- Expediente N.º: EXP202213770

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante el reclamante) con fecha 19/11/2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la UNIVERSIDAD DE VALLADOLID con NIF ***Q4718001C*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: el reclamante manifiesta que participó en una convocatoria de plazas ofertadas por el reclamado, aportando para ello extensa documentación con sus datos personales, si bien tuvo noticia de que existió una impugnación de un participante en la convocatoria, que solicitó documentación presentada al proceso por el resto de candidatos, siendo facilitada esta por el reclamado sin acometer las debidas medidas de seguridad que garantizaran la confidencialidad de datos sobre los que el recurrente de la convocatoria no cuenta con interés legítimo. Señala que el reclamado le remitió copia de la solicitud realizada por el recurrente, incluyendo el Código de Verificación del Documento (C.V.D.), además de códigos de barras y QRS que permiten el pleno acceso a los documentos originales sin censurar.

Aporta copia de su solicitud de participación en la convocatoria, extracto de la reclamación presentada por el recurrente en la convocatoria, reclamación planteada por el reclamante ante el reclamado y copia de la solicitud del recurrente en el proceso selectivo.

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), el 30/12/2022 se dio traslado de dicha reclamación a la parte reclamada, 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 04/01/2023 como consta en el acuse de recibo que obra en el expediente.

El DPD mediante escrito de 31/01/2023 respondía que analizada la incidencia había solicitado información y que vista la información aportada se habían constatado una serie de riesgos.
En su Guía de Privacidad desde el Diseño la Agencia Española de Protección de Datos recomendaba disponer de estrategias de diseño de la privacidad, una de las cuales *“ocultar”* sin duda debió haberse aplicado correctamente.
Se había oficiado instrucciones a los Órganos de gobierno y Servicios administrativos correspondientes.

En lo que respecta a la petición de la AEPD de identificar nominalmente a la autoridad o directivo responsable del tratamiento en el momento de la emisión de los informes técnicos y recomendaciones, la opinión del delegado es que debe diferenciarse entre la responsabilidad jurídica y la relativa a la gestión.
En cuanto a la primera, la Secretaria General tiene delegadas las competencias en dirección de la política de protección de datos en la Universidad.
Sin embargo, las tareas de tratamiento de la información objeto de la reclamación han sido efectuadas por el Servicio de Profesorado.

TERCERO: Con fecha 19/02/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por el reclamante.

CUARTO: Con fecha 10/07/2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por las presuntas infracciones de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en el artículo 83.5.a) y 83.4.a) del RGPD.

QUINTO: Notificado el acuerdo de inicio en fecha 24/07/2023, la parte reclamada presentó escrito de alegaciones formulando en síntesis lo siguiente: que como consecuencia del requerimiento de la AEPD de 30/12/2022, analizada y comprobada la incidencia producida, se emitió informe de 28/01/2023 analizando los riesgos existentes en el proceso de anonimización y se proponía una estrategia de diseño incorporando medidas para evitas situaciones como la producida. Entre estas medidas destacaba la *Propuesta de instrucciones para la gestión de procesos selectivos en los que se trate documentación curricular que contenga datos personales.* El 31/01/2023 el reclamado dio respuesta al citado requerimiento dando traslado de los informes del DPD e informes técnicos y propuestas de actuación; como medida de remedio se contemplaba que el documento anterior fuera puesto en conocimiento del Servicio correspondiente. Se realizaron reuniones de trabajo y el documento fue mejorado y completado resultando el documento *Instrucciones para la gestión de procesos selectivos en los que se trate documentación curricular que contenga datos personales* de 07/02/2023. El DPD señalaba que el uso de los sistemas de verificación de los documentos administrativos basados en códigos que se utilizan en las Administraciones públicas españolas suponen un riesgo para la privacidad de los interesados al proporcionar estos sistemas la descarga del documento original y que para ofrecer una copia anonimizada a quienes soliciten el acceso al expediente, se requeriría la eliminación, precisamente, del único elemento que permite verificar su autenticidad, así el acceso a la documentación presentada, encontraría una barrera para quien solicita ese acceso a la información pública, al no poder verificar la autenticidad del documento. Que para dar cumplimiento al derecho a acceder y obtener copia de los documentos contenidos en el procedimiento selectivo de referencia, se facilitó la documentación pedida por el solicitante en el convencimiento de que esta comunicación quedaba amparada por la LPACAP y que, no obstante, con el fin de mitigar el riesgo y salvaguardar el derecho fundamental a la protección de datos el reclamado ha optado por exigir el enmascaramiento del número de validación de cada documento emitido electrónicamente. Asimismo, alerta que el riesgo detectado por el reclamado en lo relativo al uso de los sistemas de verificación documental se esté produciendo en el conjunto de las Administraciones Publicas por lo que solicita a la AEPD una Auditoría de Oficio y dicte instrucciones para que se pueda adoptar en el conjunto de las Administraciones.

SEXTO: Con fecha 27/09/2023 se acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

> Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento.
>
> Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por el reclamado, y la documentación que a ellas acompaña.

SEPTIMO: Con fecha 24/05/2024 fue emitida Propuesta de Resolución en el sentido de que por la Directoria de la AEPD se declarara que la parte reclamada había infringido los artículos 5.1.f) y 32.1 del RGPD, infracciones tipificadas en los artículos 83.5.a) y 83.4.a) del citado RGPD.

Con fecha 06/06/2024 la parte reclamada presento escrito de alegaciones manifestando, en síntesis: que, de acuerdo con la documentación que fue facilitada, en la ofuscación de los campos se había evidenciado una mala aplicación de la medida de seguridad debido a un error material y que se han adoptado una serie de medidas dirigidas a la reparación del daño y a la mejora de los procedimientos para evitar e incidencias similares.

OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes,

HECHOS PROBADOS

PRIMERO. Con fecha 19/11/2022 tiene entrada en la AEPD escrito de la parte reclamante en la que manifiesta que concurrió a una oferta de empleo público convocada mediante Concurso nº ***XXXX/XX***, plazas ofertadas por la parte reclamada, aportando documentación conteniendo datos de carácter personal; posteriormente tuvo noticias de que existió impugnación por uno de los participantes en la convocatoria, solicitando la documentación presentada al proceso por el resto de candidatos, siendo facilitada por la parte reclamada sin acometer las debidas medidas de seguridad que garantizaran la confidencialidad de los datos; asimismo, señala que la parte reclamada le remitió copia de la solicitud llevada a cabo por el tercero impugnante, incluyendo el Código de Verificación del Documento (C.V.D.), además de los códigos de barras y QRS que permiten el pleno acceso a los documentos originales sin censurar.

SEGUNDO. Consta aportado Extracto de la Resolución del Rectorado de la Universidad, de ***FECHA.1, por la que se convoca Concurso Nº ***XXXX/XX*** para la Provisión de plazas de Cuerpos Docentes Universitarios, en régimen de interinidad y de personal docente investigador contratado en régimen de Derecho Laboral, en la que participa del reclamante.

TERCERO. Consta aportada por el reclamante su solicitud de participación en el Concurso Nº XXXX/XX para la provisión de plazas de cuerpos docenes universitarios.

CUARTO**.** Consta aportado el escrito dirigido por la parte reclamante a la parte reclamada en relación con el recurso presentado por el participante impugnante en el concurso contra la Propuesta de Provisión realizada por la Comisión de Selección del Concurso nº ***XXXX/XX***, señalando la posible infracción de la legislación en materia de protección de datos y solicitando el acceso a la información solicitada por el impugnante, la documentación aportada por él, la documentación que le fue remitida, detalle del procedimiento, modo de tratamiento y condiciones en las que se produjo dicha cesión de datos.

QUINTO. Consta copia de la reclamación presentada por el participante impugnante contra la Propuesta de Provisión realizada por la Comisión de Selección del Concurso nº ***XXXX/XX***, que motivo que la parte reclamada le proporcionara el acceso a la documentación presentada al concurso por el resto de los candidatos.

SEXTO. Consta aportado el formulario donde figuran los datos personales de la parte reclamante, enviado al resto de candidatos a la plaza a concurso y los formularios con los datos personales del resto de candidatos de las plazas a concurso, remitidos al reclamante con los datos personales de sus firmantes.

SEPTIMO. Consta aportado formato de remisión de reclamaciones en procesos selectivos de la parte reclamada, con datos personales censurados, manteniendo los códigos seguros de verificación sin censurar y formato de remisión de reclamaciones en procesos selectivos del reclamado al que se accede a través del CVD, con los datos personales sin censurar.

OCTAVO. La parte reclamada en escrito de 24/07/2023 señalaba:
"(…)
A partir de la información obtenida, el DPD verificó que, si bien se habían ocultado los datos personales en el expediente del reclamante con carácter previo a su cesión, esta ofuscación no había alcanzado a los códigos seguros de verificación y QR que permiten comprobar la autenticidad de los documentos administrativos en las plataformas habilitadas al efecto por las Administraciones públicas.
(…)"

NOVENO. La parte reclamada su escrito de 31/01/2023 ha manifestado:
"(…)
Segundo. - Vista la información aportada por los correspondientes servicios de la UVa, el delegado constató los siguientes riesgos:
(…)
b) En el expediente facilitado al concursante se han ocultado la mayoría de los datos personales, aunque alguno de ellos ha permanecido visible. No se han suprimido los códigos QR o códigos seguros de verificación que permiten asegurar la autenticidad de los documentos emitidos por las Administraciones públicas. Se observa un posible error humano a la hora de censurar la información de manera manual debido al elevado volumen.

c) Existiría un riesgo de acceso a datos personales debido a la obligación de publicidad
de los códigos seguros de verificación prevista en el art. 27.3 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
Este riesgo afectaría no solo a la UVa, sino a todas las Administraciones públicas.
Se proponen una serie de medidas mitigadoras para estos riesgos.
(…)
Cuarto. - En su Guía de Privacidad desde el Diseño la Agencia Española de Protección de Datos recomienda disponer de estrategias de diseño de la privacidad, una de las cuales "ocultar" sin duda debió haberse aplicado correctamente. La ejecución de esta estrategia requiere de un "patrón de diseño", cuya propuesta se adjunta a este documento para la consideración del responsable del tratamiento como "PROPUESTA DE INSTRUCCIONES PARA LA GESTIÓN DE PROCESOS SELECTIVOS EN LOS QUE SE TRATE DOCUMENTACIÓN CURRICULAR QUE CONTENGA DATOS PERSONALES". Este protocolo de actuación aborda una gestión integral de la información desde el diseño de su recogida, hasta su eventual entrega en el marco del ejercicio de un derecho de acceso a la información pública. Se recomienda su implantación a mayor brevedad. Del mismo modo, se propone que desde las unidades administrativas encargadas de los procesos selectivos se haga un seguimiento de su despliegue para comprobar su efectividad"
(…)".

DECIMO. Consta aportada *"Propuesta de instrucciones para la gestión de procesos selectivos en los que se trate documentación curricular que contenga datos personales"* para una gestión integral de la información objeto de tratamiento.

UNDECIMO. Consta aportado Informe Análisis de Riesgos, considerándolos adecuados y proporcionados a la actividad, naturaleza y recursos disponibles de la parte reclamada.

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 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

Primera obligación incumplida: infracción del artículo 5.1.f) del RGPD

Hay que señalar que la parte reclamada lleva a cabo el tratamiento de datos de carácter personal, toda vez que realiza, de conformidad con lo señalado en el artículo 4.2 del RGPD, entre otros, la recogida, el registro, la conservación, de datos personales, preferentemente de alumnos, exalumnos, personal docente, investigadores, etc.

La parte reclamada realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y los medios relacionados con el tratamiento de los datos de carácter personal, en virtud del artículo 4.7 del RGPD.

Además, el responsable del tratamiento se debe encargar también de aplicar las medidas técnicas y organizativas que garanticen la seguridad de los datos personales al llevar a cabo el tratamiento. Y ser capaz de demostrar el cumplimiento RGPD y de la LOPDGDD.

Los hechos denunciados se materializan en el acceso a los datos de carácter personal por un tercero que impugnó la convocatoria de un proceso selectivo en el que también participaba la parte reclamada, que había solicitado se le aportara la documentación presentada por el resto de los candidatos a dicho proceso, siendo facilitada por la parte reclamada con ausencia de medidas técnicas y organizativas apropiadas que garantizaran un nivel de seguridad y confidencialidad de datos, lo que vulneraria la normativa en materia de protección de datos de carácter personal.

El artículo 58 del RGPD, *Poderes*, establece en su apartado 2:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

(…)"

El tratamiento llevado a cabo podría ser constitutivo de una infracción del artículo 5, *Principios relativos al tratamiento,* del RGPD que establece que:

"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»).

(…)"

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al permitir el acceso a los datos de carácter personal del reclamante (y del resto de participantes), al ser facilitados a uno de los participantes que impugnó la convocatoria donde participaba, infringiendo la confidencialidad e integridad de los mismos.

En este sentido, el citado art. 5.1.f) del RGPD, prevé que los datos personales serán tratados de tal manera que se garantice su seguridad, 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.

También el considerando 39 del RGPD, en clara referencia al principio recogido en el artículo 5.1.f) del RGPD, dispone 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".*

Y es que la pérdida de confidencialidad supone un riesgo, que puede conllevar daños y perjuicios, materiales o inmateriales para las personas físicas (considerando 85 del RGPD). En tal sentido, el considerando 75 del RGPD establece que: *"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; …"*

Por tanto, el acceso no autorizado a los datos de carácter personal supone que éstos puedan ser utilizados para usos no conocidos, incluso fraudulentos, conllevando una pérdida total y absoluta de control sobre los mismos. Debe tenerse en cuenta además que la mayoría de los datos personales filtrados son datos que no pueden ser modificados o cambiados por otros (nombre, apellidos, DNI, domicilio…).

En este mismo sentido, el artículo 28 de la LOPDGDD, y respecto de las obligaciones del responsable del tratamiento en el marco de los artículos 24 y 25 del RGPD para garantizar y acreditar que el tratamiento es conforme al RGPD respecto de diversos riesgos, dispone que,

"(…)

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional,

reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados. …".

Y la Sentencia del Tribunal Constitucional (STC) 292/2000 en el FD séptimo, señala: *"… resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular."*

Hay que señalar que la propia parte reclamada en escrito de fecha 31/01/2023 ha manifestado que:

"(…)

a) El sistema de acceso a ficheros no permite la trazabilidad del acceso a la información y el acuse de recibo.

b) En el expediente facilitado al concursante se han ocultado la mayoría de los datos personales, aunque alguno de ellos ha permanecido visible. No se han suprimido los códigos QR o códigos seguros de verificación que permiten asegurar la autenticidad
de los documentos emitidos por las Administraciones públicas. Se observa un posible error humano a la hora de censurar la información de manera manual debido al elevado volumen.

c) Existiría un riesgo de acceso a datos personales debido a la obligación de publicidad de los códigos seguros de verificación prevista en el art. 27.3 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Este riesgo afectaría no solo a la UVa, sino a todas las Administraciones públicas.

(…)" (El subrayado corresponde a la AEPD).

Y también en escrito de 24/07/2023 ha manifestado que:

"Segundo. - A partir de la información obtenida, el DPD verificó que, si bien se habían ocultado los datos personales en el expediente del reclamante con carácter previo a su cesión, esta ofuscación no había alcanzado a los códigos seguros de verificación y QR que permiten comprobar la autenticidad de los documentos administrativos en las plataformas habilitadas al efecto por las Administraciones públicas.

Una vez comprobada la existencia del error material debido a la falta de la ocultación de los códigos seguros de verificación y QR, el DPD emitió el informe N. REF. UVA/01/2023 (2), de 28 de enero de 2023, en el que se analizaban los riesgos existentes en el proceso de anonimización y se proponía una estrategia de diseño de la privacidad que incorporaba una serie medidas de remedio para evitar que la situación se reproduzca en el futuro".

Por otro lado, la parte reclamante aporta la reclamación presentada por el tercero participante en el Concurso contra la Propuesta de Provisión, instrumento a través del cual la parte reclamada le proporcionó la documentación presentada a concurso por el resto de los candidatos, entre ellos el de la parte reclamante, donde figuran sus datos de carácter personal.

E igualmente aporta el formulario donde figuran los datos personales de la parte reclamante, que fue enviado sin censurar al resto de candidatos a la plaza a concurso y los formularios con los datos personales del resto de candidatos de las plazas a concurso, remitidos al reclamante con los datos personales de sus firmantes.

Por tanto, esta conducta supone la vulneración del principio de integridad y confidencialidad de los datos de conformidad con lo establecido en el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.5 del RGPD.

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

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable .

Por su parte, la LOPDGDD en su artículo 71, *Infracciones,* señala 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".*

También la LOPDGDD, a efectos de prescripción, en su artículo 72 indica: *"Infracciones consideradas muy graves:*

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.
(…)"

IV
Segunda obligación incumplida: infracción del artículo 32.1 del RGPD

También se le atribuye al reclamado la infracción del artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

El RGPD define las violaciones a la seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

La documentación obrante en el expediente evidencia la vulneración del artículo 32.1 del RGPD, como consecuencia de la falta de medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado al riesgo del tratamiento.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el

cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad al riesgo se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En el presente caso, se evidencia que las medidas de seguridad que la parte reclamada tenía implantadas en relación con los datos que sometía a tratamiento no eran apropiadas ni adecuadas para garantizar la seguridad de los datos personales en el momento de producirse los tratamientos.

Como señala igualmente el Considerando 39:

"…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 el presente caso, tal y como consta en los hechos probados la parte reclamada remitió copia de la solicitud realizada por uno de los participantes que impugnó la propuesta de provisión realizada por la Comisión de Selección del Concurso, incluyendo el Código de Verificación del Documento (C.V.D.), además de códigos de barras y QRS que permitían el pleno acceso a los documentos originales sin censurar. Además, algunos datos permanecían visibles y sin ocultar.

La parte reclamada ha confirmado el incidente provocado y, además, señalaba que *"En su Guía de Privacidad desde el Diseño la Agencia Española de Protección de Datos recomienda disponer de estrategias de diseño de la privacidad, una de las cuales "ocultar" sin duda debió haberse aplicado correctamente".*

Hay que señalar que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos ya que no es posible asegurar el citado derecho si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo que sean adecuadas.

En el Informe de fecha 05/01/2023 aportado por el DPD señalaba que: "*Con fecha 17 de agosto de 2022* el participante impugnante *presentó escrito en el que solicitaba «copia electrónica de toda la documentación que obre en el expediente relativo a las plazas PAYUD K070K06/RP06017 y PAYUD K070K06/RP06018 de dicho concurso; en concreto la documentación presentada por el resto de aspirantes, la baremación detallada de todos los candidatos conforme a los criterios específicos del concurso y las actas de las reuniones de la comisión, a efectos de poder formular las reclamaciones que estime pertinentes". Dicha petición, conforme a los artículos 13.d) y 53.1.a) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, fue atendida y el día siguiente, mediante correo electrónico en el que se adjuntaba un oficio de la Jefa de Sección de Acceso PDI Laboral del Servicio de Gestión de Profesorado, se ponía a su disposición la documentación censurada presentada por el resto de aspirantes a dichas plazas, en cuanto aspirante al proceso selectivo, por tener un interés propio, directo y legítimo en conocer el contenido de los expedientes del procedimiento administrativo.*

Con fecha 30 de agosto de 2022 el participante impugnante *presentó escrito de reclamación contra a propuesta de provisión de la Comisión de Selección, acorde a lo establecido en la base 7.5 de la correspondiente convocatoria, para su valoración por parte de la comisión de reclamaciones.*

Posteriormente, se dio traslado de dicha reclamación a los demás participantes en el procedimiento, a efectos de la defensa de sus derechos y, en respuesta el reclamante presento escrito señalando que la cesión al tercero de documentación conteniendo sus datos de carácter personal podría vulnerar la legislación en materia de protección de datos, por lo que solicitaba el acceso a la solicitud de aquel y a la documentación que le fue remitida y que contuviese información aportada al expediente por la parte reclamante, detalle del procedimiento, modo de tratamiento y condiciones en las que se produjo dicha cesión de datos, así como el traslado de la reclamación al DPD.

Asimismo, se señala en el citado Informe que: *El proceso de censura realizado en los documentos enviados a los interesados (número de folios censuradas 1.067) se realiza por el personal del servicio de forma manual y a la mayor rapidez posible para atender las peticiones, toda vez que los interesados lo necesitan para poder defender sus derechos en la reclamación que presenten. Para la presentación de dichas reclamaciones tienen los interesados un plazo de 10 días".*

En este sentido, relacionado con el proceso de censura se recomendaba *"Es obligación de la administración dimensionar los medios disponibles a las necesidades del servicio. Y es evidente que la gestión del riesgo obliga a disponer de personal suficiente y formado para la anonimización parcial de documentos en el marco de la*

gestión de concursos en los que, como es el caso, la decisión recae esencialmente en un proceso de baremación entre candidaturas que presentan un volumen significativo de méritos".

Para finalizar, en relación con la omisión del traslado del escrito del reclamante al Delegado de Protección de Datos y al Responsable de privacidad señalaba que "*ha sido obviada al venir incorporada en el trámite de alegaciones solicitado al interesado y del que se incorporó al oportuno expediente de reclamación ante la Comisión de Reclamaciones sin advertir dicha petición ni por parte del personal del Servicio ni de los miembros de dicha Comisión. Omisión que en ningún momento fue con intención de eludir dicha petición)".*

Asimismo, en el escrito de fecha 31/01/2023 la parte reclamada manifiesta que "*en el expediente facilitado al concursante se han ocultado la mayoría de los datos personales, aunque alguno de ellos ha permanecido visible. No se han suprimido los códigos QR o códigos seguros de verificación que permiten asegurar la autenticidad de los documentos emitidos por las Administraciones públicas. Se observa un posible error humano a la hora de censurar la información de manera manual debido al elevado volumen.*

Hay que señalar que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos ya que no es posible asegurar el citado derecho si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo que sean adecuadas.

La adecuación del nivel de seguridad al riesgo debe ser evaluada por el responsable y reconsiderada periódicamente en función de los resultados obtenidos, teniendo en cuenta para ello -entre otros factores- los riesgos que pueda presentar el tratamiento como consecuencia de la comunicación no autorizada de dichos datos. Las medidas técnicas y organizativas de seguridad que deben de aplicarse son las pertinentes para responder al riesgo existente, valorando, entre otros factores, el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento y los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Uno de los requerimientos que establece el RGPD para responsables y encargados del tratamiento que realizan actividades de tratamiento con datos personales es la necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información con el fin de establecer las medidas de seguridad y control orientadas a cumplir los principios de protección desde el diseño y por defecto que garanticen los derechos y libertades de las personas.

La responsabilidad de la parte reclamante viene determinada por la falta de medidas técnicas y organizativas idóneas y necesarias puestas de manifiesto, ya que es responsable de tomar decisiones destinadas a implantar de manera efectiva las medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. En este sentido, las medidas no eran apropiadas.

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32.1, infracción tipificada en su artículo 83.4.a) del RGPD.

V
Tipificación de la infracción del artículo 32.1 del RGPD

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.
(…)"

Por su parte, la LOPDGDD en su artículo 71, *Infracciones,* señala 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".*

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

"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.
(…)"

VI
Régimen aplicable a las infracciones cometidas

El artículo 83 *"Condiciones generales para la imposición de multas administrativas"* del RGPD en su 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*."

También la LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento,* establece lo siguiente:

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

(…)
i) Las Universidades Públicas.
(…)

"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".

En el caso examinado, el presente procedimiento sancionador tiene su causa, tal y como se expone en los hechos, de la vulneración de la normativa en materia de protección de datos de carácter personal, tanto del principio de confidencialidad de los datos como las medidas técnicas y organizativas implantadas.

De conformidad con las evidencias de las que se dispone, dicha conducta constituye, por parte de la parte reclamada la infracción a lo dispuesto en los artículos 5.1.f) y 32.1 del RGPD.

Hay que señalar que el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de declarar la infracción y establecer las medidas que proceda para corregir los tratamientos de datos personales que no se adecúen a sus previsiones, 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.

Adicionalmente, el artículo 58 del RGPD, en su apartado 2 d) que cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".*

No obstante, hay que resaltar que la parte reclamada ha manifestado que, una vez analizado el incidente, había adoptado medidas para evitar que incidentes como el que ha dado lugar al presente procedimiento se vuelva a producir, adjuntando el *documento "PROPUESTA DE INSTRUCCIONES PARA LA GESTIÓN DE PROCESOS SELECTIVOS EN LOS QUE SE TRATE DOCUMENTACIÓN CURRICULAR QUE CONTENGA DATOS PERSONALES"*.

Así en el escrito dando respuesta al requerimiento de la Agencia señalaba que:

"Este protocolo de actuación aborda una gestión integral de la información desde el diseño de su recogida, hasta su eventual entrega en el marco del ejercicio de un derecho de acceso a la información pública. Se recomienda su implantación a mayor brevedad. Del mismo modo, se propone que desde las unidades administrativas encargadas de los procesos selectivos se haga un seguimiento de su despliegue para comprobar su efectividad.

• *La "PROPUESTA DE INSTRUCCIONES PARA LA GESTIÓN DE PROCESOS SELECTIVOS EN LOS QUE SE TRATE DOCUMENTACIÓN CURRICULAR QUE CONTENGA DATOS PERSONALES",* consta aportada por la parte reclamada a la AEPD.

Quinto. - Se han oficiado distintas instrucciones a los Órganos de gobierno y Servicios administrativos correspondientes, como puede observarse en los siguientes anexos:

- *Oficio adopción instrucciones ocultación datos. Se da traslado de las instrucciones sobre anonimización en procesos selectivos a todas los Servicios encargados de su gestión y al órgano encargado de resolver las solicitudes de acceso a la información pública.*
- *Oficio Comité Seguridad de la Información. Se le encarga la verificación, seguimiento y remedio del incidente de seguridad que afecta a la confidencialidad del uso de códigos seguros de verificación.*
- *Oficio responsables de la Sede electrónica. Se solicita a los desarrolladores conocer los fundamentos jurídicos utilizados para la especificación de requisitos del software de Sede Electrónica y tener en cuenta las recomendaciones del delegado de protección de datos para el desarrollo futuro del aplicativo".*

Por último, en relación con lo señalado por la parte reclamada en su escrito de alegaciones al Acuerdo de inicio: *"El riesgo detectado derivado del uso de los sistemas de verificación documental de las Administraciones públicas, el cual, tal y como se ha comprobado, la Universidad de Valladolid no había tenido en cuenta, puede estar produciéndose de manera generalizada en el conjunto de la Administración, por lo que nos gustaría aprovechar estas alegaciones para solicitar a la Agencia Española de Protección de Datos que se inicie una auditoría de oficio para verificar cuál es la práctica administrativa común en estas situaciones y que dicte instrucciones precisas que puedan ser adoptadas por el conjunto de las Administraciones públicas",* se informa a la parte reclamada que este organismo ha tomado debida nota de lo señalado y ha trasladado a la División de Innovación Tecnológica para su análisis y actuación a los efectos que se estimen oportunos.

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 la UNIVERSIDAD DE VALLADOLID, con NIF ***Q4718001C,*** ha infringido lo dispuesto en el artículo 5.1.f) del RGPD y el artículo 32.1 del RGPD, infracciones tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a la UNIVERSIDAD DE VALLADOLID.

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.

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