- **Expediente N.º: PS/00442/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 03/06/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN con NIF S2801299E (en adelante, ANECA). Los motivos en que basa la reclamación son los siguientes:

-Que, de conformidad con lo establecido en la Resolución de 17 de diciembre de 2020 de la Secretaría General de Universidades, presentó a la ANECA solicitud de evaluación de su actividad investigadora.

-Que se le comunica el resultado de la Resolución del Pleno de la Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI), cuya valoración es negativa, y se adjunta como motivación de esta resolución el Informe del Comité Asesor, pero, en vez de facilitarle únicamente su informe, le trasladan un documento de 58 páginas en el que, además del suyo, aparecen 28 Informes más.

Junto a la reclamación, la parte reclamante no aportó ninguna prueba ni documento que justificase su reclamación, por lo que en fecha 24/06/2021, la Directora de la Agencia Española de Protección de Datos (en adelante, AEPD) inadmitió la reclamación.

SEGUNDO: Con fecha 12/07/2021, la parte reclamante presentó Recurso de Reposición contra la resolución de inadmisión, aportando con el mismo diversos informes emitidos por la ANECA a nombre de diferentes personas, así como un escrito firmado por la Jefa de la Unidad de Calidad en el que se reconoce el error cometido, y se comunica que han procedido a adoptar las medidas necesarias para garantizar que no se vuelva a producir un incidente similar.

TERCERO: Con fecha 18/08/2021 la Directora de la AEPD estima el Recurso de Reposición, siéndole notificado a la parte reclamante en fecha 30/08/2021

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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 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:

ANTECEDENTES

La presente investigación parte de la reclamación interpuesta el día 03 de junio de 2021 por ***A.A.A.*** (en adelante, parte reclamante), siendo como reclamado la AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN (en adelante, ANECA) y que dio lugar al procedimiento E/07213/2021.

Con fecha 4 de abril de 2022, en el marco del AI/00138/2022, se decide realizar requerimiento de información a la ANECA. En este requerimiento se solicita información marcada por la siguiente línea de investigación:

- Conocer detalles sobre la notificación del incidente de seguridad a todos los afectados.
- Conocer los detalles sobre el mencionado procedimiento interno de fuga de información.
- Conocer los detalles sobre la existencia de registro documental del incidente.
- Tener más información sobre la posible permanencia del informe erróneo en los expedientes de ANECA de las personas afectadas.

Con fecha 19 de abril de 2022, con entrada en registro REGAGE22e00013723923, se recibe respuesta a este requerimiento la cual es analizada en el apartado “resultado de las actuaciones de investigación”.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se ha investigado la siguiente entidad:

AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN con NIF S2801299E

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En relación con la respuesta recibida por parte de ANECA al requerimiento de información y que dio lugar a la entrada REGAGE22e00013723923, se concluye:

- ANECA confirma que sí envió notificación del incidente a los diferentes afectados con fecha 8 de junio de 2021 mediante correos electrónicos emitidos desde la cuenta ***cneai-comunicacion@aneca.es***. En este correo se le facilitó la siguiente información:
    1. Que durante el proceso de notificación de sexenios de investigación de la Convocatoria 2020, varios informes del Comité Asesor del campo 09 se generaron mal por la aplicación informática de ANECA llamada “Aplicación de gestión CNEAI”, y en vez de proporcionar la información de cada solicitud, en cada informe se incluyó la información de otras solicitudes negativas del campo 09, sin ningún tipo de error.
    2. Que en cuanto ANECA tuvo conocimiento de este hecho se pusieron en marcha todas las medidas técnicas y organizativas pertinentes para solucionarlo, siguiéndose los pasos marcados por el PROCEDIMIENTO INTERNO DE FUGA DE INFORMACIÓN en aras de garantizar la normativa de protección de datos, analizándose si se había producido brecha de seguridad que deba ser notificada a la AEPD y a las

personas afectadas, adoptándose las medidas adicionales para garantizar que no vuelva a darse un incidente similar.

- Se nos aporta el procedimiento interno de fuga de información, este procedimiento está marcado por una serie de fases a llevar a cabo para gestionar un incidente de seguridad, se resume a continuación el contenido de cada una de ellas:

  (…)

- Nos confirman que ANECA siguió el procedimiento de fuga de información anteriormente resumido.

- En relación con la descripción de los hechos nos aportan:

  1. Que para la convocatoria 2020 de Sexenios CNEAI se realizaron una serie de desarrollos para la aplicación web con la que se ha gestionado hasta ahora dicho procedimiento, llamada “Aplicación de gestión CNEAI”. Estos desarrollos principalmente consisten en integrar la antigua aplicación de evaluación de Sexenios con el sistema ACCEDA, de la Secretaría General de Administración Digital (SGAD). Para la comunicación de las resoluciones al ciudadano se implementó un proceso que notifica varios ficheros PDF a través de la plataforma ACCEDA, uno de estos ficheros con el resultado de la valoración. La generación de este documento como tal SI es un nuevo desarrollo. En caso de que la resolución fuese negativa se le envía también otro fichero con el informe del comité, conteniendo las observaciones de cada aportación, la generación de este documento NO es un nuevo desarrollo. La generación de estos ficheros debía ser única para cada solicitud, y se realizaron pruebas en un entorno de preproducción sin encontrar comportamientos extraños.
  2. Que el día 2 de junio realizaron una prueba con pocos expedientes en el entorno de producción y comprobaron que todo fue correcto.
  3. Que el mismo día 2 de junio, lanzaron el proceso para notificar las resoluciones del campo 09.
  4. Que para dicho campo existían 26 resoluciones negativas de 26 personas y que se ejecutó el código que generaba el informe del comité para cada solicitud (este código no formaba parte del nuevo desarrollo).
  5. Que el mismo día 2 de junio reciben correo electrónico por parte de una de las personas notificadas indicando el error en el fichero PDF recibido. Constatándose por ANECA el error en la generación del fichero para el campo 09, parándose de forma inmediata el proceso para el resto de los campos.
  6. Que el fichero generado contenía 29 informes que correspondían a 26 expedientes y a 26 afectados.
  7. Que buscaron forma alternativa de generar correctamente y de forma individualizada los informes procediéndose a su correcta notificación en torno a las 12:53 horas del mismo día. Se nos confirma que ANECA solucionó el incidente en el mismo día y que se han tomado las medidas técnicas para evitar que vuelva a suceder.

8. Que en ACCEDA se eliminaron los informes erróneos y se dejaron los correctos, no obstante, indican que en ACCEDA permanecen las primeras notificaciones erróneas realizadas con el fichero erróneo adjunto en cada notificación, que ANECA no tiene los roles adecuados en ACCEDA para eliminar esta información y que se solicitó con, fecha 4 de junio de 2021, al soporte técnico de ACCEDA su eliminación.
9. Que se utilizó la herramienta COMUNICA-BRECHA de esta Agencia para valorar la obligación de informar a las personas afectadas, teniéndose en cuenta la siguiente información:
    - Que los datos filtrados son datos identificativos (nombre, apellidos y NIF) así como datos de su situación profesional.
    - Que la brecha se detecta el 2 de junio de 2021.
    - Que el número de personas afectadas es reducido y que nunca había existido un incidente similar.
10. Indican que asumen el fallo cometido, pero que confían en los 26 destinatarios afectados en el sentido de que no harán mal uso de la información recibida, lo cual hace que las consecuencias del fallo no sean graves al eliminarse la probabilidad de riesgo. Por otro lado, indican que el impacto para las personas afectadas no es elevado, con inconvenientes fáciles de superar, como el propio malestar generado, por lo que concluyen que no hay alto riesgo para los derechos y libertades de los afectados.
11. Nos indican que no procede notificar la notificación de la brecha ante la AEPD porque entienden que es improbable que la brecha constituya un riesgo para los derechos y libertades de las personas afectadas. De la misma forma justifican que no hace falta notificar la brecha a las personas afectadas.
12. No obstante, en aras a la transparencia, indican que ANECA envió correo electrónico a los afectados explicando lo ocurrido, informando la solución de la incidencia e instándoles a que por favor eliminen los informes recibidos por error.
13. Indican que se ha procedido, por parte del DPD de ANECA, a documentar el incidente en el Registro de Brechas de ANECA, nos aportan copia de este registro y se contrasta que efectivamente aparece esta información.
14. Indican que, como medida de mejora principal, se determina que se debe ampliar el conjunto de datos de prueba para que cubran un mayor rango de posibilidades y casuísticas a probar, antes de su ejecución real.
15. Que en relación con las notificaciones erróneas que continúan estando accesibles en ACCEDA, en fecha 12 de agosto de 2021 recibieron respuesta por parte de la SGAD indicando que ACCEDA no presta el servicio de eliminar los procedimientos, expedientes y documentos, por lo que en el apartado notificaciones/comunicaciones seguirá figurando junto a la notificación realizada.

CONCLUSIONES

- ANECA asume el error que dio lugar a la reclamación, confirmando que se produjo por fallos en el módulo de la aplicación que generaba los ficheros, tras haberse subido previamente nuevas versiones de otros módulos del aplicativo

a producción, y habiéndose pasado una serie de pruebas anteriormente. Como medida de mejora asumen que se debe ampliar el rango de casuísticas de pruebas a realizar previamente a la puesta en producción, por lo que se deduce que las pruebas realizadas no fueron exhaustivas.

- No se procede a notificar ante la AEPD al considerarse que es improbable que exista riesgo para los derechos y libertades de las personas afectadas. De la misma forma, indican que no procede notificar a las personas afectadas, no obstante, envían correo a cada afectado con información de lo sucedido y la solución dada, este envío se realizó el 8 de junio de 2021.
- Los ficheros erróneos permanecen en ACCEDA. ANECA contactó con SGAD para proceder a su eliminación, pero contestaron que la plataforma no presta el servicio de eliminar los documentos por lo que en el apartado “notificaciones realizadas” siguen apareciendo.

CUARTO: Con fecha 19 de mayo 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 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD.

Notificado el acuerdo de inicio, ANECA presentó escrito de alegaciones en el que en síntesis manifestaba:

-Que ANECA aplicó las medidas técnicas que consideró pertinentes y adecuadas al riesgo, cumpliendo así con el artículo 32 del RGPD. De conformidad con ello, antes de proceder a la remisión de notificaciones con los informes de evaluación, se habían realizado pruebas en un entorno de preproducción sin encontrar comportamientos extraños. Que , entre las medidas técnicas tomadas, se hizo un chequeo previo para garantizar la seguridad de los datos y el buen funcionamiento de la nueva sede electrónica y de la nueva aplicación de evaluación se sexenios, no encontrándose funcionamiento anómalo alguno.

> A este respecto, esta Agencia considera que las medidas tomadas por ANECA no resultaron apropiadas para garantizar un nivel de seguridad adecuado al riesgo, tal como se establece en el artículo 32 del RGPD, puesto que, de hecho, ha quedado acreditado que los informes negativos obrantes en el campo 09 de la aplicación de gestión CNEAI, no se generaban de forma individual para cada solicitante, dando lugar al incidente sustanciado en el presente procedimiento sancionador.

-Que teniendo siempre presente garantizar la seguridad adecuada en el tratamiento de datos, como prescribe el artículo 5.1.f) del RGPD, y evaluando la adecuación de las medidas técnicas y organizativas a tomar para garantizar un nivel adecuado al riesgo del aseguramiento de los datos, como prescribe el artículo 32.1 del RGPD, se decidió realizar una primera notificación de resultados en un campo con pocas evaluaciones negativas, en concreto, el campo 09, del total de 14 campos científicos existentes, y que fue entonces cuando se produjo un fallo en la aplicación informática, no detectado previamente, y se enviaron los 26 ficheros a las 26 personas afectadas, hecho que se lamenta, como fue comunicado a dichas personas.

A este respecto, esta Agencia se remite a lo ya expuesto en relación a la alegación anterior, en el sentido de remarcar que las medidas no resultaron adecuadas. Cabe citar, asimismo, el considerando 28 del RGPD, según el cual:

> *"La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos."*

-Que ANECA considera que cumplió lo previsto en el artículo 33.1 del RGDP, en la medida en que realizó una evaluación de lo acontecido y consideró que era improbable que la violación de seguridad que había tenido lugar constituyera un riesgo para los derechos y libertades de las personas físicas afectadas, razón por la cual no se realizó la notificación a la AEPD, de conformidad con lo señalado en dicho precepto.
Para realizar dicha evaluación siguió los pasos que aparecen en su procedimiento interno, que recogen las recomendaciones que ha venido dando la propia AEPD, que señala que "*No es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas*".

A este respecto, y teniendo en cuenta que en el presente Procedimiento Sancionador no se ha imputado infracción por incumplimiento del artículo 33 del RGPD, esta agencia no tiene nada que añadir.

-Que al concluir que no era probable que la violación de seguridad producida constituyera un "ALTO" riesgo para los derechos y libertades de las personas físicas afectadas, ni tenían aquellas que realizar ninguna acción para protegerse o minimizar las consecuencias derivadas de la actuación de este Organismo, fue por lo que se afirma que no procedía llevar a cabo notificación a las mismas, tal y como establece el artículo 34 del RGPD. Y, no obstante, ANECA quiso ser transparente, dar explicaciones y pedir disculpas, y, aun considerando que no se encontraba incursa en la obligación de realizar la notificación de una brecha de datos personales a las personas afectadas, prefirió informar a todas ellas sobre lo sucedido y expresarles su malestar por lo ocurrido.

A este respecto, y teniendo en cuenta que en el presente Procedimiento Sancionador no se ha imputado infracción por incumplimiento del artículo 34 del RGPD, esta agencia no tiene nada que añadir.

Que deben tenerse en cuenta la existencia de elementos atenuantes, como son, la breve duración de la brecha, la rapidez con la que se detectaron y solucionaron los hechos, el pequeño número de personas afectadas y el nivel de los daños y perjuicios sufridos, así como las categorías de los datos de carácter personal que se vieron afectados, que no fueron en ningún caso datos sensibles, teniendo en cuenta el colectivo en cuestión. Igualmente afirma que no hubo ninguna intencionalidad por parte de ANECA, que tomó las medidas precisas que se consideraron pertinentes para

paliar los daños posibles, cumpliendo además con los pasos que establece la normativa en cuanto a cómo actuar ante una posible brecha de datos personales.
Asimismo, señala que no ha habido más casos y la aplicación “Gestión de CNEAI” funciona correctamente, no habiéndose tenido conocimiento de ninguna otra fuga ni reclamación en materia de protección de datos.

> A este respecto, esta Agencia señala que, a la hora de fijar la sanción correspondiente a las infracciones imputadas en un Procedimiento Sancionador, siempre se toman en consideración todos los factores concurrentes.

QUINTO: Con fecha 30 de junio de 2022 se formuló propuesta de resolución, proponiendo:

Que por la Directora de la Agencia Española de Protección de Datos se imponga a AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN, con NIF S2801299E, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

Que por la Directora de la Agencia Española de Protección de Datos se imponga a AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN, con NIF S2801299E, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD una sanción de apercibimiento.

SEXTO: Notificada la propuesta de resolución, ANECA presenta un nuevo escrito de alegaciones en fecha 20/07/2022, en el que principalmente reitera las ya presentadas al Acuerdo de Inicio y añaden que:

-No consideraron que fuera viable la aplicación, en este procedimiento de evaluación de sexenios, de medidas como la seudonimización a los datos personales, atendiendo no solo al contexto y finalidad del tratamiento sino además a los medios técnicos con los que se disponen en ese Organismo.

-Cabe asimismo indicar que el artículo 32 del RGPD también señala que entre las medidas a aplicar para la seguridad de los datos se encuentra la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, lo cual se ha demostrado que se dio en el presente caso, donde apenas en unas horas se solucionó el incidente técnico ocurrido.

-Unido a lo anterior, al evaluar el nivel de seguridad y las medidas tomadas para evitar riesgos en los desarrollos informáticos practicados que se han mencionado, es importante atender a que se trata de un colectivo no vulnerable sobre el que la Disposición adicional vigésima primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, establece que no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.

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 la parte reclamante presentó a la ANECA solicitud de evaluación de su actividad investigadora.

SEGUNDO: Consta acreditado que al comunicar a la parte reclamante el resultado de la Resolución del Pleno de la Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI), cuya valoración fue negativa, se adjuntó como motivación de esta resolución el Informe del Comité Asesor, un documento de 58 páginas en el que, además de su propio informe, aparecen 28 más correspondientes a diferentes personas.

TERCERO: Consta acreditado que durante el proceso de notificación de sexenios de investigación de la Convocatoria 2020, varios informes del Comité Asesor del campo 09, (resoluciones negativas), se generaron mal por la aplicación informática de ANECA llamada “Aplicación de gestión CNEAI”, y en vez de proporcionar la información de cada solicitud, en cada informe se incluyó la información de otras solicitudes negativas del campo 09.

FUNDAMENTOS DE DERECHO

I

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

En relación con las alegaciones presentadas a la propuesta de resolución, ANECA repite sustancialmente las ya presentadas al acuerdo de inicio, añadiendo que:

1-No se ha considerado por este Organismo que fuera viable la aplicación, en este procedimiento de evaluación de sexenios, de medidas como la seudonimización a los datos personales, atendiendo no solo al contexto y finalidad del tratamiento sino además a los medios técnicos con los que se disponen en este Organismo.
Pero cabe asi mismo indicar que el artículo 32 del RGPD también señala que entre las medidas a aplicar para la seguridad de los datos se encuentra la capacidad de

restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, lo cual se ha demostrado que se dio en el presente caso, donde apenas en unas horas se solucionó el incidente técnico ocurrido.

> -A este respecto esta agencia considera que, aun cuando el incidente se solucionara con rapidez, el envío de informes de resultado negativo ya se había efectuado, por lo que, aun cuando posteriormente se hayan tomado medidas que puedan resultar más eficientes, en el momento de producirse el incidente las medidas establecidas resultaron insuficientes, conforme a lo que establece el artículo 32 del RGPD.
>
> Asimismo, se indica que la seudonimización de datos es un ejemplo de medida tendente a evitar exposición de datos personales, que, efectivamente, cada responsable o encargado de datos debe valorar para su implementación, no pretendiendo esta agencia considerarlo impositivo, sino una mera indicación, y no basando en su ausencia el incumplimiento del articulo 32 RGPD, sino en la constatación de la insuficiencia de todas las medidas adoptadas.

2-Al evaluar el nivel de seguridad y las medidas tomadas para evitar riesgos en los desarrollos informáticos practicados que se han mencionado, es importante atender a que se trata de un colectivo no vulnerable sobre el que la Disposición adicional vigésima primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, establece que no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.

> -A este respecto esta agencia señala que, si bien la citada disposición adicional, en su punto 4 establece: *"Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación",* no cabe aplicarla al presente caso, dado que no se ha tratado de la publicación del RESULTADO de la actividad de la parte reclamante y resto de profesores, sino que lo que se ha enviado por correo electrónico a cada uno de ellos es el INFORME COMPLETO, con todos los datos, y no únicamente el resultado, positivo o negativo, del mismo, tanto propio como del resto de evaluados con carácter negativo, por lo que no puede tenerse en cuenta la citada disposición.

III

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) 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»).”

En el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos de la ANECA, fueron indebidamente expuestos a un tercero, ya que la parte reclamante ha aportado al expediente copia de informes emitidos a nombre de otras personas, que recibió junto con el suyo propio.

De la instrucción llevada a cabo en el presente procedimiento se concluye que ANECA ha vulnerado lo establecido en el artículo 5.1.f) del RGPD, al enviar conjuntamente a cada uno de los solicitantes los informes de 26 personas en los que constan los datos personales de cada una de ellas.

IV

El artículo 83.5 del RGPD, 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 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)”

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 72 “*Infracciones consideradas muy graves*” de la LOPDGDD indica:

“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)”

V

El articulo 83 apartado 7 del RGPD dispone lo siguiente:

“7. 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”.

Por su parte, 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. (…)"

VI

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, en el momento de producirse la brecha, la ANECA utilizaba una aplicación informática para la generación de informes que, en lugar de generar un informe por cada solicitud individual, generaba al mismo tiempo información correspondiente a otras solicitudes, poniendo de manifiesto, por tanto, datos personales de diversos solicitantes a cada uno de ellos, puesto que cada solicitante recibió, al mismo tiempo que su propio informe, el correspondiente al resto de solicitantes.

VII

El artículo 83.4 del RGPD, 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.*
> *(…)*

VIII

El articulo 83 apartado 7 del RGPD dispone lo siguiente:

"7. 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".

Por su parte, 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. (…)"

IX

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 AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN, con NIF S2801299E, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

IMPONER a AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN, con NIF S2801299E, 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 AGENCIA NACIONAL DE EVALUACIÓN DE LA CALIDAD Y ACREDITACIÓN.

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.

938-120722

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