- **Procedimiento Nº: E/07024/2019**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La reclamación interpuesta por D. ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 05/09/2018 en la Agencia Española de Protección de Datos. La reclamación se dirige contra ***AYUNTAMIENTO DE GIJÓN,*** con NIF ***P3302400A*** (en adelante, el reclamado). Los motivos en que basa la reclamación son: que el 27/11/2018 detecta una brecha de seguridad en la realización de su propio trabajo; que es agente de policía local de Gijón, desarrollando funciones de notificador; que entre sus funciones se encuentra la de trasladar a sedes de otras administraciones y a otros departamentos del mismo ayuntamiento oficios, denuncias y atestados que contienen datos personales, incluso sensibles; que dicha documentación se manipula sin la debida protección, de forma que cualquier funcionario puede tener acceso a ella sin ser instructor ni secretario ni parte interesada alguna en esos informes, atestados, etc.; que habitualmente gran parte de esos informes se depositan en bandejas abiertas colgadas de una pared de las oficinas de la comisaría en la zona de atención al público; que no se han aplicado medidas preventivas antes de la brecha; que las categorías de datos afectados son datos básicos, DNI, NIE, pasaporte, condenas e infracciones penales, datos económicos o financieros, datos de contacto, datos de localización; que habiendo comunicado esta circunstancia a sus superiores, hacen caso omiso y no lo consideran brecha.

Y, entre otra, anexa la siguiente documentación:

 Aporta correo electrónico enviado el 15/12/2018 por el denunciante a *ifgancedo@gijon.es* siendo este último DPD del Ayuntamiento de Gijón, según manifiesta el denunciante, y conteniendo las siguientes manifestaciones:

o Que la documentación que se traslada, se hace sin ningún tipo de protección, sin ser protegidos en sobre cerrado, de forma que cualquier funcionario que la maneje puede ver su contenido aunque no sea parte interesada, instructor ni secretario de dichos expedientes, informes, atestados, etc.
o Que habitualmente muchos de estos expedientes, informes, atestados, etc., se depositan en unas bandejas porta documentos situadas en la pared de las oficinas de Jefatura de Policía Local, situadas en la zona de atención al público donde pueden acceder a ellos tanto cualquier funcionario como los ciudadanos que acuden a estas oficinas a realizar algún trámite, ya que, además, estas bandejas no están bajo la custodia de ningún funcionario concreto.
o Que se le pedía a él que examinara esos expedientes, informes, atestados, etc., para asegurarse de que las copias de los mismos iban bien colocadas para determinar cuál de ellas era la que debía entregar en otros organismos y cuál era la que debía

devolver sellada con el acuse de recibo a Jefatura cuando su función es única y exclusivamente la de trasladarlos, si bien este aspecto, se corrige esta semana solo en parte marcando la copia que debe devolver firmada con un sello en su primera hoja.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

Con fecha 25/01/2019, se da traslado de la reclamación al reclamado, reiterándose dicho traslado el 05/02/2019, no recibiéndose

El 15/07/2019 se inician las presentes actuaciones. Con fecha 07/11/2019, el reclamado remite a esta Agencia la siguiente información y manifestaciones:

1. Que en relación a la no respuesta del traslado en las actuaciones con referencia E/00597/2019, manifiesta que se adjuntan nuevamente los documentos que se enviaron a esta Agencia, documentos que fueron generados entre el 14/03/ y el 26/04/2019. Manifiesta que de la no recepción en el registro no consta el motivo, por lo que podría deberse a una incidencia en los sistemas.

2. Que la incidencia se encuentra cerrada ya que la solución adoptada se notificó al reclamante con fecha 26/04/2019 sin que por parte del mismo se haya recibido ninguna reclamación o comunicación posterior.

3. Aporta informe firmado electrónicamente por el Jefe del Servicio de Policía Local en fecha 14/03/2019 con las siguientes manifestaciones:

a. Que el denunciante está adscrito a la unidad de apoyo administrativo en el equipo de informadores con las siguientes funciones, entre otras:

i. Informes para todos los juzgados de España sobre averiguaciones.
ii. Citaciones de servicios sociales.
iii. Ratificaciones de sanciones y denuncias de tráfico de diferentes ayuntamientos.
iv. Gestiones D.G.T.
v. Notificaciones de inspección veterinaria, empadronamientos, mesas electorales.
vi. Averiguaciones de convivencias a efectos de pensiones.
vii. Presentación de informes en empresas y organismos municipales.

b. Que los encargos diarios de trabajo a los informadores, en el caso del denunciante, son entregados directamente por un mando de la Policía Local a quien el denunciante devuelve una vez finalizada la jornada.
Las observaciones o necesidad de ampliación de información que se puedan advertir o derivar en cada expediente o encargo, se clasifican, dentro de las Oficinas Generales, en bandejas con destinatarios específicos.

c. Que a los efectos de custodia y confidencialidad de los datos, todos los expedientes o encargos que los informadores tramitan pasan exclusiva y únicamente por manos de funcionarios de la Policía Local, ya sea el mando correspondiente o los agentes destinados en las Oficinas Generales. Igualmente, el acceso a estas Oficinas está restringido al personal autorizado.

d. Que existe tanto en el interior de las dependencias como en el acceso a las salas un sistema CCTV con grabación permanente 24h.
e. Que existe un agente destinado en el control de accesos que está situado en el punto intermedio de ambas salas (Oficinas Generales a la Este y Oficina de Informadores ala Oeste).
f. Se aporta fotografía titulada *"acceso ala este de las dependencias Oficinas generales al fondo".*
En la fotografía se observa el acceso a unas dependencias al fondo, con un agente de la Policía Local en un mostrador.
g. Se aporta fotografía titulada *"acceso ala oeste de las dependencias Oficina de informadores al fondo".*
En la fotografía se observa el acceso a unas dependencias al fondo con el mismo agente de la fotografía anterior. Se visualiza una cámara de videovigilancia al fondo.
h. Se aporta fotografía de detalle del acceso a las oficinas generales con una puerta acristalada cerrada.
i. Se aporta fotografía de detalle del acceso a la oficina de informadores.
En la fotografía se observa en la puerta de entrada un cartel con el mensaje *"Prohibido el paso sin autorización"* y otro cartel informativo de zona videovigilada. Junto a la puerta se visualizan asimismo 3 carteles más rotulados con *"Atención al Público", "Objetos Perdidos", "A control de gestión Policía Local".*
j. Se aporta fotografía de detalle de la entrada a la oficina de informadores.
En la fotografía se observa una puerta abierta y una cámara de videovigilancia dentro de la oficina.
k. Manifiesta que teniendo en cuenta lo expuesto, los documentos que maneja el denunciante están perfectamente custodiados.

4. Aporta informe de intervención de la delegada de protección de datos firmado electrónicamente en fecha 15/03/2019 con las siguientes manifestaciones:

a. Que la normativa específica del cuerpo policial es la Ley 2/2007, de 23 de marzo, de Coordinación de las Policías Locales de Asturias (LCPLA).
Esta ley establece en el artículo 6, relativo a los principios básicos de actuación, que los miembros de los Cuerpos de Policía Local deberán ajustarse en su actuación a los principios básicos recogidos en el Capítulo ll del Título I de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (en adelante LOFCSE), así como por
el resto de las normas que resulten de aplicación. Estos principios comprenden, según el artículo 5.5 LOFCSE, el secreto profesional expresado en los siguientes términos: *"Deberán guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones. "*
b. Que el régimen general aplicable a todos los funcionarios públicos viene señalado en el EBEP (Artículo 52 y 53.12) y comprende el deber de confidencialidad y el de mantener discreción sobre los asuntos que conozcan por razón de su cargo, sin que puedan hacer uso de la información obtenida para beneficio propio o de terceros, o en perjuicio del interés público.
c. Que asimismo es considerada falta muy grave (art. 95.2.e) la publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.

d. Que constituye igualmente delito tipificado en el artículo 417 del Código Penal (L.O. 10/1995, de 23 de noviembre) la revelación de secretos o informaciones de los que el funcionario tenga conocimiento por su oficio o cargo y que no deban ser divulgados.
e. Que la normativa de procedimiento administrativo en ningún momento restringe el transporte o manejo de documentación a las personas, como indica el escrito del denunciante, tienen la condición de *"instructor o secretario del expediente".* Que de otro modo la actividad administrativa de los distintos servicios municipales a los que corresponde registrar, tramitar, informar una actuación o en un expediente o entregar una notificación devendría imposible de ejecutar.
f. Que a la vista del informe del Jefe de la Policía Local se propone la desestimación de la reclamación sin perjuicio de realizar un análisis de riesgo dentro de toda la organización municipal.

5. Se aporta resolución de la Alcaldía firmado electrónicamente en fecha 04/04/2019 con las siguientes manifestaciones:

a. Que, a la vista de los informes realizados, no consta la existencia de una brecha de seguridad.
b. Que es necesario reforzar las medidas de formación y acompañamiento a los servicios para asegurar el adecuado cumplimiento de las obligaciones en materia de protección de datos.
c. Que se ordena la convocatoria de acciones formativas.
d. Que se notifique a la persona afectada de las actuaciones realizadas.

6. Se aporta notificación al reclamante de fecha 04/04/2019 con el contenido de la resolución de la Alcaldía y acuse de recibo en fecha 26/04/2019.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo sucesivo RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

En el presente caso, a la luz de la documentación obrante en el expediente no existen indicios que se hubiera producido brecha de seguridad en los sistemas del reclamado; además, el responsable tenia implementadas medidas que, en principio, eran las adecuadas a fin de garantizar que los datos personales no fueran accesibles por personal ajeno a las dependencias municipales y, como consta en los hechos, se intenta reforzar con nuevas medidas de seguridad adicionales con el fin de minimizar riesgos posibles, extremando las dificultades para el acceso y extracción de la información.

De la respuesta ofrecida por el reclamado se desprende que la confidencialidad de los datos en relación con los expedientes, informes, citaciones, notificaciones, etc, y, en general, cualquier tipo de documentación administrativa que se tramita en las dependencias oficiales pasan exclusivamente por manos de funcionarios de la Policía Local, con independencia de su cargo.

Paralelamente, el acceso a dichas dependencia u oficinas se encuentra restringido al personal autorizado, existiendo en el interior de las dependencias como en los accesos sistema CCTV con grabación permanente las 24h; asimismo, existe un agente destinado en el control de accesos situado en el punto intermedio entre las oficinas generales y la de informadores, quedando todo ello acreditado mediante la aportación de fotografías.

También se aporta informe del DPD y Resolución de la propia Alcaldía en la que se pone de manifiesto el necesario reforzamiento de las medidas de formación y de acompañamiento a los servicios para asegurar el adecuado cumplimiento de las obligaciones en materia de protección de datos; la convocatoria de acciones formativas, etc., lo que muestra una razonable diligencia a fin de mejorar los riesgos reclamados.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a D. ***A.A.A.*** y al AYUNTAMIENTO DE GIJÓN, con NIF ***P3302400A***.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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