- **Procedimiento Nº: E/06379/2021**

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 ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 1 de febrero de 2021 en la Agencia Española de Protección de Datos. La reclamación se dirige contra **AYUNTAMIENTO DE ****LOCALIDAD.1,*** con CIF P2807400C (en adelante, el reclamado).

Los motivos en que basa la reclamación son:
Que recibió del Ayuntamiento, desde una dirección no segura, un correo con un listado en el que se han revelado indebidamente los datos de todas las personas autorizadas para acudir a un evento.

Junto a la reclamación aporta:
Correo electrónico identificado en el dominio ******DOMINIO.1*** donde consta un listado en el que figuran el nombre y apellido de unas 50 familias. En el escrito de reclamación también se ha incluido el listado.

Aporta, asimismo, correo electrónico remitido a ******EMAIL.1*** al que se adjunta el correo recibido por el reclamante.

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), con número de referencia E/02610/2021, se dio traslado de dicha reclamación al reclamado, 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.

TERCERO**:** Al no constar contestación, con fecha 28 de mayo de 2021 la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

CUARTO: 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:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se ha investigado la siguiente entidad:

AYUNTAMIENTO DE ******LEGANÉS.1*** con CIF P2807400C con domicilio en ****DIRECCIÓN.1*

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 22 de junio de 2021 se solicitó información al reclamado y de la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos.

Tras la publicitación de la campaña navideña “Leganés tendrá unas Navidades Seguras con espectáculos infantiles y visita de los Reyes Magos a los patios de los colegios” publicitada con fecha 12 de diciembre de 2020 en la web municipal ******URL.1***, se procede a gestionar un total de ***XXXXXXXXXXXXXXXXXXXXXXXXXXXX***.

La actividad “Visita a los Reyes Magos” se programó para suplir la Cabalgata de Reyes que se suspendió debido a la situación sanitaria derivada de la Covid 19. Se planifica en pases de mañana y tarde en los distintos centros escolares.

El periodo de solicitud era desde el 10 al 30 de diciembre de 2020 y a través del correo electrónico con el fin de evitar colas dada la situación sanitaria. Una vez cubiertos los aforos de las distintas actividades navideñas se notificaba a las familias.

El evento “Visita a los Reyes Magos”, tuvo un gran volumen de solicitudes ***y debido al corto espacio de tiempo en el que procedió a la confirmación a los solicitantes, XXXXXXXXXXXXXXX*** “VISITA A LOS REYES MAGOS EL DÍA 5 EN EL ***COLEGIO ***COLEGIO.1*** en el pase de 17:00 a 17:30h.

Respecto de las causas que hicieron posible la brecha

El Ayuntamiento manifiesta que ***Las causas de la brecha fueron debidas a un error material XXXXXXXXXXXXXXXXXXXXXXXXXX.***

Respecto de los datos afectados.

En total este incidente ha afectado a XXXXXXXXXXXXXXXXXXXXXXXXXX.

Los datos personales corresponden a XXXXXXXXXXXXXXXXXXXXXXXXXX.

El Ayuntamiento manifiesta que ***no se observa daño y perjuicio grave sobre las personas afectadas dado que, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

El Ayuntamiento considera que ***no existen daños en XXXXXXXXXXXXXXXXXXXX.***

Respecto de las medidas de seguridad implantadas

- Con anterioridad a la brecha
    - El Ayuntamiento manifiesta que las medidas de seguridad implantadas corresponden a ***XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX***.
    - ***No se dispone de evaluación de impacto en la Protección de Datos, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***
- El Ayuntamiento ha aportado los siguientes documentos de seguridad:
    - ***Registro de Actividades XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***
    - ***Existencia de políticas internas del buen uso del correo electrónico XXXXXXXXXXXXX.***

- ***Política de Privacidad y aviso legal Municipal XXXXXXXXXXXXXXXXX.***

A este respecto desde la Inspección de Datos se ha accedido con fecha 14 de julio de 2021 a la dirección mencionadas con el siguiente resultado:

- ***Dirección XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

- Medidas adoptadas con posterioridad
  - ***Revisión del Registro de Actividad de Tratamiento XXXXXXXXXXXX"***
  - ***Remisión de aviso y recomendación a todos los interlocutores XXXXXXXXXXXXXXXXXXXXXX.***
  - ***Remisión de un recordatorio con las políticas internas y buenas prácticas en materia XXXXXXXXXXXXXXXXXXX.***
  - ***Incorporar una recomendación organizativa consistente en XXXXXXXX.***
  - ***Contar con buzones específicos y públicos para el envío XXXXXXXXX.***

Respecto de la notificación con posterioridad a las 72 horas.

El Ayuntamiento manifiesta que ***no tenía constancia de la situación, y XXXXXXXXX.***

Dado que no se tenía constancia de lo acontecido, ni de XXXXXXXXXXXXXXXXX.

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 artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como "*todas aquellas violaciones de la seguridad que ocasionen 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.*"

El artículo 5 apartado 1 f) del RGPD establece que "*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 seguridad de los datos personales viene regulada en el artículo 32 del RGPD:

Artículo 32

"Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y

tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse enviado datos personales por parte del responsable de su tratamiento, a través de un correo electrónico y sin que mediara autorización expresa para ello.

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, el reclamado ha informado de todas las actuaciones llevadas a cabo para paliar el incidente, entre ellas, como más destacables, la ***remisión de un recordatorio con las XXXXXXXXXXXXXXXXXXXX.***

Cabe destacar la buena disposición del reclamado en el sentido de que, en cuanto ha tenido conocimiento del incidente, ha puesto en marcha las medidas oportunas para evitar que se pueda repetir en el futuro.

No constan ante esta AEPD reclamaciones de posibles afectados, salvo la que ha dado origen al presente expediente.

III

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

Así pues, 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 al reclamante, ***A.A.A.,*** y al reclamado, **AYUNTAMIENTO DE ****LOCALIDAD.1,*** con CIF P2807400C.

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.

940-0419

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