la presente resolución a **AYUNTAMIENTO DE RENEDO DE ESGUEVA**.

**TERCERO:** 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.

938-16012024

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