- **Expediente Nº: E/06660/2021**

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: Con fecha 2 de junio de 2021, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por AYUNTAMIENTO DE VALDEOLMOS-ALALPARDO con NIF P2816200F (en adelante, el AYUNTAMIENTO), recibido en fecha 26 de abril de 2021, en el que informa a la Agencia Española de Protección de Datos de lo siguiente: Se detectó que en la cuenta de correo de una empleada del ayuntamiento ***(***USUARIO.1@alalpardo.org)*** existía una regla de redirección, de forma que todos los correos que le llegaban a esta dirección se redirigían a una cuenta externa a la organización ***(***USUARIO.2@gmail.com***), cuya propiedad nos es desconocida.

Junto a la notificación no se aportan ni documentos ni otras evidencias relativas a la notificación de la brecha.

SEGUNDO: 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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, teniendo conocimiento de los siguientes extremos:

Cronología y naturaleza del incidente

En el Escrito el investigado describe la siguiente cronología de hechos:

(…):
(…)

- ***(…)***
- ***(...)***

Adjunta al Escrito (Anexo 3) el documento "Contrato de protección de datos personales Encargado del tratamiento" suscrito entre el investigado y CISET. Figura firmada digitalmente por el investigado el día 4 de febrero de 2021 y por CISET con fecha de 9 de febrero de 2021.

Número de afectados, categorías de los datos personales expuestos y uso posterior

En relación con los datos personales afectados en el incidente, el investigado en el Escrito manifiesta lo siguiente:
(…)
(…)

Comunicación a los afectados

Según lo visto en el apartado de antecedentes, el investigado señaló en la Notificación (registrada de entrada en la AEPD el día 26 de abril de 2021) que la decisión de comunicar a los afectados estaba *"Pendiente de decidir".*
Posteriormente, con fecha de 5 de mayo de 2021 la AEPD dirigió el Escrito AEPD en el que en relación con esta brecha de seguridad ordenó lo siguiente:
"Se lleve a cabo la comunicación de la mencionada brecha de seguridad a los interesados, sin dilación indebida, para que, una vez tengan conocimiento de esta, puedan adoptar las medidas que consideren oportunas para evitar aquellos riesgos que pudieran afectar a su persona.
La comunicación a los interesados se realizará siguiendo lo previsto en el artículo 34 del RGPD, en particular en su apartado segundo, debiendo describir en lenguaje claro y sencillo la naturaleza de la violación de seguridad de los datos personales y las posibles medidas que pudieran ser tomadas por los interesados en función de los riesgos que, en cada caso, pudieran ser identificados por los afectados.
El cumplimiento de lo ordenado se exige a tenor de lo previsto en los artículos 34.4 del RGPD como consecuencia de que en la brecha de seguridad de los datos personales se han visto afectados (…).
Si la comunicación a los afectados supone un esfuerzo desproporcionado, podrá optar por una comunicación pública o medida semejante por la que se informe de manera igualmente efectiva a los interesados, en virtud del artículo 34.2c del RGPD.
Así mismo, se requiere confirmación por parte del responsable de tratamiento del cumplimiento de la orden de comunicación a los afectados mediante registro de entrada en sede electrónica en el plazo de 30 días, haciendo referencia a esta orden. […]"
Según el documento emitido por "carpeta ciudadana" (Rechazo de notificación por caducidad) el Escrito AEPD fue rechazado por caducidad de la notificación con fecha de 21 de mayo de 2021.
Sobre este particular el investigado en el Escrito (fecha de registro fecha de 11 de octubre de 2021) señala lo siguiente:
(…)

Motivo por el cual no se ha notificado a la AEPD en el plazo de 72 horas

A este respecto el investigado en el Escrito manifiesta lo siguiente:
(…)

Medidas de seguridad implantadas con anterioridad

(…)
(…):
(…)

Adjunta el investigado al Escrito (Anexo 2) el análisis de riesgos que incluye, entre otras cuestiones, las siguientes:

- ***(…)***
- ***(…):***
  - ***(…)***
  - ***(…)***
- ***(…)***
- ***(…)***
- ***(…):***
  - ***(…)***
    - ***(…)***
  - ***(…)***
    - ***(…)***
    - ***…)***
  - ***(…)***
    - ***(…)***
    - ***(…)***
  - ***(…)***
    - ***(…)***
    - ***(…)***
- ***(…)***
- ***(…)***

Información sobre la recurrencia hechos análogos

Manifiesta en el Escrito el investigado que *"Hasta el momento no se había producido ningún incidente análogo en el Ayuntamiento que haya causado la destrucción, pérdida, alteración, comunicación o el acceso no autorizado a los datos personales responsabilidad del Ayuntamiento."*

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones*

reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el AYUNTAMIENTO realiza, entre otros tratamientos, la recogida, registro y conservación de los siguientes datos personales de personas físicas, tales como: nombre y apellidos, número de identificación, dirección de correo electrónico, datos de salud…, etc.

El AYUNTAMIENTO realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del citado artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha 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."

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 producido un acceso no autorizado de personas u organizaciones que no están autorizadas, o no tienen un propósito legítimo para acceder a los datos.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Seguridad del tratamiento

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y

organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

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

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, de la documentación aportada por el AYUNTAMIENTO en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, el AYUNTAMIENTO careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Tampoco constan reclamaciones ante esta Agencia por parte de terceros, relacionadas con la presente brecha de seguridad.

IV
Notificación de una violación de la seguridad de los datos personales a la autoridad de control

El artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control"* del RGPD dispone:

"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".

En el presente supuesto, se ha notificado la brecha de seguridad en un plazo superior a las 72 horas desde que se tuvo conocimiento de que se había producido, pero se han acreditado correctamente los motivos de tal dilación, el AYUNTAMIENTO alega que es el día 26 de abril cuando el delegado de protección de datos tiene la información necesaria para determinar la necesidad de notificar esta violación de seguridad a la AEPD.

V

Comunicación de una violación de la seguridad de los datos personales al interesado

El artículo 34 "*Comunicación de una violación de la seguridad de los datos personales al interesado"* del RGPD establece*:*

"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 el presente caso, no resultaba probable que la brecha de seguridad entrañara un alto riesgo para los derechos y libertades de las personas físicas, el AYUNTAMIENTO había adoptado las medidas de protección técnicas y organizativas apropiadas y estas medidas se habían aplicado a los datos personales afectados por la brecha de seguridad.

El AYUNTAMIENTO había tomado medidas que garantizaban que no existía la probabilidad de que se concretara un alto riesgo para los derechos y libertades de los interesados, por lo que el AYUNTAMIENTO no estaba obligada a realizar la comunicación a los interesados de que se había producido una brecha de seguridad, en los términos del artículo 34 del RGPD.

Cabe destacar que no consta ante esta Agencia reclamación alguna sobre la brecha de seguridad objeto del presente expediente.

VI
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

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 *AYUNTAMIENTO DE VALDEOLMOS-ALALPARDO.*

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.

1245-120122

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