Expediente N.º: PS/00059/2022

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 18 de marzo 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 CONSEJERÍA DE EDUCACIÓN Y CULTURA con NIF S3011001I (en adelante, CEC), recibido en fecha 06/03/2021, en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

"(…)".

Con fecha 29/03/2021 se recibe una notificación complementaria con la que se aporta, como documentación adjunta, denuncia presentada ante la Dirección General de la Policía, y un informe elaborado por la Subdirección General de Informática Corporativa de la Consejería de Presidencia y Hacienda de la Región de ******LOCALIDAD.1***, en el que se evalúan el alcance, acciones y daños en relación con el incidente de seguridad producido.

SEGUNDO: Con fecha 07/03/2021 se recibe una reclamación de ***A.A.A.***. Los motivos en que basa la reclamación son los siguientes:

"(…)".

Con fecha 25/03/2021, de conformidad con el artículo 65 de la LOPDGDD, se admite a trámite la reclamación y se une al expediente iniciado tras la notificación de la brecha de seguridad.

TERCERO: Con fecha 12/03/2021 se recibe otra reclamación de la ***(…),*** representada por ***B.B.B.*** abogado colegiado Nº ***XXXX***, del Ilustre Colegio de Abogados de ******LOCALIDAD.1***, en la que se expone lo siguiente:

"(…)".

Con fecha 08/04/2021, de conformidad con el artículo 65 de la LOPDGDD, se admite a trámite la reclamación y se une al expediente iniciado tras la notificación de la brecha de seguridad.

CUARTO: 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:

- Con fecha de 7 de marzo de 2021, los servicios informáticos de la Comunidad Autónoma Región de ******LOCALIDAD.1*** emitieron un comunicado anunciando que habían sufrido ataques masivos en los sistemas de la CONSEJERÍA DE EDUCACIÓN Y CULTURA. Sin embargo, no se aclaró si los ataques habían tenido éxito, y si alguna información personal había sido expuesta a desconocidos. La única acción solicitada desde dichos servicios ha sido el cambio de contraseña, hasta cuatro veces en un fin de semana, con el consiguiente bloqueo en las cuentas y la actividad de sus usuarios.

- En la plataforma que ha sido víctima del ataque hay almacenados datos de unos 37.500 docentes. Algunos de ellos han notado que sus datos bancarios han sido modificados. Se conjetura que se habría podido violar la integridad o la confidencialidad de otras tipologías de información personal que también se albergan en la plataforma, como expedientes académicos, titulaciones, experiencia docente o notas de oposiciones.

Número de afectados según notificación: ***XX.XXX***.

Tipología de los datos según notificación: usuario y contraseña

Indican que han comunicado la brecha a los afectados.

Respecto de la empresa

La entidad notificante es una institución pública española. Se ha encontrado en los archivos de la AEPD expedientes anteriores al presente con relación a brechas de esta entidad (E/04753/2020).

Se ha solicitado información y documentación a la entidad notificante, y de la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

(…).

Según la documentación recibida (y que no ha podido ser comprobada) las medidas adoptadas para la resolución de la brecha son satisfactorias.

Respecto de las causas que hicieron posible la brecha

(…).

Puede concluirse de la documentación recibida, que no se han aplicado las medidas técnicas y organizativas necesarias para evitar que la brecha se produjera.

Respecto de los datos afectados

(…).

Respecto del contrato de encargado del tratamiento

(…).

Respecto de las medidas de seguridad implantadas

(…).

Estas supuestas medidas de seguridad implantadas con anterioridad no han podido ser comprobadas, al no aportar el reclamado, constancia de haberlas implementado. Se duda que se haya tenido un control de acceso efectivo, si no la brecha no se hubiera producido ya que indican que se produjo por ***(…)***. Además, indican que habían implementados diferentes niveles de acceso a los datos, afirmación que queda en entredicho cuando en el apartado de "cómo se produjo la brecha" se indica:

*"**(…)**"*

Medidas técnicas y organizativas adoptadas para evitar, en lo posible, incidentes como el sucedido***.***

(…).

- Otras medidas:

(…).

Estas medidas no han podido ser verificadas, pero en sí parecen suficientes para evitar eventos similares a futuro.

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

(…).

QUINTO: Con fecha 4 de marzo de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

Notificado el acuerdo de inicio, la CEC presentó un escrito de alegaciones en el que en síntesis, manifestaba que:

-Aunque en un primer momento, se consideró que el incidente se debía a ***(…)***, y que no se considera infringido el artículo 32 del RGPD ya que, con anterioridad al incidente que ocasiona la brecha de seguridad de los datos, el Responsable había adoptado una serie de medidas técnicas y organizativas destinadas a la protección de los datos de carácter personal y la seguridad de los sistemas de información, por tanto el origen del incidente no es debido a la falta de medidas de seguridad, ***(…)***.

A este respecto hay que señalar que, aunque el responsable en sus alegaciones afirma disponer con carácter previo a la brecha de unas certificaciones que acreditarían las medidas implantadas, no aporta soporte documental alguno que las acredite.

De la documentación que obra en el expediente se infiere que el incidente se podría haber evitado con un sistema de doble autenticación, y que las medidas implantadas previamente no resultaron adecuadas y suficientes para evitarlo.

-No se considera infringido el artículo 34 del RGPD, ya que el Responsable actuó de forma diligente y pro activa al informar a los interesados como primera medida de reacción frente al incidente, y ello teniendo en cuenta, además, que no ha existido en ningún momento un alto riesgo para los afectados que debiera poner en marcha la comunicación a los interesados conforme al artículo 34 RGPD.

Alegan, asimismo, que para el cálculo del riesgo de la brecha se ha seguido la metodología y las pautas de la AEPD. El riesgo es el resultado de multiplicar el impacto por la probabilidad. Debido a la premura de la situación se aplica el procedimiento abreviado, cuyo resultado es un impacto bajo (severidad de la brecha) y una probabilidad media. Los factores tenidos en cuenta para calcular la probabilidad han sido: (A) el volumen de afectados (***XX.XXX*** usuarios), (B) la probabilidad de identificar a los afectados (datos ilegibles) y (C) los datos afectados en un periodo de tiempo (desde noviembre de 2020). En consecuencia, trasladando dichos datos a la matriz del Anexo III del procedimiento de gestión de incidentes, el riesgo de la brecha es bajo.

A este respecto, esta Agencia procede a analizar de nuevo las comunicaciones efectuadas a los afectados en el momento de producirse la brecha, concluyendo que no se puede afirmar que se haya incumplido el artículo 34 del RGPD, pues la CEC acredita no solo haber informado a cada uno de los profesores afectados, sino también que la noticia se publicó en prensa: ******URL.1***.

Se estiman pues las alegaciones en lo que a la infracción al artículo 34 del RGPD se refiere, dejando sin efecto la imputación inicial por el incumplimiento de dicho artículo.

SEXTO: Con fecha 17 de mayo de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se

imponga a CONSEJERÍA DE EDUCACIÓN Y CULTURA, con NIF S3011001I, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD una sanción de apercibimiento.

Notificada la citada propuesta en fecha 20/05/2022, no consta que se hayan presentado alegaciones a la misma.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Consta acreditado que el día 04/03/202, la CEC sufrió un incidente de seguridad, calificado como brecha de confidencialidad, integridad y disponibilidad, al haberse constatado que los datos personales de los afectados han quedado expuestos a terceros no autorizados, que se cambiaron contraseñas de acceso, por lo que algunos de los afectados no tuvieron temporalmente acceso a sus cuentas, así como que se modificaron datos bancarios de algunas personas.

SEGUNDO: Consta acreditado que la CEC contaba con una serie de medidas que no resultaron apropiadas ni suficientes, y que, según su propia manifestación inicial al contestar al requerimiento de la AEPD, el proceso de implantación de las medidas derivadas del análisis de riesgos realizado en su momento no estaba finalizado a la fecha del incidente**.**

TERCERO: Consta acreditado que la CEC comunicó a los afectados el incidente de seguridad mediante el envío de un SMS, y que los servicios informáticos de la Región de ******LOCALIDAD.1*** enviaron un correo electrónico a todos los docentes informándoles de lo sucedido. Además, se informó del incidente a los sindicatos y se publicó en el periódico "******PERIÓDICO.1***" de ******LOCALIDAD.1***.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido 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 adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento 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

Artículo 32 del RGPD

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".

De la instrucción llevada a cabo en el presente procedimiento se concluye que, en el momento de producirse la brecha, la CEC no contaba con las medidas adecuadas para impedir que se produjera un incidente como el que se examina en el presente expediente, ya que tal y como la propia CEC manifiesta, el origen de la brecha es debido a que el proceso de implantación de las medidas derivadas del análisis de riesgos realizado en su momento no estaba finalizado a la fecha del incidente.

III

Tipificación de la infracción del artículo 32 del RGPD

La infracción se tipifica en el artículo 83.4 del RGPD, que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *(…)*
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*
> *(…)*

IV

Sanción por la infracción del artículo 32 del RGPD

El artículo 83 apartado 7 del RGPD, dispone lo siguiente:

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58 apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *(…)*
> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
> *(…)*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
(…)

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a CONSEJERÍA DE EDUCACIÓN Y CULTURA, con NIF S3011001I, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a CONSEJERÍA DE EDUCACIÓN Y CULTURA.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-

administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-050522

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