

- **Expediente N°: EXP202101828**

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 3 de septiembre 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 SINDICATO INDEPENDIENTE DE POLICÍA LOCAL DE GRANADA con NIF G18225615 (en adelante, SINDICATO), recibido en fecha 2 de septiembre de 2021 en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

El exsecretario del sindicato ha tenido acceso a un correo electrónico que adjunta un documento con información de los afiliados. El exsecretario habría utilizado los datos de los afiliados obtenidos de esta forma para enviarles publicidad del sindicato al que esta persona pertenecería actualmente.

Junto a la notificación se aporta informe pericial de fecha 05/07/2021 que contiene certificados de 5 correos electrónicos.

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:

Notificación a la AEPD

- (...)

Cronología y naturaleza del incidente

- (...)

Medidas de seguridad implantadas con anterioridad

Se ha obtenido la siguiente información a este respecto:

(...)

Causas del incidente

(...)

Medidas de seguridad implantadas tras el incidente

(...)

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

Sobre esta cuestión se ha obtenido la siguiente información:

(...)

Comunicación a los afectados

Sobre la comunicación a los afectados el investigado ha facilitado la siguiente información:

(...)

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 registrarán 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 SINDICATO realiza, entre otros tratamientos, la recogida, registro y utilización de los siguientes

datos personales de personas físicas, tales como: datos de contacto, número de identificación y datos de afiliación sindical..., etc.

El SINDICATO 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 de personas que no están autorizadas, o no tienen un propósito legítimo para acceder a ella.

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 SINDICATO en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, el SINDICATO careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

El SINDICATO tenía implementadas medidas de seguridad que, en principio, eran las adecuadas para garantizar que los datos personales no fueran accesibles por terceros.

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.

Como consta en los hechos en cuanto el ataque fue detectado y confirmado se adoptaron una serie de medidas de seguridad adicionales con el fin de minimizar los riesgos.

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 SINDICATO informa que notificó al Consejo de Transparencia y Protección de Datos de Junta de Andalucía en el plazo establecido al entender que era el órgano competente en esta materia. Con posterioridad el día 1 de septiembre de 2021 se nos comunicó por el propio Consejo de Transparencia de que había dado traslado de la brecha a la Agencia Española de Protección de Datos. Es por dicho motivo por el que se notificó a esta Agencia el día 2 de septiembre de 2021.

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."

El SINDICATO aporta copia de la comunicación enviada a los usuarios afectados, de acuerdo con lo establecido en el citado artículo 34 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 la actuación del SINDICATO INDEPENDIENTE DE POLICÍA LOCAL DE GRANADA.

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 a SINDICATO INDEPENDIENTE DE POLICÍA LOCAL DE GRANADA.

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