- **Expediente Nº: PS/00392/2020**

- **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, el reclamante), con fecha 22/06/2020 interpuso reclamación ante la Agencia Española de Protección de Datos. Los motivos en que basa la reclamación son que se ha realizado "*un tratamiento ilícito de datos personales, consistente en la captación inconsentida de mis datos personales de imagen y voz mediante grabación de vídeo y su posterior difusión masiva a través de redes sociales y medios de comunicación*". Explica que salió (…) el ***FECHA.1 "*cuando veo un coche rotulado de la policía (…) desde cuyo interior un agente me hace señales para que me acerque al coche*". Identifica varias divulgaciones del video en redes sociales, ***WEB.1 y ***DIARIO.1 en las que se puede ver el video.

Señala que se enteró porque a las pocas horas de haber sucedido (10,30), le avisaron amigos que el video se estaba difundiendo masivamente por redes sociales, considerando el reclamante que la captación la hizo el agente con "*su teléfono móvil*".

En ***WEB.1, referencia: "******REFERENCIA.1***" (…), perfil "******PERFIL.1***", ******FECHA.2***, de duración, 34 segundos. Aporta copia del CD en el que se visiona el video que coincide con el que figura en ***WEB.1 y relación de páginas y medios en los que se difundió el video.

Solicita que se inicie procedimiento sancionador contra quienes resulten infractores.

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5/12 de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), el 17/07/2020, se traslada la reclamación al AYUNTAMIENTO DE OVIEDO, (reclamado) con el literal:

Se recibe respuesta de 18/08/2020, manifestando que *"el 10/8/2020 y tras haber determinado al funcionario de ese Cuerpo que pudiera ser el origen de las grabaciones objeto de la denuncia, se le informó que se le remitiría copia de la reclamación presentada, dándole plazo hasta el día 13/8/20 para que emitiera informe al efecto".*

El 11/8/2020, el funcionario se personó en las dependencias de la Policía Local y se le entrega la documentación".

Concluye que el 14/8/2020, dicho funcionario manifestó que por indicación de su abogado y por el momento, no informará sobre la reclamación trasladada por la AEPD.

TERCERO: Con fecha 22/10/2020, la reclamación es admitida a trámite.

CUARTO: Con fecha 23/03/2021, la Directora de la AEPD acordó:

"*INICIAR PROCEDIMIENTO SANCIONADOR de apercibimiento a AYUNTAMIENTO DE OVIEDO, por las presuntas infracciones del artículo 32 y del artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27/04/2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo, RGPD); en relación con el artículo 5 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), conforme señala el artículo 83.4.a) y 83.5.a) del RGPD*."

QUINTO: Con fecha 13/04/2021, presenta alegaciones en las que manifiesta:

1-En el traslado de la reclamación no se aprecia que el Ayuntamiento figurara como denunciado por lo que se iniciaron diligencias para verificar la identificación del presunto autor de las grabaciones con su número de identificación profesional. Con ello, se entendía que se daba respuesta al escrito, y que serviría como base para apoyar la solicitud del reclamante en su deber de colaboración.

2- El reclamante por los hechos denunciados solicita cuantas actividades de investigación se consideren precisas. No les consta si se ha realizado alguna actuación de investigación adicional a la remitida por el Ayuntamiento.

Considera que se han conculcado los derechos y garantías de cualquier procedimiento sancionador reconocido en nuestro ordenamiento jurídico, puesto que la Agencia no ha realizado ninguna investigación para el esclarecimiento de los hechos y el reclamante no solicitaba iniciar actuaciones contra el reclamado al que no señala como presunto responsable. No existe una investigación mínima de los hechos antes del inicio del procedimiento sancionador, lo que supone que la carga de la prueba ha recaído en el reclamado, al que se pretende sancionar por unos hechos de los cuales no es responsable. "*Se desprende en los propios hechos contenidos en la reclamación que no ha sido el autor ni de las grabaciones ni de su difusión*". Tampoco el reclamado aparece relacionado con los medios en los que se difunden las imágenes, no es titular del medio o página en las que aparece.

3- Los hechos relacionados con la manifestación del reclamante de que las imágenes se graban desde el interior del vehículo policial han de tener en cuenta que el tratamiento de datos no es municipal, esos datos no se incluyen en ningún expediente administrativo ni se alojaron en sus sistemas, por lo que no se ha producido ninguna violación de las medidas de seguridad del reclamado.

4-No concurre culpabilidad en cuanto a que la conducta que se reprocha ha de ser antijuridica tipificada y culpable, consecuencia de acción u omisión imputable al presunto infractor, "*por malicia, imprudencia, negligencia o ignorancia inexcusable*".

Se está atribuyendo al Ayuntamiento la comisión de unos hechos por la mera circunstancia de que el presunto responsable sea un trabajador municipal que elude el principio básico del

régimen sancionador y también la propia normativa de Protección de Datos, al ser contraria a la definición de responsable del tratamiento contenido en el artículo 4 del Reglamento, pues las imágenes no las capta ni divulga el reclamado.

La asunción de responsabilidad por los hechos cometidos por un funcionario público en un acto de servicio no puede ser considerada como directa, sino subsidiaria. En caso de la existencia de un ilícito, tampoco es automática, sino que requiere un análisis de la situación. Sería preciso que el hecho sancionable se produjera en el desempeño de funciones propias de la policía utilizando de forma indebida su función pública con falta de la debida observancia y diligencia en el control de la actuación del empleado por parte de la administración, debiendo valorarse todas las circunstancias concurrentes de los hechos denunciados. Esta valoración de las circunstancias concurrentes ha sido obviada en el procedimiento.

5- El medio por el que se realizaron las grabaciones no procede de los sistema municipales, pues carecen de dispositivos móviles corporativos mediante los que puedan hacer grabaciones.
La presunta grabación y difusión de un apercibimiento verbal realizado por un agente a un ciudadano que es en lo que consiste la denuncia en este caso, se extralimita de las funciones propias de cualquier empleado municipal, máxime de un agente de la policía, ya que no existen instrucciones dictadas por los superiores ni por ningún responsable municipal que ordenen la captación y difusión de imágenes de personas detenidas o apercibidas como medio de prueba.

No existe un vínculo entre las funciones de la policía y la grabación y difusión de las imágenes ya que no existía la necesidad de realizar tales grabaciones para su incorporación a una diligencia o expediente administrativo, ni los agentes disponen de medios corporativos para poder captarlas.

6-El video continúa expuesto, si bien la AEPD dispone de un "*canal prioritario*" para comunicar la difusión de contenidos sensibles y solicitar su retirada, con una serie de mecanismos tendentes a su retirada, y en caso procedente, un sancionador contra las personas que hayan difundido dicho material.

7-Disponen de medidas de seguridad técnicas y organizativas de conformidad con el anexo dos del Esquema Nacional de Seguridad, y desarrolla un plan formativo para los empleados municipales que incluye material formativo online y de refuerzo con cursos de formación especializados en Protección de Datos.

8-Dado que no se considera responsable del tratamiento ni de la difusión de las imágenes ni de su grabación, "*no he podido incurrir en las infracciones imputadas*". Solicita el archivo del procedimiento.

SEXTO: Con fecha 14/04/2021, se decide practicar pruebas, incorporando la reclamación y la documentación obtenida del traslado así como las alegaciones al acuerdo de inicio.

Además, se solicita al reclamado que informe:

a) Si los Agentes tienen instrucciones por escrito o cualquier otro medio, sobre el uso de los datos personales de los ciudadanos, específicamente con el uso de dispositivos como los móviles personales, cuando se hallan en la vía pública prestando servicio, ¿cómo se les ha proporcionado esa información?

Se recibe respuesta el 6/05/2021, indicando haber recibido la petición de pruebas y manifestar que se trata de "*alegaciones*".

Pone de manifiesto que en las alegaciones al acuerdo de inicio de 14/04/2021 pedían que se investigaran los hechos, considerándolo como petición de pruebas y no se ha hecho, y que esas alegaciones no obtuvieron respuesta. No se le han trasladado las actuaciones de inspección de la AEPD que se dice en el acuerdo de prueba: se dan por reproducidos "*los documentos obtenidos y generados por los Servicios de Inspección ante el Ayuntamiento*", y desconocen si ese Servicio realizó averiguaciones, no pudiendo alegar ni solicitar prueba relacionado con ellos, pues se desconoce si se hizo tal inspección o que averiguaciones figuran.

Sobre lo solicitado, manifiesta que los empleados del Ayuntamiento disponen de información que puede verse en una página web del municipio, sobre el uso de dispositivos "*código telemático*", dentro del apartado de transparencia. El link ofrecido, al clicarse lleva a la página del reclamado pero no directamente a la información, dando error, desconociendo a nivel organizativo y de medidas de seguridad en materia de protección de datos que información y a través de que medios se da a los empleados, a los policías locales en concreto.

Además, señala, al grupo de Policía al que pertenece el presunto autor de las grabaciones se remitieron instrucciones sobre el uso de las imágenes en correo electrónico el 22/11/2017. Se adjunta copia del email remitido como correo electrónico con instrucciones sobre el uso de imágenes. Las instrucciones se refieren a una "*guía de uso de videocámaras móviles por las Fuerzas y Cuerpos de Seguridad*", que también se expuso en el tablón de órdenes del centro de trabajo junto con un informe de la Abogacía del Ayuntamiento sobre el uso de videocámaras privadas de funcionarios policiales como medio de defensa de denuncias. Acompaña los correos electrónicos, y se aprecia que originariamente parte de un sindicato policial que lleva el literal "*mirar el documento adjunto*", titulado "*guía de uso de videocámaras móviles por las fuerzas y cuerpos de seguridad*". A su vez, desde Jefatura Policía Local, se remite a diversas direcciones y personas, y el día 22/11/2017, se envía a diversos grupos de destinatarios de la policía.

a) Si existe alguna referencia tipificada en la normativa aplicable en el cumplimiento de la prestación del servicio, que pueda ajustarse al caso en el que un agente que capta presuntamente con su móvil particular a una persona desde el interior del vehículo policial, que luego además aparece en ***WEB.1, sin motivo, ¿que tipo de infracción podría ser.?

Manifiesta que el expediente está en fase de incoación y que a fecha actual no es posible identificar la infracción sin vulnerar los derechos del presunto autor de la grabación, procedimiento sancionador que se establece en la Ley Orgánica 4/ 2010 de 20/05, del régimen disciplinario del Cuerpo Nacional de Policía.

b) ¿Si esa entidad, sobre el presunto autor de la captación de las imágenes que luego se difundieron, ha iniciado actuaciones disciplinarias o de algún otro tipo, sea de oficio o por petición del afectado.?

Manifestó que: "*El Comité de Seguridad ENS del Ayuntamiento de Oviedo en reunión de 16 de abril del 2021 ha tomado acuerdo y enviado comunicado al Jefe de la Policía Local, instando la realización de actuaciones pertinentes de al menos la apertura de un expediente informativo al presunto autor de los hechos mientras la Agencia realiza las averiguaciones sobre los mismos que sean pertinentes para establecer la autoría*."

En la propuesta que aporta, se indica que se recibió el 6/08/2020 el traslado de la reclamación de la Agencia Española de Protección de Datos y se propone al policía local que se identifica, por la posibilidad de haber hecho un tratamiento ilícito de datos por medio del teléfono móvil y su posterior difusión captación inconsentida de datos personales de imagen y voz mediante grabación de video por medio del teléfono móvil y su posterior difusión.

Manifiesta que: "*Con fecha 3 de mayo del 2021 del Jefe de la Policía Local propuso incoación de expediente disciplinario al agente presuntamente implicado*". Si bien indica que se aporta copia, el documento que indica tiene 22 paginas, se corta en la página 9, pudiendo no haber anexado bien el documento.

Manifiesta que no queda constancia de la autoría de la difusión de la grabación ya que hasta la fecha el Ayuntamiento carece de información sobre quién difundió el video en las redes sociales requiriendo a la Agencia para que realice investigaciones oportunas.

Además solicita que se amplíe el plazo para la realización de la prueba hasta los límites máximos, a fin de que la Agencia pueda realizar averiguaciones pertinentes sobre los hechos.

Solicita que la Agencia investigue los hechos aportando pruebas suficientes de la autoría al menos de la difusión de los vídeos, remitiendo al Ayuntamiento el resultado de dichas investigaciones para que puedan ser aportadas como prueba en el procedimiento sancionador y en su caso en el expediente al presunto infractor exonerando al Ayuntamiento de la responsabilidad de la grabación y difusión del video.

SÉPTIMO: Con fecha 3/11/2021, se emite propuesta de resolución con el literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento a **AYUNTAMIENTO DE OVIEDO**, con NIF **P3304400I**, por las infracciones del RGPD de los artículos:*

- 32 del RGPD, de conformidad en el artículo 83.4.a) del RGPD,
- 5.1.f) del RGPD de conformidad en el artículo 83.5.a) del RGPD"

Frente a la propuesta, se reciben alegaciones el día 19/11/2021, en las que manifiesta:

– "*Incongruencia de la propuesta de Resolución con la reclamación presentada por el afectado que da lugar al inicio del expediente, contraviniendo el artículo 88 de la LPACAP. En la propuesta de Resolución solo se aborda la captación de la imagen, sin entrar a valorar la difusión que también forma parte del objeto de la reclamación con la publicación en redes sociales, internet o medios de comunicación de la imagen del reclamante*."

-"*El tratamiento de difusión no es tenido en cuenta ni se han realizado actuaciones para paralizar la publicación de las imágenes en los medios. Así, desde el 17 de julio de 2020,*

fecha de registro de la reclamación, a fecha de 15 de noviembre de 2021, el video del reclamante sigue publicado."

- "*Incumplimiento de los principios del procedimiento sancionador en la propuesta de sanción al Ayuntamiento. Atendiendo a que el daño al interesado no se produce tanto por la grabación sino por la difusión de las imágenes, es necesario reiterar que, entre los principios de la potestad sancionadora recogidos en la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, se encuentra el principio de necesidad en su artículo 29 en cuyo inciso 3 señala: "En la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá observar la debida idoneidad y necesidad de la sanción a imponer y su adecuación a la gravedad del hecho constitutivo de la infracción*".

-Reitera que:

- "N*o se considera responsable del tratamiento de las grabaciones que no son realizadas en el ejercicio de sus funciones. El Ayuntamiento no es el responsable ni de los fines - ajenos a las necesidades del desempeño del trabajo -, ni de los medios de captación - el dispositivo es propio del empleado- ni de los de difusión identificados por el reclamante*."

- "*La realización del video no es consecuencia ni de una acción ni omisión del Ayuntamiento de Oviedo. El Ayuntamiento no autoriza a los integrantes de la policía local a realizar grabaciones para otros fines diferentes al control de tráfico o la seguridad pública ni se trata de una actuación enmarcada en sus funciones profesionales*. *La derivación de la responsabilidad al Ayuntamiento por unos hechos que no ha cometido quiebra los principios básicos del procedimiento sancionador ya que, según la jurisprudencia, "[…] de lo contrario, se derrumbaría el fundamento del sistema punitivo, según el cual cada uno responde de sus propios actos, sin que quepa, con el fin de una más eficaz tutela de los intereses públicos, establecer responsabilidad alguna sancionable solidariamente por actos ajenos*".

- Ausencia de responsabilidad, sea por dolo o sea por culpa o falta de diligencia en el cumplimiento de obligaciones en materia de Protección de Datos.

-Consideran en cuanto a la manifestación de que han actuado con tardanza en la toma de medidas en concreto en la iniciación del procedimiento disciplinario contra el presunto responsable del video, que no ha sido así, ya que en fase de traslado de la reclamación comunicó a la Agencia la identidad de la persona que presuntamente había realizado las grabaciones y es la misma la única que tiene facultades y competencias para la investigación en materia de protección de datos, careciendo el Ayuntamiento de medios de prueba alguno contra el agente más allá del visionado de la imagen y la reclamación, procediendo a la colaboración con la Agencia.

Cuando el Ayuntamiento fue consciente que la AEPD no iba a realizar ninguna averiguación adicional "*inició los trámites para la apertura del procedimiento sancionador, indicando que en el mismo* "*se ha tomado declaración al presunto responsable*."

Aportan copia de un escrito de 30/04/2021, comunicado a personal de la "*propuesta de incoación de expediente disciplinario"* en el que se revela el inicio de las actuaciones de la AEPD que reciben el 6/08/2020 y "*visto el informe emitido por el Jefe de la Unidad de Gabinete técnico de 15/08/2020*" narrando los hechos del traslado de la reclamación al policía y la postura de este.

-Para justificar que dispone de medidas técnicas y organizativas en el tratamiento de datos aportan un ANEXO 1 sobre la formación impartida en seguridad y protección de datos desde mayo 2018, señalando que a las acciones presenciales han acudido mas de 500 empleados. A esto, deben sumarse las actividades que se realizan especialmente para la policía local, con formación presencial para un total de 30 efectivos, con cursos especializados sobre ciberseguridad, redes sociales o menores. Además, se impartió formación online abierta a cualquier empleado, incluyendo a la policía local. El ANEXO no indica cuantos miembros componen la policía local , ofreciendo el numero de empleados que han efectuado las acciones formativas a lo largo de las ediciones de las varias acciones en cada año. Otro cuadro diferente especifica las acciones formativas de la policía local , figurando en 2018, ocho personas, en 2019, una, en 2020 seis y en 2021, una.

HECHOS PROBADOS

PRIMERO: El reclamante reclama por el hecho de "*la captación inconsentida de mis datos personales de imagen y voz mediante grabación de vídeo*" y "*su posterior difusión masiva a través de redes sociales y medios de comunicación*". Explica que salió (…) el ***FECHA.1 y desde un coche de la Policía Local se le hicieron *señales para que me acerque"* al coche. Se puede ver el video, indica el reclamante en ***DIARIO.1, o "*en redes sociales como ***WEB.2, ***WEB.3, ***WEB.4, ***WEB.1",* según indica. En ***WEB.1, se aprecia que el video es realizado desde el interior del vehículo de la Policía Local, también lo pone de manifiesto en la reclamación el reclamante, en concreto desde asiento del copiloto. Se capta a la persona (…) desde enfrente, el reclamante. Conforme avanza hacia el lado izquierdo del vehículo, se mueve la toma que siempre le enfoca a él, y advertido, se para. El Agente de policía conductor del vehículo, que también es grabado de costado hablando a través de la ventanilla, (…) y el reclamante (…) de motu proprio se da la vuelta hacia su casa. Cuando se retira también es seguido en su alejamiento por la cámara. Se escucha perfectamente la conversación y se identifica plenamente al reclamante.

TERCERO: En el traslado de la reclamación el reclamado manifestó que había podido identificar al funcionario que pudiera ser origen de la grabación a quien le entrega el requerimiento, y que este declinó realizar manifestación alguna sobre el caso.

CUARTO: El reclamado, en la petición de pruebas iniciada el 14/04/2021 manifestó, con fecha 6/05/2021, que "*El Comité de Seguridad ENS del Ayuntamiento de Oviedo en reunión de 16 de abril del 2021",* "ha tomado acuerdo y enviado comunicado al Jefe de la Policía Local, instando la realización *de actuaciones pertinentes de al menos la apertura de un expediente informativo al presunto autor de los hechos*."

En ejecución de la medida, "*Con fecha 3 de mayo del 2021 del Jefe de la Policía Local propuso incoación de expediente disciplinario al agente presuntamente implicado*".

QUINTO: Solicitado en pruebas, si el reclamado, como responsable del tratamiento de los datos que realizan sus Agentes, ha dado a estos instrucciones sobre el uso de los datos personales de los ciudadanos, específicamente con el uso de dispositivos como los móviles personales, cuando se hallan en la vía pública prestando servicio, su respuesta fue que remitió el 22/11/2017 un documento titulado "*guía de uso de videocámaras móviles por las Fuerzas y Cuerpos de seguridad*", del que se ignora su contenido o responsable de edición y contenido. La guía procedía de un Sindicato policial dirigido a correos electrónicos de empleados y Policías del Ayuntamiento, que lo reenviaron a otros listados de correos por grupos/escalas de Policías. Se ignora su contenido, elaboración y en todo caso, su origen no procede del responsable imputado en este procedimiento, siendo un documento de además anterior a la entrada del RGPD, aplicable a partir de 25/05/2018.

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 arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

En cuanto a las alegaciones del reclamado sobre necesidad de practica de actuaciones de investigación, indicar que de ser obligatorias, habrían de haberse practicado antes del acuerdo de inicio, no en la fase de instrucción.

"Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas con objeto de determinar con carácter preliminar si concurren circunstancias que justifiquen tal iniciación (artículo 55 de la LPACAP). En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros."

Las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia y, en defecto de éstos, por la persona u órgano administrativo que se determine por el órgano competente para la iniciación o resolución del procedimiento.

Las actuaciones previas no constituyen una fase propiamente dicha del procedimiento administrativo sancionador ya que, tal y como hemos señalado, tienen por objeto determinar con carácter preliminar si concurren las circunstancias que justifiquen la iniciación del procedimiento.

La LOPDGDD sobre las actuaciones previas de investigación indica en el artículo 67:

"*1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo*

actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento"

Una vez en la fase de instrucción del procedimiento sancionador, resultan aplicables los principios generales del derecho penal con matices. Durante la fase de instrucción tienen lugar las actuaciones de comprobación de los hechos y alegaciones y finaliza la instrucción con la propuesta de resolución que fijará "*de forma motivada los hechos que se consideren probados" y su exacta calificación jurídica, se determinará la infracción que, en su caso, aquéllos constituyan, la persona o personas responsables y la sanción que se proponga, la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión"* (art 89.3 LPACAP).

Los hechos que motivan la incoación e imputación de responsabilidad al reclamado aparecen claros en el acuerdo de inicio. Estos hechos fueron conocidos por el reclamado a través del traslado de la reclamación. En ningún momento mencionaron la autoría del video expuesto sino la propia realización del video, como se deriva de que se ve en ***WEB.1 y que se capta desde dentro del vehículo las imágenes del reclamante.

En el periodo de pruebas de este procedimiento no resulta procedente tal como pide el reclamado que se investigue la autoría de la exposición del video, al que no se refieren los fundamentos del acuerdo de inicio, sino solo para autenticar que las imágenes se obtuvieron desde su interior.

III

Dentro de las definiciones, señala el RGPD:

Artículo 4:

1*) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

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

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

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;"

Se deriva del RGPD la distinción entre responsable del tratamiento y empleado de este, que tiene efectos de ser autorizado para tratar los datos personales bajo su autoridad y en su nombre. Los tratamientos de datos no se realizan únicamente por el responsable o el encargado del tratamiento, sino que el número de usuarios que tratan datos personales en cualquier Administración pública es equivalente al número de empleados públicos de la misma.

Con ello, se quiere significar, que tanto los cargos decisorios de responsabilidad cómo los empleados que actúan por cuenta del responsable del tratamiento, al llevar a cabo tratamientos de datos de carácter personal en el desempeño de sus funciones, en el seno de su estructura, se hallan en el círculo de poder de dirección y actuación de dicho responsable del tratamiento, también en lo que afecta a la implementación de su política de protección de datos (gobernanza de datos).

El RGPD o la LOPDGDD en ningún momento determinan que la responsabilidad en el tratamiento le pueda ser exigida al empleado o cargo, si que alude a las responsabilidades disciplinarias en el artículo 77 de la LOPDGDD que refiriéndose al tratamiento de datos de carácter personal por entidades públicas, precisa:

"*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"

La responsabilidad es exigible al responsable del tratamiento, con independencia de que traten los datos personales por sí mismo, decisión de su Director o cargo titular, como si la decisión la toma un empleado, máxime si se produce como en este caso, en el desarrollo de las funciones profesionales encomendadas.

IV

El artículo 5 del RGPD refiere los principios relativos al tratamiento de los datos personales, y en su número 2:"*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)", conocido como* "*compliance"* que podría equivaler a, no solo cumplimiento, normativo en este caso, sino también en prevención y responsabilidad de los miembros que integran sus organizaciones y el compromiso total de sus dirigentes, un mecanismo de aseguramiento de buen gobierno y cumplimiento normativo en materia de protección de datos.

El origen de esta medida de actuación, surge de exigir a las empresas implantar estos modelos de compliance para evitar la denominada *"autopuesta en peligro"* que pueda suponer que directivos o personas con apoderamientos expresos para realizar funciones, puedan encontrar facilidades para llevar a cabo conductas de falsedad en documentos mercantiles y estafas en concurso medial, incorporándose al Código Penal en su artículo 31 bis. Como modalidad de prevención, desplegando controles a priori eficaces y pudiendo suponer su Defecto de implementación efectiva infracciones normativas. De ahí surge la figura del "*compliance officer*" que se inserta en un órgano de supervisión y control que vele por el cumplimiento del plan de prevención; encargando a dicha persona, estos cometidos con autonomía e independencia. Dentro de este sistema se prevé el establecimiento de *un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezcan el modelo», como forma de* persuadir al cumplimiento del código ético y preventivo del delito por los empleados, y como expresión de una verdadera política de tolerancia cero ante la comisión de infracciones de relevancia penal, previendo medidas contra las personas que incumplen de manera grave el sistema de prevención de delitos

Con la Directiva 95/46/CE del Parlamento y del Consejo, de 24/10/1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos-y la consiguiente Ley Orgánica 15/1999, de 13/12 de protección de datos de carácter personal, el modelo de protección de los datos se basaba en un esquema "*estático*" de las medidas de seguridad a implantar, en función de la tipología de los datos tratados, se buscaba evitar la infracción de los derechos de los interesados como obligación principal.

Con el RGPD, se busca la anticipación a la infracción o lesión de derechos, el cumplimiento con antelación para evitar así la lesión o infracción del derecho o libertad del interesado. Si bien, el binomio RGPD/LOPDGDD no enumera específicamente cuáles sean esas medidas de seguridad a implantar, no se centra en la información perteneciente a la organización

(pública o privada), sino que se vincula especialmente a la protección de los datos de las personas físicas, exigiendo una responsabilidad proactiva, y no una responsabilidad reactiva, como sucedía en el modelo anterior. Este enfoque proactivo en la "*implementación permanente"* de las medidas de seguridad, implica que las mismas ya no son estáticas (como en el modelo anterior), sino dinámicas, correspondiendo al responsable de tratamiento determinar en cada momento cuáles de aquellas medidas de seguridad son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales , siendo el primer paso llevar a cabo un «*análisis de riesgos*».

Una vez evaluadas tales amenazas, el responsable podrá determinar cuáles son las medidas más apropiadas para mitigar o eliminar los riesgos para el tratamiento de datos que puedan surgir y afectar a los derechos y libertades de las personas físicas.

En consecuencia, se exige una responsabilidad proactiva, en lugar de la responsabilidad reactiva (enfoque basado en riesgos), debiéndose actuar con carácter preventivo, tener la diligencia debida para evitar tratamientos o incumplimientos no deseados en la protección de los intereses de los ciudadanos en el ámbito de su privacidad.

Es el responsable o encargado de tratamiento el que deberá acreditar dicha diligencia con un sistema de control interno sólido y eficaz. Por ello, no será suficiente la mera demostración formal de cumplimiento, sino que este principio exige una actitud previa, consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

La obligatoriedad de estas medidas, o el modo en que se apliquen, dependerá de factores que habrá que tener en cuenta en cada caso, como el tipo de tratamiento y el riesgo que dicho tratamiento implica para los derechos y libertades de los interesados. En consecuencia, la diligencia debida, debe adecuarse al nivel de riesgos en la protección de los datos y las características de la organización.

Se puede definir el concepto de diligencia debida como "*la medida de prudencia, actividad o asiduidad que cabe razonablemente esperar, y con la que normalmente actúa, una organización prudente y razonablemente en unas circunstancias determinadas; no se mide por una norma absoluta, sino dependiendo de los hechos relativos del caso en cuestión*". Por ello, la diligencia debida es un proceso en continua observación y prevención de los efectos negativos de las actividades de las entidades sobre la protección de datos.

La diligencia debida en materia de protección de datos:

-Debe abarcar las posibles consecuencias negativas sobre la protección de datos que la empresa pudiera provocar o contribuir a provocar a través de sus propias actividades u omisiones, que guarden relación directa con sus operaciones, productos o servicios prestados.

-Variará de complejidad en función del tamaño de la organización, el riesgo de graves consecuencias negativas sobre la protección de datos y la naturaleza y el contexto de sus operaciones.

- Debe ser un proceso continuo, ya que los riesgos pueden cambiar con el tiempo, en función de la evolución de las operaciones y el contexto operacional de las organizaciones.

En consecuencia, la diligencia debida se compone de cuatro elementos: identificar, prevenir, mitigar y la rendición de cuentas, es decir:

1. Una evaluación del impacto real y potencial de las actividades sobre los datos (evaluación de riesgos).

2. La integración de las conclusiones, y la actuación al respecto (los controles).

3. El seguimiento y monitoreo (evaluación del desempeño).

4. La comunicación de la forma en que se hace frente a las consecuencias negativas (rendición de cuentas).

La diligencia debida proporciona una defensa contra la responsabilidad, permite una reducción de las sanciones o brinda un recurso de defensa cuando la empresa puede probar que había implementado los "*procedimientos adecuados» para prevenir un impacto*."

Para poder acreditar diligencia debida, la entidad debe demostrar que ha dado todos los pasos razonables y llevado a cabo las acciones necesarias para evitar que se genere un impacto negativo. Ello se interpretará dependiendo de las circunstancias concretas de cada caso.

El Reglamento pretende que se anticipe el momento en que el responsable o encargado del tratamiento actúe con diligencia debida, mediante este principio de responsabilidad proactiva, gestionando los riesgos mediante un sistema de control interno sólido, que permita acreditar esta actuación diligente con carácter previo, lo cual inicialmente, pueda presentar cierta incertidumbre en su aplicación, debido al paso de un sistema cerrado, basado en una enumeración específica de las medidas de seguridad a implantar en función de la tipología de datos tratados, a un sistema abierto, cuyo objetivo es la aplicación de las medidas técnicas y organizativas "*apropiadas*" para garantizar y poder demostrar que el tratamiento es adecuado conforme al ámbito, el contexto y los fines del tratamiento.

Para el cumplimiento del principio de "*Responsabilidad Proactiva"* el responsable y encargado de tratamiento deberán previamente realizar un análisis y estudio del cumplimiento en materia de protección de datos basado en el riesgo. Es decir, deberán analizar qué medidas de protección de datos son necesarias implantar para garantizar el cumplimiento del Reglamento, en función de naturaleza, alcance, contexto y finalidades del tratamiento de datos que realicen, así como de los riesgos (probabilidad y consecuencia) de intromisión en los derechos y libertades de los interesados.

De esta manera cuanto más probable y mayores sean las consecuencias del riesgo del tratamiento, más medidas u de mayor calado deberán ser las necesarias a implantar para contrarrestarlas (conviene aclarar que no se trata únicamente de medidas de seguridad técnica).

El enfoque basado en el riesgo se configura como un factor clave dentro del proceso de adecuación o cumplimiento de la normativa de protección de datos, ya que todo responsable o encargado deberán previamente analizar el nivel de riesgo en el que se encuentra los tratamientos. Como consecuencia, el RGPD implanta la obligación de los responsables y encargados de implantar un sistema interno de cumplimiento en materia de protección de datos. Sistema que estará integrado por distintas políticas o procesos internos de privacidad que deberán ser actualizados y auditados periódicamente de manera que permitan demostrar el cumplimiento del Reglamento.

La Ley 40/2015, de 1/10 de Ley de Régimen Jurídico del Sector Público, señala en su artículo 28.4:

"*Las leyes reguladoras de los distintos regímenes sancionadores podrán tipificar como infracción el incumplimiento de la obligación de prevenir la comisión de infracciones administrativas por quienes se hallen sujetos a una relación de dependencia o vinculación. Asimismo, podrán prever los supuestos en que determinadas personas responderán del pago de las sanciones pecuniarias impuestas a quienes de ellas dependan o estén vinculadas*."

V

Por la grabación de los datos personales del reclamante plasmados en las imágenes del video que se ha identificado previamente, se imputa al Ayuntamiento de Oviedo la infracción del artículo 32 del RGPD, que indica:

"*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.

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 relación a adoptar las correspondientes medidas de seguridad, el RGPD busca aprovechar las ventajas que ofrece la gestión de riesgos, pero introduce una nueva visión, donde el foco de atención no se centra en las amenazas que se ciernen sobre la compañía, centrando su atención en las amenazas sobre los derechos y libertades de los interesados. La evaluación de los riesgos debe ser el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen sobre los interesados. Se trata de establecer hasta qué punto una actividad de tratamiento, por sus características, el tipo de datos a los que se refiere o el tipo de operaciones puede causar un daño a los interesados. Este enfoque implica estimar el daño y la tipología de daño que se puede producir sobre los interesados, por ejemplo, un daño material derivado de la vulneración de sus derechos y libertades, o a su intimidad. Por lo tanto, y antes de la adopción de las citadas medidas se debe proceder a valorar el riesgo inherente a los tratamientos.

El Considerando 74 del RGPD dice que indica: *"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas."* (El subrayado es de la AEPD).

Cualquiera de esos empleados puede realizar un tratamiento de los datos que no sea conforme con la normativa de protección de datos personales, sea a través de los medios proporcionados o de otros, por lo que la formación en materia de privacidad debe ser integral para la práctica totalidad de miembros de la organización.

El responsable debe establecer información y formación de sus empleados en la materias, directrices y difusión de la información sobre tratamientos de datos, de modo que se consiga una aplicación uniforme en su ámbito.

Así y todo, los empleados, y cargos directivos deben considerar antes de proceder a un tratamiento de datos, especialmente si es distinto del habitual, o novedoso, por interpretación o por situación concreta, llevar a cabo antes una consulta al responsable del tratamiento. Este deberá emitir normas a sus empleados y centros directivos para coordinar aspectos básicos de los tratamientos de datos.

Aparte del conocimiento que se ha de proporcionar y se presupone a los policías sobre la captación de imágenes en vías públicas por las Fuerzas y Cuerpos de Seguridad, que se rige por su legislación específica, constituida por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en

lugares públicos, lógicamente se debería haber informado y previsto las consecuencias del uso de dispositivos móviles personales. Sobre estos, salvo el uso que se pueda hacer de los denominados institucionales para el ejercicio de las funciones en los supuestos en que puedan ser precisos, se debe indicar que, su uso, como cámaras o móviles personales de los agentes para captación de imágenes en el desarrollo de la labor profesional, no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía deben adoptarse por los responsables del tratamiento, debiendo acomodar y prever concretas responsabilidades y sanciones en su caso. En este caso, se acredita que no existen tales medidas que han supuesto una intromisión no legítima en el derecho de protección de datos del reclamante.

En este caso, no se acredita que el reclamado dispusiera de medidas implantadas sobre uso de dispositivos personales en relación con la realización de sus tareas, donde advirtiera de su régimen de uso y sanción, o la no necesidad ni proporcionalidad de grabación de imágenes como la que ha sido objeto de esta reclamación. El régimen de diligencia en el cumplimiento de los principios del tratamiento de datos se relaciona con la adopción de estos protocolos, considerando que se pueden afectar derechos de los ciudadanos. Se acredita la infracción de este artículo.

Por lo demás, el inicio del proceso disciplinario, que es solo una parte de la política de cumplimiento normativo en la organización, se revela tardía, y reactiva, pues ha sido con ocasión de la practica de pruebas, cuando se acredita que no existe especificidad relativa a las medidas de seguridad en el desarrollo de las tareas encomendadas en función con los riesgos y dispositivos.

VI

El autor del video que se visiona en ***WEB.1 presta servicios para el reclamado, y se imputa al AYUNTAMIENTO DE OVIEDO la infracción de artículo 5.1.f) del RGPD:

"*Los datos personales serán:*

"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»)."

La LOPDGDD señala en su artículo 5:

"*1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679"*

No se habla aquí del autor de la difusión del video que figura en ***WEB.1, sino de algo previo sin cuyo registro no hubiera sido posible y de datos que han escapado del control de sus autores. Este procedimiento es sobre el tratamiento derivado de la recogida de imágenes tomadas, sin lugar a dudas desde el interior del vehículo, que coincide con el video expuesto, según se desprende de la misma visión del video. Captación deliberada y clara que recoge los datos personales del reclamante, se le puede identificar y ubicar en la vía pública. Esta

imagen solo tiene un origen que es el de los agentes que en ese momento hablan con el reclamante. Se aprecia que se recoge la imagen total del agente sentado en el asiento conductor del vehículo parado y este es el que le habla al reclamante. La imagen tuvo que ser captada por su acompañante, dado el ángulo de las imágenes que recaba. La recogida de la imagen es la que luego posibilita que circule en ***WEB.1 y en otras redes sociales.

VI

El artículo 83.4 a) del RGPD indica: "*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:*

"Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

A efectos de prescripción, la infracción del artículo 32 se contiene en el artículo 73 f) de la LO-PDGDD, que determina:

"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:

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."

Mientras que el artículo 83.5 a) del RGPD indica:

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

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

A efectos de prescripción, la infracción del artículo 5.1.f) se contiene en el artículo 72. 1.a) de la LOPDGDD, que determina:

"*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:*

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

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

b)dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

El reclamado no adopta o prevé adoptar alguna media que tienda a mitigar hechos como los examinados.

El artículo 29.3 de la Ley 40/2015, de Régimen Jurídico del Sector Público, en orden a la graduación de las sanciones dispone: "*En la determinación normativa del régimen sancionador, así como en la imposición de sanciones se deberá observar la debida idoneidad y necesidad de la sanción a imponer y su adecuación a la gravedad del hecho constitutivo de la infracción. La graduación de la sanción considerará especialmente los siguientes criterios: a) El grado de culpabilidad o la existencia de intencionalidad. b) La continuidad o persistencia en la conducta infractora. c) La naturaleza de los perjuicios causados. d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa."*

Aplicable a ambas infracciones, en este caso por ser el presunto infractor una entidad local, el artículo 83.7 del RGPD indica:

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*"

El ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6. de la LOPDDGG: "*1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*

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

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

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."

Por lo tanto, de acuerdo con la legislación aplicable
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **AYUNTAMIENTO DE OVIEDO**, con NIF ***P3304400I***, por una infracción de los aartículos 32 y 5.1.f) del RGPD, de conformidad con los artículos 83.4.a) y 83.5.a) una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a **AYUNTAMIENTO DE OVIEDO**.

TERCERO: De acuerdo con el artículo 58.2.d) del RGPD: "*cada autoridad de control podrá ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado*…" se conmina a la reclamada a que introduzca en función de los riesgos de tratamiento derivados de la actuación policial y los derechos afectados, las medidas apropiadas para el tratamiento de datos con dispositivos como política de personal en el desempeño de las funciones, otorgándole dos meses para informar de las mismas llevadas a cabo.

CUARTO: COMUNICAR la presente resolución al DEFENSOR DEL PUEBLO, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia

Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-26102021

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