- **Expediente N.º: EXP202307807**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 27 de abril de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra VICEPRESIDENCIA, CONSEJERÍA DE EDUCACIÓN Y UNIVERSIDADES DE LA COMUNIDAD DE MADRID con NIF S7800001E. Los motivos en que basa la reclamación son los siguientes:

La parte reclamante se inscribe en proceso de solicitud de beca para alumnos con discapacidad y al poco tiempo le envían un email con los plazos de apertura de la plataforma, filtrando las direcciones de email de todos los solicitantes de la beca en el campo "Para" en lugar de ponerlo en CCO.

Se adjunta a la reclamación el email.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la Consejería de Educación y Universidades de la Comunidad de Madrid, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 9 de junio de 2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 22 de junio de 2023 se recibe en esta Agencia escrito de respuesta indicando que, "*El correo referido por el reclamante fue enviado como recordatorio con el único propósito de que nuestros solicitantes no perdiesen la oportunidad de beneficiarse de esta beca y que, por un error humano y de manera excepcional, fue remitido a una pluralidad de solicitantes sin hacer uso de la funcionalidad de copia oculta (CCO). Además, procede indicar que, aun tratándose el correo electrónico de un dato personal protegido, ningún otro dato personal ha sido expuesto a terceros con la acción del envío referido*".

TERCERO: Con fecha 5 de julio de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 18 de octubre de 2023, 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 83.4 del RGPD y artículo 83.5 del RGPD. Dicho acuerdo de iniciación fue debidamente notificado en fecha 23/10/2023, como consta en el acuse de recibo que obra en el expediente.

QUINTO: El día 6/11/2024, se recibieron alegaciones frente al acuerdo de iniciación en las que, en síntesis, se exponía lo siguiente:

- La Consejería sostiene que el responsable del tratamiento de ese organismo, cumpliendo con las obligaciones que le marca el Reglamento General de Protección de Datos, realizó el oportuno análisis de riesgos del tratamiento de datos personales en enero de 2023, implantando las medidas oportunas resultantes de dicho análisis.

- En segundo lugar, la Consejería mantiene que al ser conocedora de las obligaciones legales que condicionan la gestión de datos personales de terceros ha seguido todas las instrucciones y recomendaciones derivadas de esta gestión, tramitando más de 6.000 solicitudes cada año, sin que de ello haya derivado ni una sola reclamación de este tipo.

- Otra de las alegaciones mantenida por el organismo responsable es que, con el fin de eliminar la puntual brecha de seguridad acaecida en la convocatoria de este año, ha implementado el envío de correos electrónicos automáticos mediante la herramienta informática de gestión de las becas de la Comunidad de Madrid y no mediante correos electrónicos desde Outlook, como hasta ahora se venía realizando.

SEXTO: Con fecha 13 de febrero de 2024 se formuló propuesta de resolución en la que se dio respuesta a todas las alegaciones planteadas y se propuso la declaración de infracción por incumplimiento de los artículos 5.1.f) y 32 del RGPD. La propuesta fue debidamente notificada en fecha 14/02/2024, como consta en el acuse de recibo que obra en el expediente.

Con respecto a la contestación a las alegaciones presentadas al acuerdo de inicio, la Agencia expuso en la propuesta de resolución:

- El hecho de haber realizado el análisis de riesgos del tratamiento de datos personales en enero de 2023 no impidió que se produjera la difusión de las direcciones de correo a terceros sin adoptar las medidas exigidas por la normativa en materia de protección de datos de carácter personal que garantizasen la confidencialidad de los mismos.

- No procede admitir como atenuante o como circunstancia que disminuya la gravedad, el hecho de que la Consejería haya seguido todas las instrucciones y recomendaciones derivadas de la gestión de datos personales, tramitando más de 6.000 solicitudes cada año, más bien al contrario, pues precisamente

por el elevado número de tratamientos que realiza y por afectar a datos personales relativos al estado físico, el organismo reclamado está obligada a actuar con la especial diligencia que debe exigirse a un organismo de estas características, que realiza numerosos tratamientos de datos personales de forma masiva, entre ellos categorías especiales de datos.

- En cuanto a la alegación sobre la implementación del envío de correos electrónicos automáticos mediante la herramienta informática de gestión de las becas de la Comunidad de Madrid y no mediante correos electrónicos desde Outlook, como hasta ahora se venía realizando, se señala que aunque esta Agencia valora positivamente la adopción de nuevas medidas que redunden en una mayor seguridad en lo que al tratamiento de datos personales se refiere y que puedan prevenir, en un futuro, incidentes como el que se sustancia en el presente procedimiento, las medidas de seguridad deben adoptarse en atención a todos y cada uno de los riesgos presentes en un tratamiento de datos de carácter personal, incluyendo entre los mismos, el factor humano.
  Los hechos probados en el procedimiento evidencian la divulgación de las direcciones de correo electrónico al ser remitido al reclamante un correo electrónico sin copia oculta con quebrantamiento de las medidas técnicas y organizativas y vulnerando la confidencialidad de los datos.

En consecuencia, la Agencia consideró que las alegaciones debían ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

SEPTIMO: En fecha 26/02/2024 se ha recibido en esta Agencia escrito de alegaciones a la propuesta de resolución en el que, en síntesis, reitera lo formulado en el escrito de alegaciones del 6/11/ 2023:

- La Consejería manifiesta que adoptó las medidas oportunas con el fin de eliminar la brecha de seguridad mencionada en el acuerdo de inicio de procedimiento sancionador.

- Desde el 8/11/2023, han implementado el envío de correos electrónicos automáticos mediante la herramienta informática de gestión de las becas de la Comunidad de Madrid y no mediante correos electrónicos desde Outlook, como habían venido realizando.

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: La parte reclamante se inscribe en la convocatoria “becas discapacidad 2022-2023” de la Dirección General de Universidades y Enseñanzas Artística de la Comunidad de Madrid.

SEGUNDO: El 27 de abril recibe un correo electrónico donde se recuerda que “el pasado 12 de abril se ha publicado la Convocatoria de Ayudas a Alumnos con discapacidad que cursan estudios universitarios o de enseñanzas artísticas superiores para el curso 2022-2023”.

TERCERO: Este correo fue enviado a todos los solicitantes de dicha beca sin la funcionalidad de “copia oculta”, quedando expuestas las direcciones de correo electrónico a todos los destinatarios.

## 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, 48.1, 64.2 y 68.1 de la 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
### Alegaciones a la Propuesta de Resolución

El 26/02/2024 se recibió escrito de alegaciones de la Consejería de Educación, Ciencia y Universidades, Dirección General de Universidades en el que, en síntesis, reitera lo manifestado en el escrito de alegaciones al acuerdo de inicio y expone que:

- Ese organismo adoptó las medidas oportunas con el fin de eliminar la brecha de seguridad mencionada en el acuerdo de inicio de procedimiento sancionador.

- Desde el 8/11/2023, han implementado el envío de correos electrónicos automáticos mediante la herramienta informática de gestión de las becas de la Comunidad de Madrid y no mediante correos electrónicos desde Outlook, como habían venido realizando.

Por lo tanto, la Agencia considera que las alegaciones deben ser desestimadas, significándose nuevamente que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

III
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 la Consejería de Educación y Universidades de la Comunidad de Madrid realiza la utilización de datos personales, tal como la dirección de correo electrónico de las personas que pueden acceder a la convocatoria de becas discapacidad 2022-2023.

La Consejería de Educación y Universidades de la Comunidad de Madrid 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 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, consecuencia del envío de un correo electrónico sin copia oculta, siendo accesibles las direcciones de correo electrónico correspondientes.

IV
Artículo 5.1.f) del RGPD

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 destinatarios del correo electrónico que ha motivado la reclamación, obrantes en la base de datos de la Consejería de Educación y Universidades de la Comunidad de Madrid, fueron indebidamente expuestos a terceros con el envío de un correo electrónico sin copia oculta, siendo accesibles sus respectivas direcciones de correo electrónico para todos los destinatarios.

De conformidad con las evidencias de las que se dispone en el presente momento de resolución del procedimiento sancionador se considera que la Consejería de Educación y Universidades de la Comunidad de Madrid ha tratado datos personales de la parte reclamante, en concreto la dirección de correo electrónico, sin adoptar las medidas técnicas y organizativas apropiadas exigidas por la normativa en materia de protección de datos de carácter personal que garantizasen la confidencialidad de los

mismos y por tanto este hecho se considera constitutivo de una infracción por vulneración del artículo 5.1.f) del RGPD.

V
Tipificación de la infracción del artículo 5.1.f) del RGPD

El artículo 83.5.a) del RGPD tipifica como infracción administrativa cualquier vulneración de *"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. (…)"*

VI
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 resiliencias 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 accesos 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".*

A pesar de que la Consejería de Educación y Universidades de la Comunidad de Madrid había realizado un análisis de riesgos, no se garantizaba un nivel de seguridad adecuado al riesgo que permitiera la confidencialidad, integridad y disponibilidad de los servicios del tratamiento, máxime cuando se estaban tratando categorías especiales de datos.

De conformidad con las evidencias de las que se dispone en este momento de resolución del procedimiento sancionador se considera que los hechos conocidos son constitutivos de una infracción, imputable a la Consejería de Educación y Universidades de la Comunidad de Madrid, por vulneración del artículo 32 del RGPD.

## VII
## Tipificación de la infracción del artículo 32 del RGPD

El artículo 83.4.a) del RGPD tipifica como infracción administrativa cualquier vulneración de *"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
Sanción por las infracciones de los artículos 5.1.f) y 32 del RGPD

El Artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD apartado 7 establece:

*"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 declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*
*La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.*

*3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.*
*Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.*

*4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.*

*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.*

*6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.*
*Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".*

Este precepto excluye la imposición de multas administrativas cuando las infracciones a las que se refieren los artículos 72 a 74 de la LOPDGDD se cometan por las categorías de responsables o encargados del tratamiento enumerados en el apartado 1 del citado artículo 77, estableciéndose que los procedimientos que tengan causa en vulneraciones de la normativa de protección de datos personales cometidas por aquellas entidades se resuelvan declarando las infracciones.

## IX
## Adopción de medidas

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

La parte reclamada en su respuesta de fecha 26/02/2024 ha señalado que el 8/11/2023 ha quedado totalmente implementada la medida por la cual el envío de correos electrónicos automáticos se realiza mediante la herramienta informática de gestión de las becas de la Comunidad de Madrid y no mediante correos electrónicos desde Outlook, como habían venido realizando, lo cual garantiza que se han tomado las acciones necesarias para eliminar posibles brechas de seguridad como la que ha motivado el inicio de este expediente.

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: DECLARAR que VICEPRESIDENCIA, CONSEJERÍA DE EDUCACIÓN Y UNIVERSIDADES, con NIF S7800001E, ha infringido lo dispuesto en el artículo 5.1.f) del RGPD y artículo 32 del RGPD, infracción tipificada en el artículo 83.4 del RGPD y artículo 83.5 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a VICEPRESIDENCIA, CONSEJERÍA DE EDUCACIÓN Y UNIVERSIDADES.

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.

938-16012024

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