- **Expediente Nº: E/07781/2020**

IMI Case Register **177442**

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 28 de septiembre de 2020, las actuaciones de inspección se inician como consecuencia del análisis de un escrito de notificación de brecha de seguridad de los datos personales, remitido por TEKA INDUSTRIAL, S.A con NIF A39004932 (en adelante, TEKA) en el que informa a la Agencia Española de Protección de Datos, en fecha 24 de agosto de 2020, de lo siguiente: que pertenece al grupo HERITAGE-B y que ha sufrido una brecha de seguridad producto de un ***(…)*** que ha afectado a diversas entidades del Grupo ubicadas en distintos países, entre las que se encuentra TEKA. Manifiesta también que hay empresas del grupo en Alemania, Francia, Reino Unido, Suiza y México. El Grupo HERITAGE-B ha notificado a la AEPD y a la Autoridad de Alemania ya que considera que son los países donde se encuentran ubicados los establecimientos principales del grupo.

SEGUNDO: El “Sistema de Información del Mercado Interior” (en lo sucesivo “Sistema IMI”), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), tiene por objeto favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información. A través del Sistema IMI (A56ID 175553), con fecha 20 de enero de 2021 esta Agencia se declaró autoridad principal en este asunto, en virtud del artículo 4.23 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, 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 (RGPD), dado que TEKA tiene uno de sus establecimientos principales en España.

Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúan en calidad de “autoridad de control interesada” las autoridades de control de: Berlín (Alemania), Baden-Wurttemberg (Alemania), Bavaria- Sector Privado (Alemania), Francia y Mecklenburg-Western Pomerania (Alemania). Todas ellas en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en estos Estado miembro se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

TERCERO: 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 notificación, teniendo conocimiento de los siguientes extremos:

Con fecha 27 de octubre de 2020 se solicitó información a TEKA y de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa

- TEKA es una empresa que pertenece al grupo societario HERITAGE-B dedicada a la fabricación, venta y distribución de productos fabricados en aceros especiales. TEKA es la sociedad cabecera de tres líneas de negocio distintas: cocinas, baños y contenedores industriales.

TEKA es considerada como entidad cabecera del Grupo HERITAGE-B en la medida en que determinadas decisiones relevantes relativas a sistemas de información se adoptan por dicha entidad.

- ***(…)***
(…)

Respecto de la cronología de los hechos

- ***(…)***

- (…)

- (…)

- (…)

(…)

Respecto de las causas que hicieron posible la brecha

- ***(…)***

(…)

Medidas de minimización del impacto de la brecha y acciones tomadas para la resolución final

- ***(…)***

- (…)

- (…)

(…)

Respecto de los datos afectados

- ***(…)***

- (…)

(…)

(…)

- (…)

(…)

- (…)

- (…)

(…)

(…)

- (…)

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha

- (…)

(…)

(…)

(…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

Respecto de las medidas implementadas con posterioridad a la brecha

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

- (…)

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo

- (…)

CUARTO: Con fecha 02/09/2021, la Directora de la AEPD adoptó un proyecto de decisión de archivo de actuaciones. Ese mismo día, siguiendo el proceso establecido en el artículo 60 del RGPD, se compartió en el Sistema IMI el proyecto de decisión de archivo de actuaciones y se les hizo saber a las autoridades de control interesadas que tenían cuatro semanas desde ese momento para formular objeciones pertinentes y motivadas. Transcurrido el plazo a tal efecto, las autoridades de control interesadas no presentaron objeciones pertinentes y motivadas al respecto, por lo que se considera que todas las autoridades de control están de acuerdo con dicho proyecto de decisión y están vinculadas por este, de conformidad con lo dispuesto en el apartado 6 del artículo 60 del RGPD.

FUNDAMENTOS DE DERECHO

I
Competencia

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
Cuestiones previas

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 que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, como consecuencia de un ***(…),*** que ha afectado a TEKA.

Hay que señalar que la notificación de una brecha 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.

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.

III
Artículo 32 del RGPD

El considerando (39) del RGPD dice que:

"(…) Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

En este sentido, 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 TEKA en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, TEKA 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
Artículo 33 del RGPD

El considerando (85) del RGPD dice que:

"(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".

En este sentido, 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, TEKA notificó la brecha de seguridad en el plazo establecido en el RGPD a tal efecto, con las informaciones establecidas en el artículo 33 del RGPD.

V
Artículo 34 del RGPD

El considerando (86) del RGPD dice que:

"El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que pueda 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 este sentido, 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. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

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, por lo que TEKA 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 constan ante esta AEPD reclamaciones de posibles afectados.

VI
No existencia de infracción

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 a TEKA INDUSTRIAL, S.A.

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.

940-010921

Mar España Martí
Directora de la AEPD, P.O. la Subdirectora General de Inspección de Datos, Olga Pérez Sanjuán, Resolución 4/10/2021