Expediente N.º: EXP202209615

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 27/07/2022, tuvo entrada en esta Agencia un escrito presentado por ***A.A.A.*** (en adelante, la parte reclamante), mediante el que formula reclamación contra el AYUNTAMIENTO DE PALMA con NIF P0704000I (en adelante, AYUNTAMIENTO), por un posible incumplimiento de lo dispuesto en la normativa de protección de datos de carácter personal.

Los motivos en que basa la reclamación son los siguientes:

"[…]

Primero.- El 22/05/2020, presenté en una oficina de correos cinco documentos. Todos ellos, de idéntico contenido, iban dirigidos a cinco áreas distintas del Ayuntamiento de Palma. Por error de la oficina de Correos, se sellaron con entrada de 29/09/2020 aunque el ayuntamiento de Palma los registró el día 26/05/2020 (…).

*Segundo.- El día *****FECHA.1**, el periódico de mayor tirada en Baleares (*****PERIÓDICO.1**), publicaba en su página 16, una noticia que reflejaba, con casi absoluta fidelidad, parte del contenido de los escritos que había realizado. En el subtítulo de esta noticia aparecía mi nombre completo (debajo del titular) y se repetía en el cuerpo del artículo. Se adjunta como Anexo I una copia de esa página. La edición digital del periódico, todavía disponible, también reflejaba casi idéntico texto.*

El día 04/06/2020, el mismo periódico publicaba en su página 14, una nueva noticia que se podía presumir derivada de sus mismos escritos, dando publicidad a algunos aspectos no tratados en el día anterior, también con alta fidelidad. Aparece de nuevo en el cuerpo del artículo, mi nombre completo. Se adjunta como Anexo ll una copia de esa página. La edición digital del periódico, todavía disponible, también reflejaba casi idéntico texto.

*El día 07/06/2020 aparece un tweet del periodista Sr. **B.B.B.**, uno de los autores del artículo del periódico *****PERIÓDICO.1** a que se ha hecho referencia antes. En dicho tweet se puede leer el siguiente texto:*

*"Me acabo de leer los 30 folios de informe del oficial **C.C.C.** sobre las, supuestas irregularidades y purga en la *****EMAIL.1 ***EMAIL.2**. El mismo ya está en Fiscalía de Baleares. Me acaban de 'soplar' que el tema bolsa de horas traerá cola. Judicial, me refiero."*

Ese tweet iba acompañado de una imagen que resulta ser una fotografía de una copia de uno de mis cinco escritos. Se adjunta como anexo III. Esto demostraría, a priori, que el acceso al documento no fue parcial, sino completo.

Tercero.- Ya de antemano se señala que jamás he hablado con ningún periodista de la ******PERIÓDICO.1*** *sobre mi escrito y que yo no filtré ese documento. (…)*

Los cinco documentos presentados lo fueron en oficina de correos, siendo que el acuso de recibo de que dispongo de cada uno de ellos tiene únicamente el sello de dicha oficina de correos. Por otro lado, la fotografía que de uno de los documentos publica el periodista ya citado en su tweet tiene 3 sellos. El primero, el de la oficina de correos, de fecha 29/05/2020, el segundo, el sello de entrada en el registro del Ayuntamiento de Palma, con fecha 26/05/2020, con número (…); el tercero, el sello de entrada interno en el Área de Justicia Social, Feminismo y LGTBI, de fecha 27/05/2020 (…).

Cuarto.- Los periodista Sr. ***B.B.B.*** *y Sra.* ***D.D.D.*** *hacen una difusión innecesaria de mis datos personales. No soy una figura pública ni tampoco un responsable de la Policía Local de Palma (…).*

Quinto.- En fecha 27/10/2021, mediante decreto número (…) de la Regidora de Seguridad Ciudadana, se incoa expediente disciplinario por la presunta comisión de dos faltas graves y una leve derivadas, exclusivamente, de los escrito que presenté el 22/05/2020 en la oficina de correos. No hay error en la fecha: la incoación es del 27/10/2021, 523 días después de la instancia que lo motiva. (…)

El parecer de la instructora:

[…]

Se considera que sí ha habido una vulneración de la Ley de protección de datos, pero la víctima es el propio inculpado, criterio compartido con la Oficina de la Defensora de la Ciudadanía.

[…]”

Junto a la reclamación aporta, entre otros, la siguiente documentación:

- Fotografías, de fecha 3 y 04/06/2020, de la noticia publicada en el periódico “******PERIÓDICO.1***”.

- Captura de pantalla del tweet publicado en el perfil de ******PERFIL.1*** junta a una breve explicación de lo que se advierte en la imagen publicada.

- Copia de la Resolución provisional del expediente disciplinario, de fecha 12/07/2022.

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 15/09/2022 se dio traslado de dicha reclamación a la editora del periódico mencionado, HORA NOVA, S.A. y al AYUNTAMIENTO, para que

procediesen a su análisis e informasen 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 15/09/2022 y 16/09/2022, respectivamente, como consta en los certificados que obran en el expediente.

Con fecha 13/10/2022, se recibe en esta Agencia escrito de respuesta del AYUNTAMIENTO, en el que manifiesta lo siguiente:

"[…]

La información de datos personales que se ha hecho pública no fue realizada por parte del Ayuntamiento, sino que ha sido por parte de un periodista que fotografió o publicó una fotografía en la que aparecían datos personales que constan en un documento presentado ante la Administración municipal, difundiendo dicha fotografía e información en una red social mediante un tweet. (…)

En dichas noticias publicadas en el periódico, únicamente aparece el nombre de un funcionario de la policía local, sin ningún otro dato de carácter personal identificativo (DNI, domicilio, etc)

[…]

El Ayuntamiento, a nuestro entender, únicamente tiene responsabilidad en lo que a este caso se refiere, en su deber de custodiar la documentación obrante en sus expedientes así como de garantizar el principio de seguridad de los datos personales que consten en los ficheros, expedientes administrativos de sus Concejalías/Departamentos municipales.

En el caso relativo a los hechos denunciados, existe la actividad de tratamiento de Registro General del Área de Participación Ciudadana y Gobierno Interior, publicado en el Web municipal, en el REGISTRO DE ACTIVIDADES DE TRATAMIENTO del Ayuntamiento de Palma, si bien el responsable de la custodia de la documentación municipal, una vez se ha procedido al reparto de la documentación recibida es el titular del Área donde se remite dicha documentación.

En el caso que nos ocupa, nos encontramos con la peculiaridad que el Sr*. **XXXXXXX** no presentó un único escrito, sino que presentó ante el Registro General del Ayuntamiento un total de 5 documentos con el mismo contenido de 30 páginas, y en vez de hacerlo en un documento único , (…), se presentaron en el Registro General del Ayuntamiento de Palma, los siguientes 5 escritos con copia de la correspondiente documentación (…)*

*En la fotografía que aparece en el mencionado tweet del periodista, se observa el Registro de entrada núm. **XXXXX**, Documento **XXXXX**, que como puede observarse corresponde a uno de los citados escritos, concretamente el documento dirigido al*

Área de Justicia Social, Feminismo y LGTBI. Por parte del Sr. ***XXXXXXX*** *también se dirigió escrito a la Defensora de la Ciudadanía, quien inició el expediente* ******EXPEDIENTE.1****, informe de fecha* ******FECHA.2*** *del que se adjunta copia en el Anexo I comunicándose también las actuaciones realizadas al denunciante, mediante escrito de fecha* ******FECHA.3****.*

Por parte de la Oficina de la Defensora de la Ciudadanía se requirió en esta fecha al Área de Justicia Social, Feminismo y LGTB, como primera implicada, así como a la Secretaría General del Pleno y al Gabinete de Alcaldía, solicitando información al respecto y que se valorara la actuación para establecer las medidas disciplinarias y de seguridad pertinentes, sin que conste que por parte de los responsables de Justicia Social se diera ningún tipo de contestación.

Posteriormente, con fecha 21 abril 2021, una vez que el Ayuntamiento contaba con la designación de su Delegado de Protección de Datos, por parte de la Oficina de la Defensora de la Ciudadanía se remitió por correo electrónico copia de dicho expediente para su conocimiento y seguimiento al ser objeto de datos personales.

Por parte del DPD, se solicitó el mismo día de su recepción información a los responsables del Área de Justicia Social, concretamente al Director General y a la Concejal responsable del Área, sin recibir respuesta alguna de los responsables del Área de Justicia Social; informándose de todo ello a Coordinación de Alcaldía.

Con fecha 3 de agosto 2021 se reiteró mediante correo electrónico el requerimiento de información del día 21 abril del mismo año, obteniendo de nuevo el silencio por respuesta. (…)

Recientemente, una vez recibido el requerimiento de la AEPD, por parte del Jefe de Servicio de Justicia Social, Feminismo y LGTBI, con fecha 26 de septiembre de 2022, se realizó el informe que se adjunta como anexo II y del que se desprende que de dicha documentación (la que ha originado la actuación de la AEPD) tuvieron conocimiento tanto el Jefe de Servicio como la Concejal a quien se le entregó el documento.

También informa que con fecha 16 de junio de 2020 fue devuelta esta documentación a la OAC Backoffice mediante oficio para remitir al Área de Hacienda, Innovación y Función Pública, fecha por otra parte que no hace más que confirmar que en la fecha de publicación de la publicación objeto de este asunto – del 3 al 7 de junio – estaba bajo la custodia y responsabilidad del área de Justicia Social.

Respecto a la identificación nominal de la Autoridad o directivo responsable del tratamiento en el momento en que se produjeron los hechos (junio 2020), apunta que era la Concejala titular del Área de Justicia Social, Feminismo y LGTBI, Sra. ***D.D.D.,*** *tal como se desprende de los informes realizados tanto por parte de la Oficina de la Defensora, como del Área de Seguridad Ciudadana, del Jefe de Servicio de la propia Área de Justicia Social, y de la propia Instructora del Expediente disciplinario AJT 202120479 incoado al efecto.*

Apuntar que tanto el Director General, como la Concejal responsable del Área, dimitieron de sus cargos en el transcurso de la primera mitad del año 2022, sin ostentar actualmente competencia alguna en dicha área de gobierno municipal.

En cuanto a las medidas preventivas que por parte del Delegado de Protección de Datos se han impulsado y propuesto respecto al deber de fidelidad y secreto así como de custodia y seguridad de la información, básicamente han sido las siguientes:

- *Publicación en abril de 2021, en el Portal del Personal, con la obligación de leerlo y marcar que se ha leído y entendido, del DECÁLOGO DE FUNCIONES Y OBLIGACIONES de todos los usuarios, recordando en este documento en su apartado 12 el tema de la Confidencialidad de la información y deber de secreto respecto a toda la información municipal advirtiendo de las responsabilidades administrativas y penales en que pueden incurrir.*

- *Acciones formativas diversas durante 2021 y 2022 entre el personal municipal con el fin de sensibilizar del tema de protección de datos, incluido el citado decálogo de funciones y obligaciones.*

- *Remisión del cuestionario sobre Listado de cumplimiento normativo a todos los responsables municipales, siguiendo el modelo publicado por la AEPD, mediante correo electrónico de fecha 4 octubre 2021, recordatorio de que se deben aplicar las medidas oportunas y eficaces para demostrar la conformidad de las actividades de tratamiento con el objeto de poder valorar los aspectos que deben tener en cuenta durante los procedimientos de análisis de riesgo y evaluación de impacto, sin que conste que se haya obtenido respuesta del Área de Justicia Social, Feminismo y LGTBI.*

- *Publicaciones en Intranet municipal sobre diversos temas relativos a sensibilización y obligaciones en materia de protección de datos durante 2021 y 2022.*

- *Se ha reclamado por escrito dirigido al Alcalde y también en la Memoria anual de 2021 una serie de recomendaciones (apartado 12) a los responsables de los tratamientos y de la seguridad de la información, revisar la Política de Seguridad corporativa así como aprobar las políticas específicas y realizar un análisis de riegos y redactar el plan de implementación de la política de seguridad, aprobación de la organización de la seguridad municipal, nombrar responsable y comité STIC así como poner en marcha el Centro de Operaciones de Seguridad con el fin de realizar la vigilancia y detección de incidentes de seguridad y otras funciones; medidas que se han anunciado públicamente que se han iniciado pero que aun no han culminado.*

En cuanto a las medidas adoptadas respecto al caso expuesto, cabe apuntar:

- *Decreto de Alcaldía* ******DECRETO.1*** de ******FECHA.4*** *que incoó expediente disciplinario a un agente de policía local.*

- *Por parte del DPD se ha solicitado información a las siguientes áreas: Justicia Social, Alcaldía, Función Pública y Seguridad Ciudadana, habiéndose obtenido las respuestas siguientes:*

[…]"

Junto al escrito acompaña, entre otra, la siguiente documentación:

- Copia del escrito emitido por la Defensora de la Ciudadanía en relación con el expediente ******EXPEDIENTE.1***.

- Copia del Informe de las actuaciones llevadas a cabo por el Área de Justicia Social, Feminismo y LGTIB en relación con el escrito presentado por la parte reclamante.

- Copia de la "Declaración en materia de protección de datos personales" del Ayuntamiento de Palma.

Con fecha 18/10/2022, se recibe en esta Agencia escrito de respuesta de HORA NOVA, S.A. en el que manifiesta lo siguiente:

"[…]

1.- Las noticias publicadas por el diario "Ultima Hora" en fechas 3 junio 2020 y 4 junio 2020 son fiel reflejo de los hechos ocurridos y se limitan a informar, con absoluta veracidad, acerca de las cinco denuncias presentadas nominativamente por el Oficial de la Policía Local de Palma ante cinco departamentos distintos del Ayuntamiento de Palma (Seguridad Ciudadana, Hacienda, Justicia Social, Feminismo y LGTBI) por presuntas irregularidades internas acaecidas en el seno de dicha institución, información cuya fuente, por motivos de secreto profesional, no deben desvelar. Es obvio que, de haber querido preservar su identidad, el Sr. ***XXXXXXX*** *no hubiera denunciado tales hechos por la vía y en la forma que lo hizo.*

2.- El tweet del periodista ***B.B.B.*** *es un simple comentario en relación con dichas denuncias amparado por el derecho fundamental a la libertad de información y expresión. Asimismo, en la fotografía que acompaña al expresado tweet aparecen unos documentos prácticamente ilegibles a simple vista.*

3.- Tanto los artículos de "Ultima Hora" como el tweet del Sr***. XXXXXXX*** *se limitan a informar de un hecho absolutamente veraz, de indudable interés general y de relevancia pública, sin que se revele dato alguno distinto de los que aparecen en los propios escritos y en los que se denuncian gravísimas irregularidades internas en el seno de la Policía Local de Palma, hechos que podrían ser constitutivos de graves delitos cometidos por funcionarios públicos y denunciados por funcionario público, circunstancias que hacen absolutamente noticiable la información y que -en el marco de un razonable juicio de ponderación- hacen prevalecer el Derecho a la Información frente a cualquier otro derecho en colisión. (…)*

5.- En cualquier caso, tanto los artículos periodísticos como el tweet publicados (hace ya más de dos años) han sido borrados de la edición digital y de la red social.

6.- Señalar, por último, que "Hora Nova" y "Ultima Hora" han impartido en todo momento a trabajadores y colaboradores todas las recomendaciones necesarias para garantizar el máximo respeto a la protección de los datos de carácter personal conforme a la LOPD, las políticas de privacidad y demás normativa vigente. Y así se ha hecho también en este caso concreto de cara a futuras eventuales publicaciones que pudieran surgir en relación al mismo.

[…]"

Junto al escrito aporta la siguiente documentación:

- Informe de la auditoría de ciberseguridad, de fecha 05/05/2022.

- Copia de la Política de privacidad del medio "******PERIÓDICO.1***".

TERCERO: Con fecha 25/10/2022, se comprueba que los enlaces enumerados en la reclamación relativos a la versión digital del periódico "******PERIÓDICO.1***" continúan activos con datos identificativos de la parte reclamante.

CUARTO: En fecha 27/10/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

QUINTO: Con fecha 08/12/2022, esta Agencia recibe nuevo escrito de la parte reclamante en el que comunica que *"en fecha 04/11/22 se emite decreto* ******DECRETO.1*** *de la regidora del Área de Seguridad Ciudadana del Ayuntamiento de Palma (notificado el 10/11/22), en el que se determina el archivo definitivo del expediente disciplinario propuesto por la instructora el 07/10/22"*. Adjunta copia de dicha resolución.

SEXTO: Con fecha 24/02/2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al AYUNTAMIENTO con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción de los artículos 5.1.f) y 32 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), tipificadas en el artículo 83.5.a) y 83.4 del RGPD.

Este acuerdo de inicio, que se notificó conforme a las normas establecidas en la LPACAP mediante notificación electrónica, fue entregado al AYUNTAMIENTO el 28/02/2023.

SÉPTIMO: Con fecha 10/03/2023, el AYUNTAMIENTO presentó escrito, en tiempo y forma, ante esta Agencia en el que manifiesta lo siguiente:

"[…]

Primera.- Que la presunta infracción del art. 32 RGPD, conforme a lo dispuesto en el art. 83.4 RGPD, calificada como grave, ha prescrito, puesto que de acuerdo con lo

señalado en el art. 73 de la LOPDGDD que señala: (…), dado que transcurrieron más de dos años entre los hechos (mayo/junio del 2020) y el escrito de reclamación que el Sr. ***XXXXXXX*** *presentó ante la AEPD (julio 2022), que dio inicio al expediente objeto de estas alegaciones.*

Segunda.- Que por parte del Ayuntamiento no se ha vulnerado el principio de confidencialidad establecido en el art. 5.1.f del RGPD (…):

1. Que el reclamante, (…) envió 5 escritos con copia de la correspondiente documentación dirigida a 5 áreas diferentes del Ayuntamiento de Palma (Área de Seguridad Ciudadana, Área de Hacienda, Innovación y Función Pública, Alcaldía, Área de Justicia Social, Feminismo y LGTBI y Oficina Defensora de la Ciudadanía), dando lugar con esta proliferación de escritos presentados en formato papel a devoluciones a la OAC BackOffice al no ser competentes algunas de las Áreas para resolver lo solicitado por el reclamante. Dicha proliferación de escritos dificultaron la tramitación y unificación de actuaciones entre las Áreas municipales así como el control y preservación de su identidad.

[…]

3. (…) En este caso concreto, no se tenía acceso a ningún dato de categoría especial o sensible que requiriera una especial protección, sin tenerse que aplicar ninguna restricción extraordinaria al ser los datos contenidos en dicha documentación datos meramente de carácter identificativo (nombre y apellidos, DNI y domicilio –siendo éste el domicilio facilitado el del lugar de trabajo del reclamante).

4. Por otra parte, debe tenerse en cuenta la existencia de la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno, que tiene por objeto la transparencia de la actividad pública y regular y garantizar el derecho de acceso a la información , teniendo los medios de comunicación el derecho a la información pública de los documentos o contenidos que obren en poder de la Administración, no siendo el documento objeto del expediente ninguno de lo que puedan ser limitados ni ninguno de los datos especialmente protegidos a los que se refiere el art. 15 de dicha Ley 19/2013.

[…]

6. (…) Apuntar que en nuestro caso, la posible brecha de confidencialidad, únicamente habría afectado a datos meramente identificativos del reclamante sin que ello hubiera supuesto ninguna violación de seguridad, sino un hecho puntual al no haber realizado la disociación de datos de la persona responsable. Tampoco se da ninguno de los supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados contemplados en el Considerando 75 del RGPD.

7. Que por parte del Ayuntamiento de Palma, se han impulsado y propuesto diversas medidas relativas al respeto al deber de fidelidad y secreto así como de custodia y seguridad de la información (…)”.

OCTAVO: Con fecha 07/06/2023, el órgano instructor del procedimiento acordó la apertura de un período de pruebas, teniéndose por incorporados la reclamación

interpuesta por la parte reclamante y su documentación, así como las alegaciones al acuerdo de inicio del presente procedimiento sancionador presentadas por el AYUNTAMIENTO y la documentación que a ellas acompaña.

Asimismo, requirió al AYUNTAMIENTO que aportase información y/o documentación relativa a la Resolución de la información reservada abierta por Decreto ******DECRETO.1***, de 27/02/2022, por el que se incoa expediente de información reservada; así como, aclarar la discrepancia de fechas en cuanto a la fecha de incoación del expediente de información reservada, al no existir conformidad entre la fecha indicada en las alegaciones presentadas (27/02/2022) y la indicada en la respuesta al traslado de la reclamación (27/09/2022).

Con fecha 21/06/2023, el AYUNTAMIENTO presentó escrito de respuesta ante esta Agencia, en el que aporta:

- Documento número 1: copia de la Resolución de la información reservada abierta por Decreto ******DECRETO.1***, de 27/02/2022, por el que se incoa expediente de información reservada. Se firma con fecha 12/12/2022.

- Documento número 2: traducción del catalán al castellano de parte de la Resolución.

NOVENO: Con fecha 21/08/2023, por la Directora de la Agencia Española de Protección de Datos se acordó nombrar como instructor/a a D./Dña. ***E.E.E.***, en sustitución de D./Dña. ***F.F.F.***.

DÉCIMO: Con fecha 20/10/2023, el órgano instructor elaboró propuesta de resolución en la que se proponía sancionar con apercibimiento al AYUNTAMIENTO por las infracciones de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD.

La propuesta de resolución se notificó al AYUNTAMIENTO a través de medios electrónicos el 23/10/2023, como consta en el acuse de recibo que obra en el expediente. Transcurrido el plazo otorgado para la formulación de alegaciones, esta Agencia no ha recibido alegación alguna por el AYUNTAMIENTO.

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: En la reclamación se indica que, en fecha 22/05/2020, la parte reclamante presentó en la oficina de Correos cinco documentos con idéntico contenido dirigidos a cinco áreas distintas del AYUNTAMIENTO. El sello de entrada en el servicio de Correos es de ******FECHA.4***, mientras que en el AYUNTAMIENTO es de 26/05/2020.

SEGUNDO: En fecha ******FECHA.1***, se publica en el periódico "*****PERIÓDICO.1**" una noticia con el título ***"***TÍTULO.1"*** y el subtítulo ***"***SUBTÍTULO.1***". En el contenido de la publicación se detalla el nombre y apellidos de la parte reclamante, su condición de policía y parte del contenido de la documentación reseñada.

El artículo lo firma ***B.B.B.*** y ***C.C.C.***.

TERCERO: En fecha 04/06/2020, se publica en el periódico "******PERIÓDICO.1***" una noticia con el título *"*******TÍTULO.2****"*. En el contenido de la publicación aparece de nuevo el nombre y apellidos de la parte reclamante, así como parte del contenido de los documentos.

El artículo lo firma ***D.D.D.***.

CUARTO: En fecha 07/06/2020, se publica en el perfil de Twitter de ***B.B.B.*** (***XXXXXXX***) el siguiente mensaje:

*"*******MENSAJE.1****."*

Junto al mensaje aparece una fotografía en la que se aprecian varios documentos encima de un escritorio, en los que resultan legibles algunos datos personales de la parte reclamante, como su DNI, segundo apellido y domicilio a efectos de notificaciones.

QUINTO: El Anexo I que aporta el AYUNTAMIENTO junto al escrito de contestación al traslado lleva por título "Defensora Ciudadanía. Expediente ******EXPEDIENTE.1***", no está firmado e indica que es de 27/07/2020. En el contenido del documento se indica (traducción de esta Agencia del original en catalán):

"En conclusión, resulta absolutamente inadmisible que este tipo de documentos se filtren, que se publiquen en redes sociales y que se adjunten con enlace a la cuenta de twitter del ayuntamiento y de Policía Local sin que haya consecuencias que restablezcan o preserven los derechos de la ciudadanía. Hoy, 27.07.2020, aún sigue colgado.
No es, a nuestro juicio, una cuestión de libertad de expresión sino de incumplimiento en
la obligación de custodia de documentos y de vulneración de la protección de datos personales de la ciudadanía que genera indefensión patente.
Por todo ello, se considera oportuna la comunicación de los hechos al Área de Justicia Social, Feminismo y LGTBI, como primera implicada, y en el Gabinete de Batlia y en la Secretaría General del Pleno como responsables finales de la custodia documental, todo ello para el conocimiento y efectos, solicitando que se valore ejecución actuaciones para resolver situación y para establecer las medidas de disciplinarias y de seguridad que permitan garantizar la seguridad de la información y de los datos personales."

SEXTO: En el Anexo II, firmado el 26/09/2022, que aporta el AYUNTAMIENTO junto al escrito de contestación al traslado, se recoge la respuesta emitida por el Jefe de Servicio de Justicia Social, Feminismo y LGTBI sobre quién custodia la documentación y quién ha podido tener acceso desde que se registró en su Área.

SÉPTIMO: En el Anexo IV, sin fecha y sin firma, que acompaña a la contestación al traslado el AYUNTAMIENTO, denominado "Declaració en màteria de protecció de dades personals" (Declaración en materia de protección de datos personales), se

enumeran las funciones y obligaciones de los trabajadores del AYUNTAMIENTO en materia de protección de datos personales. En el inicio del citado documento se detalla (traducción de esta Agencia del original en catalán):

"DECÁLOGO DE LOS PUNTOS BÁSICOS.

1. Es necesario acceder con el nombre de usuario y contraseña habilitado por la entidad, y que lo identifica de forma personal, y no se permite en ningún caso su utilización compartida o la anotación en otro lugar que permita el acceso a otra persona.

2. Cualquier sistema o soporte de telecomunicaciones, informático o que la entidad ha puesto en la vuestra disposición para la realización de tareas profesionales no puede ser utilizado con ninguna finalidad personal o particular.

3. No se permite la descarga, la instalación o la incorporación de ningún programa o servicio informático por parte de los usuarios, para evitar vulnerar la normativa de protección de datos y los derechos de propiedad intelectual inherente a los mismos.

4. Hay que garantizar que solo las personas expresamente autorizadas puedan acceder a la información. Cada trabajador/a es responsable de no dejar documentos encima las mesas, a los estantes o en los espacios de tal manera que los puedan ver terceros. Se tiene que tener cuidado de no dejar documentación con información sensible a ubicaciones compartidas.

[…]

9. Se ha de cumplir escrupulosamente la normativa de protección de dato y la confidencialidad respecto de toda la información del Ayuntamiento. Se puede exigir responsabilidades que puedan derivar de la vulneración del secreto profesional por parte de los empleados.

[…]"

En el punto 1 del apartado "Funciones y obligaciones de los usuarios", se señala:

"1. El tratamiento de datos personales implica que la entidad debe aplicar las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, la disponibilidad y la integridad de los datos, cumpliendo las exigencias legales determinadas por la normativa de protección de datos.
Cabe recordar que la entidad es la responsable del tratamiento de los datos; que el titular es el único propietario; que, por tanto, la entidad no tiene una libre disposición sobre los datos, y que en muchas ocasiones la información de que se trata puede no ser objeto de protección por parte de la misma normativa porque no son datos personales, pero hay que garantizar su confidencialidad por cuestiones de propiedad intelectual o industrial, o por acuerdos contractuales.
Por estos motivos es necesario que cualquier usuario que realice un tratamiento de datos o de información confidencial cumpla de forma escrupulosa estas funciones y obligaciones, y advierta su responsable si detecta su incumplimiento."

En el punto 11 del citado documento, se indica:

"11. Incidencias y violaciones de seguridad.
Incidencia.
Se considera incidencia cualquier acto u omisión que tiene como consecuencia la destrucción accidental o voluntaria, licita o ilícita, la pérdida, la alteración, o el acceso o la comunicación no autorizados de cualquier tipo de información responsabilidad de la entidad, ya sea digital o analógica. (…)
Violación de seguridad.
Se considera una violación de seguridad cualquiera de las incidencias mencionadas anteriormente que tenga que ver con datos personales y represente un riesgo para las personas físicas. En términos generales y no excluyentes, se consideran violaciones de seguridad cualquiera de las siguientes situaciones:

- *Vulneración de la confidencialidad de los datos personales (enviar un correo a un destinatario no autorizado, perder un teléfono móvil, perder un expediente en papel, etc.).*
- *Alteración de la integridad de los datos personales (acción de un virus informático tipo criptolocker, cruce de datos erróneo, etc.).*
- *Pérdida de datos personales (tanto si son en papel como o en soporte informático).*

Cualquier incumplimiento de la normativa que establece este documento de seguridad y cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de la institución se considera una violación de seguridad. (…)"

En el punto 12 del citado documento, se detalla:

"12. Confidencialidad de la información y deber de secreto.
Cualquier incumplimiento de la normativa que establece este documento de seguridad y cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de la institución se considera una violación de seguridad.
Los usuarios de los sistemas de información o con acceso a cualquier dato o información deben guardar durante un tiempo indefinido la máxima reserva y no divulgar directamente ni a través de terceras personas o empresas, bajo su responsabilidad, datos, documentos, metodologías, claves, análisis, programas y de otra información a la que tengan acceso durante su relación laboral con la institución, tanto en soporte material como electrónico. Esta obligación continúa vigente después de que finalice la relación laboral con esta entidad.
Incumplir estas obligaciones puede constituir un delito de revelación de secretos (art. 197 del Código penal)."

OCTAVO: En fecha 12/12/2022, el AYUNTAMIENTO aprobó el Decreto núm. ******DECRETO.1*** en que se acordó lo siguiente:

"Primero. Archivar las actuaciones del expediente de información reservada sin otro trámite, de conformidad con el artículo 17.5 del Decreto 32/2020 de 5 de octubre, por el que se regula el régimen disciplinario de la función pública de la Administración de la Comunidad Autónoma de las Islas Baleares, dado que el informe del Instructor

concluye que no hay ningún indicio fundado de la comisión de una falta disciplinaria por parte de ninguna persona funcionaria concreta.

Segundo. Notificar este Decreto a la Señora ******INSTRUCTORA.1****, instructora de un expediente disciplinario del Área de Seguridad Ciutadana."*

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

De acuerdo con los poderes que el artículo 58.2 del RGPD, otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la 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 realiza, entre otros tratamientos, la recogida, registro y conservación de los siguientes datos personales de personas físicas: nombre y apellidos o documento de identidad, entre otros.

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.

Por su parte, el artículo 4 apartado 12 del RGPD define, de un modo amplio, la *"violación de la seguridad de los datos personales"* como *"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."*

En el presente caso, consta una violación de la seguridad de los datos personales en las circunstancias arriba indicadas, categorizada como de confidencialidad, al haberse producido un acceso indebido a datos personales tratados por el AYUNTAMIENTO por terceros no interesados. En este sentido, el GT29 entiende que se produce una violación de la confidencialidad cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

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 artículo 5.1.f) del RGPD Por su parte, la seguridad de los datos personales viene regulada en los artículos 32 del RGPD, que reglamenta la seguridad del tratamiento.

III
Alegaciones aducidas

Esta Agencia no tiene constancia de que el AYUNTAMIENTO haya presentado escrito de alegaciones contra la propuesta de resolución.

No obstante, como ya se indicó en la propuesta de resolución, respecto a las alegaciones presentadas por el AYUNTAMIENTO contra el acuerdo de inicio del presente procedimiento sancionador, se realizaron las siguientes consideraciones.

1. De la prescripción de la infracción del artículo 32 del RGPD.

Alega el AYUNTAMIENTO que la presunta infracción del artículo 32 del RGPD, calificada como grave, está prescrita al haber transcurrido 2 años entre los hechos denunciados (mayo/junio del 2020) y la presentación de la reclamación (julio del 2022).

Al respecto, esta Agencia desea recordar que el artículo 32 del RGPD se infringe cuando las medidas de seguridad detectadas no existen o son deficientes, con independencia de la petición realizada por la parte reclamante. Esto es, aunque la parte reclamante no hubiera presentado una reclamación ante esta Agencia, las medidas de seguridad del sujeto infractor serían, en sí mismas, inadecuadas.

Por tanto, el plazo de prescripción de la infracción del artículo 32 del RGPD, calificada como grave, no empieza a contar en el momento en que se produce la violación de seguridad, sino desde que las medidas de índole técnica y organizativa implementadas son apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Hasta que no se hayan adoptado y, por consiguiente, cesado en la ejecución de la conducta infractora, el plazo de prescripción no empieza a correr.

Tal y como señaló el AYUNTAMIENTO en su escrito de alegaciones al acuerdo de inicio, las medidas relativas al deber de fidelidad y secreto, de custodia y de seguridad de la información; se adoptaron con posterioridad a los hechos denunciados. En concreto, la publicación del Decálogo de funciones y obligaciones del personal municipal publicado en el Portal del Personal y en la Intranet, la realización de acciones formativas en materia de protección de datos; así como, la publicación de las correspondientes Actividades de Tratamientos, contratos de encargo entre responsables y encargados de tratamiento, contratos de confidencialidad, Reglamento orgánico del Pleno del Ayuntamiento advirtiendo del deber de confidencialidad de los Concejales, entre otros.

En relación con lo señalado es necesario poner de manifiesto que el AYUNTAMIENTO solo aporta prueba documental que acredita la adopción de la “Declaración en materia de protección de datos”. En este documento, tal y como consta en los hechos probados, se enumeran las obligaciones y deberes del personal del AYUNTAMIENTO

en relación con los sistemas de información o acceso a la misma a fin de garantizar el adecuado cumplimiento de la normativa de protección de datos personales.

Con respecto a las actuaciones de investigación realizadas por el AYUNTAMIENTO para el esclarecimiento de los hechos denunciados, esta Agencia desea señalar que el archivo del expediente de información reservada por falta de indicios no supone la inexistencia de infracción en materia de protección de datos personales. Pues, tal y como se desprende de la Resolución de 12/12/2022, la investigación no se centra en conocer si efectivamente se ha producido o no una filtración de los datos personales de la parte reclamante, sino en determinar qué persona empleada del AYUNTAMIENTO ha podido filtrar la información.

En consecuencia, no puede considerarse que el AYUNTAMIENTO, al momento de producirse los hechos denunciados, dispusiese de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo tal y como exige el artículo 32 del RGPD. Tales medidas, como bien ha reconocido la entidad, fueron implementadas en fechas posteriores a los hechos denunciados, no siendo correcta la fecha fijada por el AYUNTAMIENTO a efectos de iniciarse el plazo de prescripción.

Por todo lo expuesto, esta Agencia desestima esta alegación.

2. De la infracción del artículo 5.1.f) del RGPD.

El AYUNTAMIENTO alega que la presentación de varios escritos por la parte reclamante ante diversas áreas dificultó el control y preservación de su identidad, pero que, al tratarse únicamente de datos personales identificativos, los datos a los que se tiene acceso no requieren de una especial protección.

Al respecto, esta Agencia desea señalar que la normativa vigente en materia de protección de datos de carácter personal tiene por objeto garantizar una protección efectiva de los datos personales de toda persona física, sin perjuicio de que otorgue una especial protección a las categorías especiales de datos personales. Así pues, aunque el acceso indebido afecte al nombre, apellidos, DNI y domicilio a efectos de notificaciones de la parte reclamante, el AYUNTAMIENTO estaba obligado a ofrecer la debida confidencialidad por considerarse dato personal *"toda información sobre una persona física identificada o identificable"*, de acuerdo con el artículo 4.1 del RGPD.

Indica el AYUNTAMIENTO que fueron los medios de comunicación, en concreto, un periodista, quien difundió los datos personales de la parte reclamante mediante la publicación de un tweet con una fotografía en la que aparecía parte de la documentación presentada por esta; en ningún caso fue el AYUNTAMIENTO quien los divulgó.

Al respecto, esta Agencia desea mencionar la Sentencia del Tribunal de Justicia de la Unión Europea en el asunto Fashion ID, C-40/17, ECLI:EU:2018:1039, que establece en su apartado 74 que *"En cambio, y sin perjuicio de una eventual responsabilidad civil prevista en el Derecho nacional al respecto, dicha persona física o jurídica no puede ser considerada responsable, en el sentido de dicha disposición, de las operaciones anteriores o posteriores de la cadena de tratamiento respecto de las que no determine los fines ni los medios". Esto es,* cualquier operación de tratamiento que se reali-

ce en el ámbito del AYUNTAMIENTO debe imputarse solo a él, con independencia de operaciones de tratamiento que se hayan realizado previamente por otros sujetos y que, en ningún caso, le eximen de su responsabilidad.

Por todo lo anteriormente expuesto, se desestima la presente alegación.

IV
Seguridad del tratamiento

El artículo 32 del RGPD, *"Seguridad del tratamiento",* 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.

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".

En el presente supuesto, se pone de manifiesto la falta de medidas técnicas y organizativa apropiadas para garantizar un nivel de seguridad adecuado al riesgo

respecto de los datos personales. Esto es, que el AYUNTAMIENTO, al momento de producirse la violación de seguridad, no contaba con las debidas medidas.

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:

“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."

En este sentido, la búsqueda en internet, por ejemplo, del nombre, apellidos, DNI o dirección del afectado puede ofrecer resultados que, combinándolos con los accedidos por terceros, nos permitan el acceso a otras aplicaciones del afectado o la creación de perfiles de personalidad, que no tiene por qué haber sido consentida por su titular. La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, 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.

Los hechos conocidos son constitutivos de una infracción, imputable al AYUNTAMIENTO, por vulneración del artículo 32 del RGPD.

V

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de una de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"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;
b) *(…)"*

A este respecto, 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".*

A efectos del plazo de prescripción, el artículo 73 *"Infracciones consideradas graves"* de la LOPDGDD indica:

"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."

VI
Integridad y confidencialidad

El artículo 5.1.f) "Principios relativos al tratamiento" del RGPD establece:

"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 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".

En el presente caso, consta que un tercero ajeno ha tenido acceso a los datos personales de la parte reclamante contenidos en documentos que presentó en el Registro del AYUNTAMIENTO. Pues, el tweet publicado por el periodista en cuestión iba acompañado de una imagen que resulta ser una fotografía de una copia de uno de los cinco escritos presentados en dicho Registro en el que se visualiza (al ampliar la misma) el nombre, los apellidos, el DNI, la dirección del domicilio a efectos de notificación de la parte reclamante y los sellos de la Oficina de Correos, del Registro General de entrada en el Consistorio y del Área a la que va dirigida el escrito.

Todo lo expuesto demuestra, como se ha indicado en apartados anteriores, que el AYUNTAMIENTO no garantizó debidamente la confidencialidad e integridad de los datos personales de la parte reclamante.

Los hechos conocidos son constitutivos de una infracción, imputable al AYUNTAMIENTO, por vulneración del artículo 5.1.f) del RGPD.

VII
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de unas de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"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; (…)"

A este respecto, 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".

A efectos del plazo de prescripción, el artículo 72 *"Infracciones consideradas muy graves"* de la LOPDGDD indica:

"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. (…)"

VIII
Propuesta de sanción

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) 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."

Corresponde sancionar con un apercibimiento al AYUNTAMIENTO por las infracciones de los artículos 5.1.f) y 32 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: IMPONER a AYUNTAMIENTO DE PALMA**,** con NIF P0704000I, una sanción de apercibimiento por las infracciones de:

- Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

- Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE PALMA**,** con NIF P0704000I.

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.

938-250923

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