- **Expediente N.º: EXP202202155**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ******SINDICATO.1*** (en adelante, la parte reclamante), con fecha 14/12/2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la entidad AYUNTAMIENTO DE GIJÓN, con NIF ***P3302400A*** (en adelante, la parte reclamada o AYUNTAMIENTO o AYUNTAMIENTO DE GIJÓN), y dentro del AYUNTAMIENTO contra quien corresponda en la Concejalía de Seguridad Ciudadana, Policía Local y Alcaldía, así como contra cualquier persona interviniente en los hechos (menciona un funcionario en concreto). Los motivos en que basa la reclamación son los siguientes:

Presenta reclamación por la filtración y difusión a través de WhatsApp y redes sociales de un escrito presentado en el Registro Electrónico del AYUNTAMIENTO DE GIJÓN, en fecha 20/01/2021, mediante el que informaba sobre la posible comisión de una infracción del régimen disciplinario de la Policía Local.

Añade que el 19/02/2021 presentó ante el mismo Ayuntamiento un nuevo escrito para comunicar aquella difusión ilícita del documento de 20/01/2021, instando a investigar la brecha de seguridad y a la depuración de responsabilidades.

Según la parte reclamante, en respuesta al escrito anterior, mediante resolución de 30/08/2021, la parte reclamada reconoce accesos indebidos al asiento registral y la filtración y difusión del mismo, así como tratamientos tales como el acceso habitual, general o indiscriminado a las anotaciones del registro de entrada, que no guardan relación con la base de licitud y finalidades contenidas en el inventario de actividades; y resuelve únicamente la adopción de una serie de medidas de cara al futuro (*"implementando todo ello, especialmente en lo relativo a la Policía Local"*).

Asimismo, advierte la parte reclamante que no consta que el AYUNTAMIENTO DE GIJÓN haya notificado la brecha de seguridad a esta Agencia o a los afectados, ni que haya adoptado medida alguna, *"y ello pese a la gravedad del asunto, dado que afecta a los ciudadanos en general y a los sindicatos en particular, pues se reconoce que se controla la actividad sindical…".*

Considera que la parte reclamada no ha garantizado la confidencialidad, ha vulnerado el deber de secreto y las normas sobre comunicaciones de quiebras de seguridad.

Junto a la reclamación aporta los escritos presentados por la parte reclamante ante la parte reclamada y la contestación emitida por ésta:

a) Escrito presentado por la parte reclamante en el Registro Electrónico del

AYUNTAMIENTO el día 20/01/2021, informando sobre una posible infracción del régimen disciplinario de la Policía Local. En este escrito, además de las circunstancias de hecho que a juicio de la parte reclamante determinan la posible infracción disciplinaria, constan los datos relativos a nombre y apellidos del posible infractor y los datos del representante de la parte reclamante relativos a nombre, apellidos, DNI y puesto que ocupa en la organización de la parte reclamante.

b) Escrito presentado en el Registro Electrónico de la parte reclamada el día 19/02/2021 denunciando una filtración/difusión del escrito reseñado en el apartado a) anterior.

En el punto tercero de este escrito, la parte reclamante señala que "*Hemos tenido conocimiento que, el citado documento se está difundiendo por la plataforma de Whatsapp, a través de varios grupos (…)*.

En este escrito, la parte reclamante solicita que *"se realicen las averiguaciones oportunas de la brecha de seguridad ocurrida en los departamentos que debían custodiar el documento antedicho. A su vez, se comprueben los accesos ilegítimos al escrito así como a las personas que lo difundieron, depurando las responsabilidades oportunas*".

c) Notificación de fecha 30/08/2021 por la que se da traslado al representante de la parte reclamante de la resolución dictada en la misma fecha por el AYUNTAMIENTO DE GIJÓN (Resolución de la Alcaldía) en relación con la denuncia de fecha 19/02/2021, reseñada en el apartado b) anterior.

En sus puntos tercero y cuarto de los Antecedentes de Hecho se hace referencia al contenido del informe emitido al respecto por el Servicio de Sistemas de Información:

"Todas las personas del Servicio de Relaciones Ciudadanas tienen acceso al Registro General para poder despachar las solicitudes de entrada hacia las unidades responsables de su tramitación, acceso indispensable para poder cumplir con su cometido.
En el momento en el que un documento entra en la organización a través del Registro, es posible seguir una traza del uso del mismo a través de las aplicaciones corporativas, pero si el documento se extrae (para enviarlo por otros medios electrónicos o se imprime), ya no es posible hacer un seguimiento del mismo.
Por otra parte, también se ha comprobado a través del sistema de gestión de impresión, si se ha impreso un documento con un nombre igual o parecido al documento original con un resultado negativo".

En el punto cuarto se indica lo siguiente:

"Del mencionado informe se deducen una serie de accesos de personal municipal al asiento registral indicado, que, por su presunto conocimiento y supuesta difusión, es citado sucesivamente tal y como consta en el referido expediente, poniendo de manifiesto los comparecientes –(…)-, en lo que interesa a los efectos de esclarecimiento de hechos y demás circunstancias concurrentes, que accedieron a dicha anotación de entrada por distintos motivos, y según cada declarante, debido a:

- Que se tiene permiso de acceso remoto desde el puesto de trabajo al módulo de comunes del libro general del registro de entrada de documentos del Ayuntamiento.

- Que se trata de accesos justificados para el desempeño ordinario de las tareas de los puestos de trabajo o porque habitualmente se revisan todas las anotaciones del registro

de entrada del Ayuntamiento; (…), con la finalidad de conocer asuntos sindicales y laborales que les puedan afectar en su condición de afiliados y parte interesada.

En cuanto a la forma de acceso, los declarantes manifestaron que disponen de cuenta de usuario -salvo un caso, que además carecía de equipo informático a su disposición-, con contraseña propia y no compartida, para el acceso a las aplicaciones informáticas de registro de entrada y de gestor de expedientes; si bien, se ha detectado que en dos puestos de trabajo se hace uso compartido con otro personal, lo que justificaría que en la auditoría de accesos conste su perfil de usuario pero afirmen no haber hecho personalmente tal acción. En general, a ninguno les consta que se haya producido algún incidente en relación a una posible suplantación de identidad o de los permisos de acceso de sus cuentas.

En relación al conocimiento directo del contenido de dicho documento objeto de reclamación, bien se niega o se atribuye a un simple error de acceso al asiento de entrada la constancia de su perfil en el registro de auditoría.

*Sin embargo, se afirma haber tenido conocimiento indirecto, bien verbalmente o a través de un grupo de whatsapp llamado "*****GRUPO.1**" -aunque un declarante niega que se haya publicado en esta red nada al respecto-, la cual, según su administrador-…* (se indica nombre y apellidos), ***(…)***- *es de carácter lúdico, tiene un total de 81 miembros, (…), y sobre la cual no "hace ningún control de lo que se publica", tampoco la lee ni participa y "elimina los mensajes que recibe".*

*Respecto a la difusión del documento en cuestión, se niega por los comparecientes haberla realizado; únicamente en un caso se ha afirmado que fue impreso el texto a petición de superior –*****PUESTO.1**-, a quien fue entregado; en otro, se manifiesta haber difundido la noticia de la presentación en el registro en otro grupo de whatsapp *****GRUPO.2**.*

Por último, en cuanto a las consecuencias de tal difusión, o no se tiene constancia, o se conoce una recogida de firmas en apoyo de la persona a quien se hacía alusión directa en el reiterado escrito de 21 de enero, para su retirada o presentación a título individual, (…), o bien para "hacer una asamblea general".

Por otra parte, en el punto quinto de los mismos Antecedentes de Hecho se detalla la información aportada a las investigaciones por el representante de la parte reclamante:

"Es reseñable que, en atención a los resultados alcanzados en la instrucción del expediente, se requirió al denunciante para que concretara algunas circunstancias de los hechos investigados, relatando éste en su comparecencia que, respecto al documento registrado el 20 de enero de 2021, tuvo un primer conocimiento de su filtración el 14 de febrero de 2021, cuando recibió un mensaje a su whatsapp personal (…), que identifica como… (se indica nombre y apellidos), donde éste "manifiesta su enfado por la presentación del citado documento, a lo cual suma insultos y amenazas", aportando captura de pantalla como prueba de ello.

*Asimismo, el reclamante presentó evidencia de la difusión del documento señalado en el grupo de whatsapp -el indicado "*****GRUPO.2**"- que tiene con los compañeros de su turno de trabajo (…),administrado por… (se indica nombre y apellidos), y donde "uno de los integrantes… (se indica nombre y apellidos) tras la eliminación de varios mensajes escritos y eliminados aporto a la conversación el documento íntegro en pdf siendo las 22;16" y que "se puede observar que el documento aportado es un reenvío".*

Al respecto de esto último, cabe indicar que el aludido… (se indican iniciales del nombre y primer apellido)*, en declaración tomada de fecha posterior, manifiesta que tuvo conocimiento del objeto del presente expediente en el grupo de "*****GRUPO.1**" y "que recuerda que en ese grupo pusieron un mensaje diciendo que había presentado el compañero…* (se indica el nombre) *por registro una reclamación de que le habían insultado o puesto un mote en un pase de lista en el que él no estaba presente. Y que la noticia que vio en ese grupo lo pasó a otro grupo llamado "*****GRUPO.2**", no recordando que fuese un documento, preguntando sólo si sabían algo de eso y nada más".*

*Por otra parte, siguiendo con el testimonio del denunciante, en este grupo de mensajería "*****GRUPO.2**", afirmó también que, como acredita, "había podido acceder a una captura de conversación de whatsapp proveniente del grupo de "*****GRUPO.1**". La hora de la captura son*

las 20:00 hasta las 20:05".
Igualmente, añade que, ese día indicado de 14 de febrero, recibió (…) "un reenvió de la conversación con… (se indica nombre y apellidos), donde se visualiza el pdf acompañado de la frase "yo no te pasé nada" y solicitando apoyo o ayuda para que se retire el citado escrito de 20 de enero de 2021": aporta justificación documental de captura de pantalla donde "en la imagen de la conversación se aprecia que el documento pdf procede de un reenvío nuevamente".
Finalmente, también señala la antedicha "recogida de firmas organizada (…)", presentando el documento que ha recibido con las mismas "donde se solicita la retirada del escrito presentado".
Lo anterior, también conocido por (…)… (se indican iniciales del nombre y primer apellido), es ratificado por éste en distinta declaración practicada, aportando también evidencia de la actuación de (se indica nombre y primer apellido) el 14 de febrero, "donde en tono amenazante y en plural, da un ultimátum para retirar el escrito presentado el 20 de enero de 2021".

Y en el punto quinto de los Fundamentos de Derecho, en cuanto a la licitud del tratamiento de los datos (artículo 6.1, letras c) y e), del RGPD), se dice:

"De ello, cabe concluir que alguno de los tratamientos expresados en los Antecedentes, como el acceso habitual, general o indiscriminado a las anotaciones del registro de entrada o para ejercicio de supuestos derechos sindicales, no guarda relación con la base de licitud y finalidades contenidas en el mencionado inventario de actividades".

Por último, en el punto sexto de los Fundamentos de Derecho de la citada resolución se mencionan las medidas que se han tomado en relación con las causas que han motivado el incidente de seguridad:

"En relación con las causas que han motivado el incidente de seguridad, se han tomado las siguientes medidas, según consta en el señalado al comienzo informe del Servicio de Sistemas de Información:

> *En la configuración de las cuentas de usuario de las aplicaciones: para las cuentas de usuario implicadas en el incidente de seguridad, se han eliminado permisos asociados que ya no deberían de estar por haber cambiado la persona de lugar de trabajo o de funciones.*
>
> *En la configuración de acceso al Registro General: se ha desactivado la posibilidad de consultar los documentos asociados a todos los registros de entrada del libro general de entrada del Ayuntamiento. Esta opción de consulta estaba asociada a un número importante de personas, que lo habían solicitado desde el año 2015 hasta la actualidad y que era necesario para poder trabajar de forma correcta con los expedientes de su competencia.*

Al respecto, no consta que la medida de limitación de accesos generalizados al módulo de comunes del registro de entradas haya afectado al desempeño de las tareas habituales de los puestos de trabajo objeto de investigación".

De acuerdo con los Antecedentes y Fundamentos expresados, se resuelve adoptar las siguientes medidas, entre otras:

. Medidas técnicas y organizativas complementarias y de regulación que sean procedentes, para minimizar la posibilidad de que se reproduzcan incidentes similares, en cuanto a la forma de altas, bajas y movilidad del personal municipal en la asignación de cuentas, permisos o autorizaciones de acceso, revocación o desactivación de aplicaciones y recursos informáticos y electrónicos, en atención a las funciones y tareas que efectivamente desempeñen en sus puestos de trabajo en la organización.

. Medidas reguladoras, técnicas y formativas que resulten adecuadas acerca de la existencia, creación y utilización de grupos de mensajería, redes sociales o de comunicación internas del personal municipal.
. Dar traslado al Servicio de Gestión de Personas para poner en su conocimiento los hechos descritos en los Antecedentes, por si fueran constitutivos de infracción disciplinaria, o precisasen de diligencias previas de investigación adicionales.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

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), fue recogido en fecha 25/02/2022 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 14/03/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

En respuesta al requerimiento que le fue efectuado por los Servicios de Inspección de la AEPD, la parte reclamada aportó la información y documentación siguiente:

1. Declara reproducida la resolución de la Alcaldía de 30/08/2021, ya aportada por la parte reclamante y cuyo contenido consta reseñado en el Antecedente Primero.

2. Aporta copia del informe elaborado por el Servicio de Sistemas de Información, de fecha 10/03/2021, con el detalle de las causas que motivaron la incidencia que originó la reclamación. Del contenido de este informe cabe destacar lo siguiente:

"En relación con las causas que han motivado el incidente de seguridad, se han tomado las siguientes medidas:

1. En la configuración de las cuentas de usuario de las aplicaciones: para las cuentas de usuario implicadas en el incidente de seguridad, se han eliminado permisos asociados que ya no deberían de estar por haber cambiado la persona de lugar de trabajo o de funciones.

2. En la configuración de acceso al Registro General: se ha desactivado la posibilidad de consultar los documentos asociados a todos los registros de entrada del libro general de entrada del Ayuntamiento. Esta opción de consulta estaba asociada a un número

importante de personas, que lo habían solicitado desde el año 2015 hasta la actualidad y que era necesario para poder trabajar de forma correcta con los expedientes de su competencia.

Para minimizar la posibilidad de que se reproduzcan incidentes similares en el futuro, se proponen además que se tomen las siguientes medidas organizativas:

1. Establecer un protocolo de alta de personas en la organización, recogiendo de forma precisa los accesos y recursos técnicos y autorizaciones que hay que asignarles.

2. Establecer un protocolo de baja de personas, que contemple todas las medidas a adoptar: desactivación de cuenta de usuario, buzones de correo, revocación de certificados electrónicos, etc.

3. Establecer un protocolo de modificación de personas por cambio de puesto o de funciones, en el que se recoja de forma precisa las actuaciones a realizar con sus cuentas de usuario, permisos de acceso a recursos informáticos, etc. También debe de recogerse como responder a las peticiones de permisos que se realizan de manera informal por los propios implicados o sus superiores".

3. Se aporta *"la relación de empleados que tuvieron acceso al documento difundido en el espacio temporal que medió entre el 20 de enero de 2021 y el 14 de febrero posterior, facilitada por el Servicio de Sistemas de la Información"*. En esta relación se detalla el DNI de las personas que accedieron al documento, nombre, apellidos, y departamento al que pertenecen (**…**).

4. Sobre la implantación de las medidas acordadas en la resolución de la Alcaldía de 30/08/2021 se informa que se ha previsto la contratación de una prestadora de servicios externa para la ejecución de aquellas medidas y que se encuentra en proceso de elaboración una Instrucción de la Alcaldía reguladora del acceso y autorización de uso de los sistemas de información municipales.

Añade que se han realizado acciones formativas sobre medidas de seguridad y que no consta que se hayan realizado acciones disciplinarias en relación con los hechos denunciados.

5. No constan análisis de riesgos ni evaluaciones de impacto.

6. Aporta copia del Registro de Actividad de Tratamientos relativo al Registro General. En los apartados *"Categoría de destinatarios de la información"* y *"Descripción de las medidas técnicas y organizativas de seguridad de la información"* se indica, respectivamente, lo siguiente:

. "Órganos administrativos municipales y otras Administraciones Públicas. Personas interesadas".

. "Se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, según normas internas".

El texto completo del inventario se encuentra publicado en la dirección web https://www.gijon.es/es/publicaciones/inventario-del-registro-de-actividades-de-tratamiento-de-datos-personales.
En dicha página web, figuran los datos identificativos del responsable (AYUNTAMIENTO) y DPD:

QUINTO: Con fecha 08/02/2023**,** la Directora de la Agencia Española de Protección de

Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por las presuntas infracciones de los artículos 32 y 5.1.f) del RGPD, tipificadas en los artículos 83.4.a) y 83.5.a) del citado RGPD, y calificadas como grave y muy grave a efectos de prescripción en el artículo 73.g) y artículo 72.1.a) de la LOPDGDD, respectivamente.

En el acuerdo de apertura se determinó que la sanción que pudiera corresponder, sin perjuicio de lo que resulte de la instrucción, sería de apercibimiento.

Asimismo, se advertía que las infracciones imputadas, de confirmarse, podrán conllevar la imposición de medidas, según el citado artículo 58.2 d) del RGPD.

SEXTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la LPACAP, la parte reclamada presentó escrito de alegaciones en el que solicita el archivo del procedimiento en base a las consideraciones siguientes:

1. El inicio del procedimiento, pasados dos años desde los hechos y más de doce meses desde la reclamación, cuando el AYUNTAMIENTO ya había dado respuesta a la parte reclamante mediante la resolución de 30/08/2021 y a la propia AEPD en el marco de sus investigaciones, reconociendo los hechos y detallando las medidas a aplicar para que los mismos no vuelvan a producir, contraviene lo dispuesto en el artículo 84 del RGPD, según el cual las sanciones deben ser “efectivas, proporcionadas y disuasorias”. Entiende que la sanción propuesta carece de efectividad cuando el responsable del tratamiento ha admitido el error y procedido a su corrección.

2. En relación con el incumplimiento del artículo 32 del RGPD, advierte sobre las medidas de seguridad contenidas en el Informe de su Servicio de Sistemas de información, de fecha 10/03/2021, cuya implementación supuso la restricción de los accesos al Registro de documentos, que fue la causa raíz de la exfiltración del documento objeto de la reclamación; y señala que la AEPD no ha tenido en cuenta estas medidas, ya adoptadas en el momento en que se reconocieron los hechos, y traslada al momento actual aquella falta de medidas de seguridad que provocaron la brecha sin haber realizado nuevas averiguaciones.

Por otra parte, señala que el “riesgo cero” no existe, según admite la propia AEPD, y reseña lo declarado por el Tribunal Supremo en la sentencia núm. 188/2022, de la Sección Tercera de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de febrero, cuando señala que *“la obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, sino de medios. Como consecuencia de dicha obligación de medios, el compromiso que adquiere el responsable del tratamiento es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución”* (F.D.3º).

Seguidamente describe otras medidas técnicas y organizativas adoptadas desde que se produjeron los hechos, las cuales se incluyen entre las mencionadas en el Hecho Probado Quinto.

3. Reconoce la filtración de la información objeto de la reclamación, por lo que señala expresamente que *"no cabe alegar a este hecho objetivo"*.

No obstante, recuerda que el deber de confidencialidad de las personas implicadas en la filtración indebida de la información (…), les viene impuesto por el artículo 5.5 de la Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad; y que, con fecha 13/09/2021, el ***PUESTO.1 remitió una nota informativa recordando expresamente esta obligación.

4. Considera la parte reclamada que el reconocimiento del incidente de filtración de datos, incluso ante la parte reclamante, y el esfuerzo continuado que viene realizando en la mejora de las medidas técnicas y organizativas para evitar que vuelvan a producirse pérdidas de la confidencialidad de los datos personales debe tenerse en cuenta para resolver el procedimiento con archivo de las actuaciones.

SÉPTIMO: Con fecha 15/09/2023, por el instructor del procedimiento se formuló propuesta de resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se imponga a la entidad AYUNTAMIENTO DE GIJÓN una sanción de apercibimiento por cada una de las infracciones siguientes:

. por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del citado RGPD, y calificada como grave a efectos de prescripción en el artículo 73.f) de la LOPDGDD.
. por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del citado RGPD, y calificada como muy graves a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD

OCTAVO: La citada propuesta de resolución se notificó a la entidad reclamada en la misma fecha del 15/09/2023, a través del Servicio de Dirección electrónica Habilitada Única (DEHÚ). En este escrito de notificación se concedió a dicha entidad plazo para formular alegaciones, que ha transcurrido sin que en esta Agencia se haya recibido escrito alguno.

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

HECHOS PROBADOS

PRIMERO: Con fecha 20/01/2021, la parte reclamante presentó un escrito en el Registro Electrónico del AYUNTAMIENTO DE GIJÓN mediante el que informaba sobre la posible comisión de una infracción del régimen disciplinario de la Policía Local. En este escrito constan los datos relativos a nombre y apellidos de la persona presuntamente autora de la infracción del régimen disciplinario y los datos de la persona que presenta este escrito en nombre y representación de la parte reclamante (nombre, apellidos, DNI y puesto que ocupa en la organización de la parte reclamante).

SEGUNDO: Con fecha 19/02/2021, la parte reclamante presentó ante el mismo AYUNTAMIENTO un nuevo escrito para comunicar la difusión ilícita del documento reseñado en el Hecho Probado Primero a través de la plataforma de mensajería Whatsapp. En este escrito solicita que se comprueben los accesos ilegítimos a aquel escrito y se investigue su difusión.

TERCERO: Mediante escrito de fecha 30/08/2021, el AYUNTAMIENTO DE GIJÓN dio respuesta a la parte reclamante sobre su denuncia de fecha 19/02/2021, reseñada en el Hecho Probado Segundo. En este escrito, cuyo contenido consta reseñado en el Antecedente Primero, el cual se declara reproducido en este acto a efectos probatorios, el AYUNTAMIENTO citado informa a la parte reclamante sobre el resultado de las comprobaciones realizadas por su Servicio de Sistemas de Información respecto de los hechos denunciados, de las que cabe destacar las siguientes:

. Confirma los accesos al Registro General del AYUNTAMIENTO DE GIJÓN (…), al asiento registral correspondiente al documento reseñado en el Hecho Probado Primero; que (…) disponen de una cuenta de usuario que les permite el acceso remoto *"al módulo de comunes del libro general del registro de entrada de documentos del Ayuntamiento"*; y que este permiso estaba justificado por "*el desempeño ordinario de las tareas de los puestos de trabajo o (…).*

. Según consta en dicho informe, (…) declararon haber tenido conocimiento de la difusión del documento reseñado en el Hecho Probado Primero a través de dos grupos de Wahtsapp ***(…),*** pero negaron haberla participado en este hecho.

. Se añade en dicho informe que el representante de la parte reclamante aportó evidencias de la difusión del documentó íntegro en formato "pdf" a través de uno de aquellos grupos de Whatsapp (…).

. En relación con las causas del incidente de seguridad y las medidas adoptadas con tal motivo, el repetido informe del Servicio de Sistemas de Información indica lo siguiente:

"En la configuración de las cuentas de usuario de las aplicaciones: para las cuentas de usuario implicadas en el incidente de seguridad, se han eliminado permisos asociados que ya no deberían de estar por haber cambiado la persona de lugar de trabajo o de funciones.
En la configuración de acceso al Registro General: se ha desactivado la posibilidad de consultar los documentos asociados a todos los registros de entrada del libro general de entrada del Ayuntamiento. Esta opción de consulta estaba asociada a un número importante de personas, que lo habían solicitado desde el año 2015 hasta la actualidad y que era necesario para poder trabajar de forma correcta con los expedientes de su competencia.
Al respecto, no consta que la medida de limitación de accesos generalizados al módulo de comunes del registro de entradas haya afectado al desempeño de las tareas habituales de los puestos de trabajo objeto de investigación".

CUARTO: El AYUNTAMIENTO DE GIJÓN aportó a las actuaciones la relación de empleados que accedieron al documento reseñado en el Hecho Probado Primero en el período comprendido entre su presentación en el Registro General y su difusión. En esta relación se detalla el DNI de las personas que accedieron al documento, nombre,

apellidos, y departamento al que pertenecen (…).

QUINTO: Durante la tramitación de la reclamación que ha dado origen a las actuaciones, el AYUNTAMIENTO DE GIJÓN informa a esta Agencia que ha resuelto adoptar medidas técnicas y organizativas complementarias adicionales:

. Modificar la forma de altas, bajas y movilidad del personal municipal en la asignación de cuentas, permisos o autorizaciones de acceso, revocación o desactivación de aplicaciones y recursos informáticos y electrónicos, en atención a las funciones y tareas que efectivamente desempeñen en sus puestos de trabajo en la organización;

. Medidas reguladoras, técnicas y formativas que resulten adecuadas acerca de la existencia, creación y utilización de grupos de mensajería, redes sociales o de comunicación internas del personal municipal.

. Emitir una Instrucción de la Alcaldía reguladora del acceso y autorización de uso de los sistemas de información municipales.

. Contratación de asistencia externa en relación con la seguridad de la información.

. Establecimiento de procedimientos de gestión de brechas; aprobación de una política de seguridad; constitución de un comité de seguridad de la información y protección de datos personales; y establecimiento de procedimientos de seguridad, aprobados en el mismo Comité, para copias gestión de terceros (servicios externos), de certificados (claves criptográficas), de análisis de riesgos, calificación de la información, gestión de la documentación, borrado de soportes, e instrucciones técnicas de limpieza de metadatos y cifrado de soportes.

(…)

FUNDAMENTOS DE DERECHO

I
Competencia

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

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
Obligación incumplida. Seguridad de los datos

Los hechos denunciados se materializan en el acceso por terceros no interesados a un escrito presentado por la parte reclamante ante la parte reclamada, a través del Registro Electrónico, vulnerando la normativa en materia de protección de datos. El escrito en cuestión fue posteriormente difundido a través de una aplicación de mensajería instantánea.

La seguridad de los datos personales se regula en los artículos 32, 33 y 34 del RGPD.

El artículo 32 del RGPD, *"Seguridad del tratamiento"*, establece lo siguiente:

"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".

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*.

Hay que señalar que el RGPD no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En el presente caso, la documentación obrante en el expediente aporta evidencias suficientes sobre un incumplimiento del artículo 32.1 del RGPD por la parte reclamada, causado por una falta de medidas de seguridad que posibilitaba el acceso por sus empleados a todos los documentos presentados en el Registro Electrónico de la entidad, incluso a aquellos ajenos a las funciones que les eran propias. El acceso a los documentos conllevaba, obviamente, el acceso a la información personal contenida en los mismos.

A este respecto, de la información aportada por la propia entidad reclamada, que consta en un informe sobre el incidente elaborado por su Servicio de Sistemas de Información, se desprende que el Registro de Entrada de documentos de esta entidad podía ser accedido sin restricción por un número elevado de personas, aunque el asunto al que correspondiera el documento en cuestión no estuviese relacionado con actuaciones o funciones específicas asignadas a tales personas. Se dice, incluso, que existían permisos de acceso a la información de dicho Registro asociados a personas que habían cambiado de lugar de trabajo o de funciones.

Prueba de las deficiencias de seguridad detectadas son las medidas anunciadas por la parte reclamada para evitar incidentes futuros, que incluye la adopción de un nuevo protocolo *"en la asignación de cuentas, permisos o autorizaciones de acceso, revocación o desactivación de aplicaciones y recursos informáticos y electrónicos, en atención a las funciones y tareas que efectivamente desempeñen en sus puestos de*

trabajo en la organización".

El AYUNTAMIENTO DE GIJÓN afirma, incluso, que las medidas adoptadas para la limitación de los accesos generalizados al módulo de comunes del Registro de Entrada no ha afectado al desempeño de las tareas habituales de los puestos de trabajo objeto de investigación, lo que viene a confirmar que los protocolos implantados por esta entidad en el momento en que tuvieron lugar los hechos analizados no eran adecuados para garantizar la seguridad de los datos y que tales protocolos no estaban justificado por el desempeño de las funciones atribuidas a las personas que disponían de permisos para acceder al mencionado Registro.

Consta, asimismo, que el escrito de la parte reclamada accedido indebidamente, en el que se informaba sobre una posible infracción del régimen disciplinario de la Policía Local, además de las circunstancias de hecho que a juicio de la parte reclamante determinan la posible infracción disciplinaria, incluía los datos personales relativos a nombre y apellidos del posible infractor y los datos del representante de la parte reclamante relativos a nombre, apellidos, DNI y puesto que éste ocupa en la organización de la parte reclamante.

Estos hechos ponen de manifiesto que la entidad reclamada no disponía de las medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de los datos, especialmente las dirigidas a impedir el acceso a la información por terceros no interesados. Ello permitió que varias personas de la organización accedieran al escrito presentado por la parte reclamante el día 20/01/2021 en el Registro de Entrada de la parte reclamada, aunque las funciones asignadas a estas personas no estuviesen relacionadas con el objeto del escrito en cuestión.

En Resolución de la Alcaldía, de fecha 30/08/2021, en relación con la licitud de los accesos comprobados, llega a manifestarse lo siguiente:

"De ello, cabe concluir que alguno de los tratamientos expresados en los Antecedentes, como el acceso habitual, general o indiscriminado a las anotaciones del registro de entrada o para ejercicio de supuestos derechos sindicales, no guarda relación con la base de licitud y finalidades contenidas en el mencionado inventario de actividades".

En consecuencia, de conformidad con las evidencias expuestas, los citados hechos suponen una vulneración de lo dispuesto en el artículo 32 del RGPD, que da lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

III
Obligación incumplida. Deber de confidencialidad

Por otra parte, el artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona, entre ellos, el de *"integridad y confidencialidad"*:

"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").
(…)".

De acuerdo con lo expuesto en el Fundamento de Derecho anterior, la documentación obrante en las actuaciones ofrece evidencias suficientes para entender que la parte reclamada vulneró el artículo 5.1.f) del RGPD, que regula el deber de confidencialidad, materializado en el acceso por terceros no interesados a los datos personales contenidos en el escrito presentado por la parte reclamante ante el AYUNTAMIENTO DE GIJÓN, reseñado en el Hecho Probado Primero.

Este deber de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos. En el presente caso, la filtración indebida de datos ha sido reconocida por la parte reclamada.

En consecuencia, los citados hechos suponen una vulneración de lo dispuesto en el artículo 5.1 f) del RGPD, que da lugar a la aplicación de los poderes correctivos que el artículo 58 del citado Reglamento otorga a la Agencia Española de Protección de datos.

IV
Alegaciones de la parte reclamada

Considera el AYUNTAMIENTO que el presente procedimiento sancionador carece de efectividad considerando que se inicia cuando dicha entidad ya había dado respuesta a la parte reclamante, se habían reconocido los hechos y se habían adoptado medidas para evitar incidentes similares, que no han sido consideradas. Entiende, por las mismas razones que debe resolverse con archivo de las actuaciones.

Sin embargo, no comparte esta Agencia dicho planteamiento, por cuanto lo procedente es analizar y resolver lo oportuno conforme a la situación de hecho objeto de la reclamación. Otra cosa es considerar la reacción de la parte reclamada ante los hechos denunciados, en cuanto a la obligación de adoptar medidas para la adecuación de su actuación a la normativa, que se analiza en el Fundamento de Derecho VII.

Por otra parte, la parte reclamada advierte sobre lo declarado por el Tribunal Supremo en la Sentencia número 188/2022, de 15 de febrero, sobre la naturaleza de la obligación de adoptar medidas, según la cual no puede una obligación de resultado, sino de medidos. A este respecto, conviene insistir que la infracción del artículo 32 no se declara, en este caso, por el hecho de que las medidas adoptadas por el AYUNTAMIENTO DE GIJÓN no hayan conseguido el resultado esperado, sino por la falta de medidas adecuadas, según ha quedado expresado en los Fundamentos de Derecho que preceden.

V
Tipificación y calificación de las infracciones

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a)

del citado RGPD en los siguientes términos:

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

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

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

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

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

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

Por otra parte, el incumplimiento de lo establecido en el artículo 5.1 f) del RGPD supone la comisión de una infracción tipificada en el apartado 5.a) del artículo 83 del RGPD, que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

A efectos del plazo de prescripción, el artículo 72 de la LOPDGDD indica:

"Artículo 72. Infracciones consideradas muy graves.
1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

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

VI

Poderes correctivos

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

"2 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;
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;".

VII
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, en su redacción vigente en el momento en que tuvieron lugar los hechos objeto de la reclamación que ha motivado las actuaciones, dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

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

(…)

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

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

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.
Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

Este precepto excluye la imposición de multas administrativas cuando las infracciones a las que se refieren los artículos 72 a 74 de la LOPDGDD se cometan por las categorías de responsables o encargados del tratamiento enumerados en el apartado 1 del citado artículo 77, estableciéndose que los procedimientos que tengan causa en vulneraciones de la normativa de protección de datos personales cometidas por aquellas entidades se resuelvan imponiendo a la entidad infractora una sanción de apercibimiento.

Asimismo, se contempla que la resolución que se dicte pueda establecer las medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido y se lleve a cabo la necesaria adecuación, en este caso, a las exigencias contempladas en los artículos 32 y 5.1.f) del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Así, conforme a lo establecido en el citado artículo 77 de la LOPD, se podrá requerir a la entidad responsable (AYUNTAMIENTO DE GIJÓN) para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En este caso, sin embargo, consta en las actuaciones que la parte reclamada, con posterioridad a los hechos objeto de las actuaciones, adoptó medidas dirigidas a impedir los accesos indiscriminados a los asientos del Registro de Entrada por parte

de sus empleados, habiendo establecido nuevos protocolos en la configuración de las cuentas de usuario de las aplicaciones, eliminando permisos y desactivando la posibilidad de consultar los documentos asociados a todos los registros de entrada del libro general de entrada del AYUNTAMIENTO; así como para los procesos de alta de personas en la organización, recogiendo los accesos, recursos técnicos y autorizaciones que deben asignarse, protocolos de baja para la desactivación de las cuentas de usuario y protocolos de modificación de personas por cambios de puesto o de funciones.

En base a ello, no se estima necesario en este caso ordenar a la parte reclamada la adopción de nuevas medidas adicionales a las ya implantadas.

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 GIJÓN, con NIF ***P3302400A***, una sanción de apercibimiento por las infracciones siguientes:

. por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del citado RGPD, y calificada como grave a efectos de prescripción en el artículo 73.f) de la LOPDGDD.
. por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del citado RGPD, y calificada como muy graves a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD

SEGUNDO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE GIJÓN.

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