

- **Expediente N°: PS/00465/2021**

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) con fecha 17 de junio de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra **AYUNTAMIENTO DE OURENSE** con NIF **P3205500F** (en adelante, la parte reclamada).

El motivo en que basa la reclamación es que el reclamante, representante sindical por el sindicato SPPME reclama contra Administración Local reclamada porque no adopta las debidas medidas de seguridad en la gestión de datos de trabajadores de la Policía Municipal.

Justifica sus manifestaciones afirmando que el citado ayuntamiento:

- publica datos de agentes de policía municipal en los Tablones de Anuncios en la Jefatura de Policía Local, exponiéndolos a todos los trabajadores.
- se realiza la entrega de documentación personal en la que figuran datos de otros compañeros, mediante sobres no cerrados; y
- ha instalado un sistema de videovigilancia en el garaje interior del edificio, sin haber informado a los trabajadores sobre su colocación, y pese a que existe cartel, en este no se indica quién es el responsable del tratamiento ni a dónde ha de dirigirse para el ejercicio de sus derechos.

Como pruebas de los hechos denunciados se aporta:

- copia del Tablón de Anuncios, donde aparecen datos de agentes, en lo relativo a comunicación de periodos de vacaciones; así como una resolución de denegación de solicitud de vacaciones en la que se recoge un listado de denegaciones, y no se trata de una comunicación particularizada.
- un correo remitido al DPD del Ayuntamiento exponiendo dicha situación.

No aporta imágenes de la ubicación de las cámaras.

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, el 28 de junio de 2021, y se reitera el 12 de agosto de 2021, 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.

No se ha recibido respuesta a dicho requerimiento.

TERCERO: Con fecha 21 de septiembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

CUARTO: Con fecha 10 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, artículo 32 del RGPD y artículo 13 del RGPD, tipificada en el artículo 83.5 del RGPD.

QUINTO: Notificado el citado acuerdo de inicio, el reclamado presentó escrito de alegaciones en el que manifiesta lo siguiente:

En relación con el sistema de videovigilancia se indica que el responsable es el Ayuntamiento objeto de esta reclamación, existiendo distintos carteles en el edificio policial con la leyenda “zona videovigilada”, tanto en la entrada del mismo, por la puerta principal como en la entrada al garaje.

La gestión del sistema de videovigilancia se realiza por personal del propio centro (un policía), sin que se encuentre contratado el mantenimiento con ninguna empresa por parte del Ayuntamiento.

En la zona del garaje de las dependencias policiales se encuentran ubicadas un total de 4 cámaras no ficticias, sino en funcionamiento, el plazo de conservación es de 1 mes.

La ficha del registro de actividades se puede consultar en el siguiente enlace: ***URL.1

Las imágenes de las cámaras únicamente pueden visionarse “in situ”, esto es, en el lugar donde se encuentra el grabador, que es un cuarto cerrado bajo llave.

Las cámaras se encuentran situadas en una zona común (garaje), no se han instalado ni existe cámara alguna en zonas no permitidas como puedan ser vestuarios, zona de descanso o aseos.

En relación con la publicación en el tablón de anuncios el ayuntamiento reclamado quiere hacer constar que el tablón de anuncios se encuentra ubicado en la sede de la Jefatura de la Policía Local, estando la entrada del mismo sometida a la vigilancia de personal externo y con los oportunos controles de acceso.

Dichos tablonos existen en el resto de Cuerpos de Seguridad del Estado y Comunidades Autónomas.

Su finalidad es la de anunciar, facilitar y trasladar información de interés para los trabajadores policiales relacionada con el servicio policial desde siempre, tales como: listados de servicio de los días en los que los policías trabajan (con su nombre, claves profesionales, secciones asignadas, si se encuentran en descanso reglamentario, de vacaciones, de asuntos propios, etc.). Así mismo se cuelgan en él comunicados y avisos varios de régimen interno, Órdenes de Servicio, listados de concesión o denegación de permisos con el nombre de los policías (asuntos propios, festividades, cambios e intercambios de turno entre policías, etc.)

En los Cuerpos de Seguridad el trabajo se desempeña a turnos, tanto de mañana, como de tarde y noche y los 365 días del año, por lo que es uno de los instrumentos que permiten facilitar la información que precisan los trabajadores dentro de una organización policial, al no encontrarse todos de servicio ni en las mismas jornadas ni en los mismos horarios.

En la fotografía que se adjunta, de uno de los escritos colgados en dicho tablón y referido al período vacacional, constan al igual que en otros tantos otros anuncios (anteriormente indicados), los nombres de los funcionarios policiales, no datos sensibles o especialmente protegidos ni otros como puedan ser teléfonos, DNI, domicilios, correos electrónicos, etc, a fin, en este caso concreto, de comunicar a los policías la situación que, en aquel momento afectaba al disfrute de su período vacacional y ello a efectos de que dispusieran, con la suficiente antelación, de la programación del trabajo en época estival en relación a las medidas de conciliación de la vida familiar y laboral.

SEXTO: Con fecha 9 de diciembre de 2021 el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, así como los documentos aportados por el reclamado.

SEPTIMO: Con fecha 7 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 OURENSE**, con NIF **P3205500F**, por una infracción del artículo 5.1.f) del RGPD, artículo 13 del RGPD y artículo 32 del RGPD, tipificadas en el artículo 83.5, las dos primeras y en el artículo 83.4 del RGPD la última de ellas, una sanción de apercibimiento.

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

HECHOS PROBADOS

PRIMERO: El ayuntamiento denunciado hace públicos datos personales de sus trabajadores a través del Tablón de Anuncios de la Jefatura de Policía Local, indicando datos relativos a comunicación de periodos de vacaciones denegados.

En segundo lugar, se denuncia además, que el cartel de zona videovigilada del ayuntamiento denunciado, no señala quien es el responsable del tratamiento y donde dirigirse para el ejercicio de los derechos.

En tercer lugar, se manifiesta que el ayuntamiento denunciado entrega información personal en sobres abiertos.

SEGUNDO: El ayuntamiento manifiesta en relación a la publicación en el Tablón de Anuncios el reclamado quiere hacer constar que el tablón de anuncios es uno de los instrumentos que permiten facilitar la información que precisan los trabajadores dentro de una organización policial, al no encontrarse todos de servicio ni en las mismas jornadas ni en los mismos horarios, y que se encuentra ubicado en la sede de la Jefatura de la Policía Local, estando la entrada del mismo sometida a la vigilancia de personal externo y con los oportunos controles de acceso.

En relación con su sistema de videovigilancia, manifiesta que existen distintos carteles en el edificio policial con la leyenda “zona videovigilada”, tanto en la entrada del mismo, por la puerta principal como en la entrada al garaje y que las cámaras se encuentran situadas en una zona común (garaje), y que no se han instalado ni existe cámara alguna en zonas no permitidas como puedan ser vestuarios, zona de descanso, o aseos.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

El artículo 6.1 del RGPD, establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

Por su parte, el artículo 5 del RGPD establece que *“los datos personales serán:*

“a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

En segundo lugar, hay que señalar que la seguridad de los datos personales viene regulado 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”.

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.
(...)”*

En tercer lugar, en relación con la información que deberá facilitarse cuando los datos personales se obtengan del interesado, el artículo 13 del RGPD establece lo siguiente:

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

En este sentido, informar sobre la videovigilancia según el RGPD es una obligación recogida en este marco legislativo.

Se debe disponer de un dispositivo informativo en zona visible (vgr. puerta de acceso) indicando que se trata de una zona video-vigilada, en el mismo se deberá indicar la existencia del tratamiento, la identidad del responsable, así como la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal, que puede ser objeto de tratamiento para diversas finalidades.

El artículo 22 de la Ley Orgánica 3/2018 (5 diciembre)-LOPDGDD- dispone:

“1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

La AEPD, en un informe relacionado, estipula que no es necesario que los carteles se sitúen justo debajo de las cámaras. Basta con hacerlo en un lugar visible y que incluya los espacios abiertos y cerrados donde el circuito de videocámaras esté operativo.

Este distintivo se exhibirá en lugar visible, y como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores. En caso de que el espacio videovigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos.

III

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”.

IV

En el presente caso, se ha constatado a través de la documentación obrante en el expediente 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 publicar en el tablón de anuncios de la policía, nombre y apellidos de agentes.

A la vista de lo indicado por la parte reclamada, amén de que se publiquen los listados con nombres y apellidos, hay información referida a personas físicas que no debe publicarse ya que va más allá de la mera finalidad organizativa del trabajo, por ejemplo, las vacaciones o los asuntos propios o permisos de cada uno, son todos ellos asuntos de interés meramente personal, y no público.

Además, toda esa información si se sigue publicando irá ligada a otros datos como el número de placa o el DNI, que identifica de manera inequívoca al agente y que puede ser perfectamente conocida por sus compañeros en el ámbito laboral.

Se considera que el tratamiento de los datos personales por la parte reclamada ha excedido claramente la finalidad para la que fueron dados, principalmente en el ámbito de vacaciones, permisos y asuntos propios.

A este respecto ha de indicarse, por tanto, que no es preciso publicar todos los datos que figuran en el tablón de anuncios para lograr la finalidad organizativa perseguida por la parte reclamada, y que es perfectamente compatible con el cumplir con el deber de confidencialidad.

El deber de confidencialidad debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos personales sin el consentimiento de sus titulares.

Por tanto, 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.

En segundo lugar, se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al entregarse documentación personal en la que figuran datos de otros compañeros, mediante sobres no cerrados, permitiendo el acceso a los mismos con quebrantamiento de las medidas establecidas.

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. Sin embargo, de la documentación aportada se desprende que la entidad no solo ha incumplido esta obligación, sino que además se desconoce la adopción de medidas al respecto, pesar de haberle dado traslado de la reclamación presentada.

Por ello, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

En relación al sistema de videovigilancia del reclamado, este manifiesta que las imágenes de las cámaras únicamente pueden visionarse “in situ”, esto es, en el lugar donde se encuentra el grabador, que es un cuarto cerrado bajo llave y que dichas cámaras se encuentran situadas en una zona común (garaje), no se han instalado ni existe cámara alguna en zonas no permitidas como puedan ser vestuarios, zona de descanso o aseos.

No obstante, se considera que la parte reclamada dispone de un sistema de videovigilancia, cuyo distintivo informativo presenta irregularidades al no acreditarse por parte del responsable del tratamiento pese a su requerimiento, una dirección efectiva dónde ejercitar los derechos regulados legalmente.

Los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada de vulneración del contenido del art. 13 RGPD.

V

La vulneración del artículo 5 del RGPD se encuentra tipificada en el artículo 83.5 a) del RGPD, considera que la infracción de *“los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9”* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, *“con multas administrativas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”*.

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

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

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

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

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

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

Por su parte, la LOPDGDD en su artículo 71, *Infracciones*, señala que:

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

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

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

(...)

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

La vulneración del artículo 13 del RGPD se encuentra tipificada en el artículo 83.5.b) del RGPD establece que:

“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:

b) los derechos de los interesados a tenor de los artículos 12 a 22;”

A su vez, el artículo 74.a) de la LOPDGGDD, bajo la rúbrica “Infracciones consideradas leves dispone:

“Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.”

VI

Por lo tanto, los hechos objeto de esta reclamación acreditan la existencia de infracción por parte del reclamado al vulnerar lo dispuesto en los artículos 5.1.f), 32.1 y 13 del RGPD.

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: QUE al **AYUNTAMIENTO DE OURENSE**, con NIF **P3205500F**, por infracción del artículo 5.1.f) del RGPD, artículo 13 del RGPD y artículo 32 del RGPD, tipificadas en el artículo 83.5, las dos primeras, y en el artículo 83.4 del RGPD la última de ellas, se le imponga por cada una, una sanción de apercibimiento.

SEGUNDO: REQUERIR al **AYUNTAMIENTO DE OURENSE**, con NIF **P3205500F**, al amparo de lo dispuesto en el artículo 58.2 d) del RGPD, que adopte las medidas necesarias para actualizar su “Política de Privacidad” a la normativa vigente en materia de protección de datos personales, *-Reglamento (UE) 2016/679 (RGPD)-*, adecuando la información ofrecida a las exigencias contempladas en el artículo 13 del RGPD, debiendo facilitar a los usuarios, con carácter previo a la recogida de los datos personales de los mismos, toda la información exigida en el citado precepto, para lo que la parte reclamada deberá tener en cuenta lo dispuesto en el artículo 6 del RGPD en relación con la licitud del tratamiento, así como lo indicado en el artículo 5 del RGPD en lo relativo a la finalidad del tratamiento y plazo de conservación de los datos.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Dichas medidas se han de adoptar en el plazo de un mes computado desde la fecha en la que se le notifique esta resolución sancionadora, debiendo aportarse los medios de prueba acreditativos de su cumplimiento.

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

CUARTO: NOTIFICAR la presente resolución a **AYUNTAMIENTO DE OURENSE**.

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