- **Expediente N.º: EXP202105669**

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, la parte reclamante), en fecha 8 de noviembre de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE, con NIF S5011001D, (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

El reclamante expone que la Dirección General de Gestión de Personal del departamento en el que presta servicios (Educación, Cultura y Deporte) remitió, en fecha 28 de septiembre de 2021, un correo electrónico en el que se adjuntaba una hoja Excel con los datos de más de 200 empleados dando a conocer a terceros, sus nombres y apellidos, DNI, puesto de trabajo y una celda adicional para indicar si deseaban realizar un reconocimiento médico, sin el consentimiento expreso de los titulares de dichos datos.

En fecha 30 de septiembre de 2021, el reclamante remitió un correo electrónico a la Unidad de Protección de Datos del Gobierno de Aragón comunicando la incidencia.

En fecha 19 de octubre de 2021, dicha Unidad de Protección de Datos puso en conocimiento del reclamante que se había comunicado a dicho departamento la necesidad de llevar a cabo medidas técnicas y organizativas que impidan el acceso de terceros a datos personales, tanto identificativos como de categoría especial.

Junto a la reclamación aporta correo electrónico enviado en fecha 28 de septiembre de 2021, la hoja Excel en la que se pueden visualizar datos personales de más de 200 empleados (entre ellos los del propio reclamante) y el correo electrónico comunicando la incidencia y su respuesta.

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 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) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada

conforme a lo previsto en el art. 43.2 de la LPACAP, en fecha 3 de enero de 2022, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 20 de enero de 2022. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: En fecha 8 de febrero de 2022, de conformidad con el artículo 65 de la LOPDGDD, se comunicó la admisión a trámite de la reclamación presentada por la parte reclamante.

CUARTO: En fecha 7 de julio de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción de los artículos 5.1.f) y 32 del RGPD, tipificados en los artículos 83.5 y 83.4 del RGPD, respectivamente.

El acuerdo de inicio fue notificado, 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), en fecha 26 de julio de 2022, como consta en el certificado que obra en el expediente.

QUINTO: Notificado el citado acuerdo de inicio 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), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que solicitado informe a la Dirección General de Personal, este indica que la remisión se realizó a las cuentas de correo corporativas de cada organismo, las cuales son atendidas únicamente por los secretarios/as de alto cargos que hay en cada una de ellas, que se desconoce si, por su parte, se reenvió la tabla al resto de trabajadores de cada organismo o si, como parece más adecuado, fueron los titulares de cada secretaría las que consultaron personalmente a cada compañero sobre sus preferencias para la realización del reconocimiento médico.

Asimismo, manifiesta que el denunciante no recibió en su cuenta de correo electrónico corporativo personal de empleado público el listado, sino que tuvo acceso a él a través de la cuenta corporativa de la Dirección General a la que está adscrito. Esto es, la Dirección General de Personal no difundió los datos de los empleados del departamento en correo masivo dirigido a todos ellos, sino que solicitó a las personas que ocupan las secretarías de los altos cargos del departamento (las Direcciones Generales) que recabaran el consentimiento al reconocimiento médico, dando por hecho que a esa tabla sólo tendrían acceso las personas que tienen acceso a esas cuentas corporativas y lo tienen en ejercicio de las funciones que les son propias.

Por último añade que se va a requerir a la Dirección General de Personal que impulse la revisión de la adecuación del procedimiento que trae causa de la denuncia a la normativa vigente en la materia (recabar el consentimiento de los empleados públicos a la realización de la revisión médica a la que tienen derecho), para lo que se le remitirá al Delegado de Protección de Datos de este departamento, a fin de que les asesore en esa revisión y que se adopten las medidas que, en su caso, sean precisas, además de aquellas que ya están implantadas en esta Administración.

SEXTO: En fecha 19 de agosto de 2022, se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se imponga al DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE, con NIF S5011001D, por una infracción del artículo 5.1.f) del RGPD, tipificado en el artículo 83.5 del RGPD, una sanción de apercibimiento y por una infracción del artículo 32 del RGPD, tipificado en el artículo 83.4 el RGPD, una sanción de apercibimiento.>>

La citada propuesta de resolución fue enviada, 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), mediante notificación electrónica, siendo recibida en fecha 22 de agosto de 2022, como consta en el certificado que obra en el expediente.

SÉPTIMO: La parte reclamada no ha presentado alegaciones a la Propuesta de Resolución.

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 que en fecha 8 de noviembre de 2021, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, toda vez que la parte reclamada ha revelado información y datos de carácter personal a terceros, sin el consentimiento expreso de los titulares de dichos datos.

SEGUNDO: Se verifica que se trata de un correo electrónico en el que se adjunta una hoja Excel en la que se pueden visualizar los datos de más de 200 empleados dando a conocer a terceros, sus nombres y apellidos, DNI, puesto de trabajo y una celda adicional para indicar si deseaban realizar un reconocimiento médico.

TERCERO: La parte reclamada expone que procederá a la revisión de la adecuación del procedimiento a la normativa vigente en la materia.

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, 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

En respuesta a las alegaciones presentadas por la entidad reclamada se debe señalar lo siguiente:

En primer lugar, la documentación obrante en el expediente acredita que la parte reclamada, desde la dirección de correo electrónico: ******EMAIL.1*** remitió un correo electrónico a la SGT y Direcciones Generales, en el que se adjuntaba una hoja Excel donde se podían visualizar el nombre, apellidos, DNI, puesto de trabajo de más de 200 empleados públicos y una celda adicional para indicar si deseaban realizar un reconocimiento médico.

La reclamada ha alegado que la remisión se realizó a las cuentas de correo corporativas de cada organismo, las cuales son atendidas únicamente por los secretarios/as de altos cargos que hay en cada una de ellas. Sin embargo, lo que ocurre en este caso no se ajusta a dicho esquema, por cuanto la información relativa al reclamante no se remite únicamente a su unidad, sino que el listado completo de todos los departamentos con el nombre, apellidos, DNI, puesto de trabajo de más de 200 empleados públicos, estaba al alcance de todos los departamentos destinatarios de dicho correo. De haberse establecido unas mínimas medidas de seguridad en el envío del listado, habría podido remitirse a cada unidad únicamente los datos de personal adscrito a cada una de ellas. Sin embargo, se remitió el listado completo a todas. Con ello, aun admitiendo la posibilidad de que el acceso al buzón corporativo de cada dirección general estuviera restringido, lo cierto es que se revelaban a todas las unidades los datos personales del personal no adscrito a ellas. Asimismo, el correo electrónico en cuestión, a su vez, arrastra debajo, el que la DG Personal recibió para que se realizara la recolección de información. Pues bien, ni uno ni otro contienen indicaciones de precauciones dirigidas a los destinatarios para que la recogida de datos se recogiera con la máxima confidencialidad, lo que apunta a falta de medidas de seguridad.

En este sentido, si bien el correo electrónico es una herramienta de comunicación corporativa que facilita y agiliza el funcionamiento en una empresa**,** a pesar de sus grandes beneficios como la accesibilidad, rapidez y la posibilidad de adjuntar archivos, se hace necesario definir un uso correcto y seguro**,** toda vez que, en algunas ocasiones, los empleados/as pueden enviar documentos confidenciales a quien no debían por error, o bien desvelar datos personales. En este sentido es muy importante concienciar al personal, a los usuarios/as del correo corporativo de las amenazas y dotarles de las herramientas adecuadas para que hagan un uso seguro del mismo.

En el caso concreto que se examina, en relación con la categoría de datos a la que terceros han tenido acceso, sobre la posibilidad de combinación de informaciones referidas a un titular de datos personales, se puede traer a colación el Dictamen 4/2007 del Grupo de Trabajo del Articulo 29, "*Sobre el concepto de datos personales*" que analiza las posibilidades de identificar a alguien a través de combinaciones con otras informaciones, partiendo únicamente de los datos básicos y combinándola con otra.

En concreto indica lo siguiente: (…) *cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean estas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual presidente del Gobierno de España»), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuesto a evitar cualquier quebrantamiento de la confidencialidad* (…). *Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones.* (…)

En este caso la búsqueda en internet, por ejemplo, del nombre, apellidos de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento que, en función de este, debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

En consecuencia, las alegaciones deben 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.

III
Cuestiones previas

El Departamento de Educación Cultura y Deporte del Gobierno de Aragón, como cualquier otra entidad pública, está obligado al cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos -RGPD-, y de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales -LOPDGDD- con respecto a los tratamientos de datos de carácter personal que realicen, entendiendo por dato de carácter personal, *"toda información sobre una persona física identificada o identificable*".

Se considera persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Asimismo, debe entenderse por tratamiento "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

Teniendo en cuenta lo anterior, el Departamento de Educación Cultura y Deporte presta una serie de servicios públicos, para los cuales trata datos de carácter personal de sus empleados y ciudadanos.

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:

«responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.*

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, toda vez que la parte reclamada ha revelado información y datos de carácter personal a terceros, sin el consentimiento expreso del titular de dichos datos, al adjuntar al correo electrónico una hoja Excel donde consta el nombre, apellidos, DNI, puesto de trabajo de más de 200 empleados públicos y una celda adicional para indicar si deseaban realizar el reconocimiento médico.

Este tipo de datos, así como cualquier otra información que se encuentre referida a personas físicas, tienen la consideración de dato de carácter personal, por lo que su tratamiento está sujeto a la normativa de protección de datos.

Según el GT29 se produce una "Violación de la confidencialidad" cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en el artículo 32 del RGPD, que reglamenta la seguridad del tratamiento.

IV

Artículo 5.1.f) del RGPD

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

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 relación con este principio, el Considerando 39 del referido RGPD señala 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".

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado vulneró el artículo 5.1 f) del RGPD, *principios relativos al tratamiento.*

En el caso presente, según documentación aportada por el reclamante y a falta de contestación de la parte reclamada, se puede constatar que, desde la dirección de correo electrónico: ******EMAIL.1*** se ha enviado un correo electrónico en el que se adjunta una hoja Excel en la que se pueden visualizar el nombre, apellidos, DNI, puesto de trabajo de más de 200 empleados públicos y una celda adicional para indicar si deseaban realizar un reconocimiento médico.

Los hechos acreditados constituyen, por parte del reclamado, en su condición de responsable del reseñado tratamiento de datos personales, una vulneración del

principio de confidencialidad, al difundir esa información entre los empleados sin constar que hubiera obtenido el consentimiento de estos para ese especifico tratamiento.

En consecuencia, se considera que los hechos acreditados son constitutivos de infracción, imputable a la parte reclamada, por vulneración del artículo 5.1.f) del RGPD.

V

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

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 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. (…)"*

VI

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

"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".

Los hechos puestos de manifiesto suponen la falta de medidas técnicas y organizativas al posibilitar la exhibición de datos de carácter personal del reclamante con la consiguiente falta de diligencia por el responsable, permitiendo el acceso no autorizado por terceros ajenos.

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 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".

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"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; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En este sentido, la búsqueda en internet, por ejemplo, del nombre, apellidos, DNI o correo electrónico de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas 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. Asimismo, deberá conocer los principales riesgos a los que está expuesto el correo corporativo toda vez que el acceso privilegiado al entorno del correo suele estar restringido a varias personas del área técnica correspondiente, por lo que las acciones de dichos accesos deben ser convenientemente trazadas para detectar cualquier situación anómala, en especial aquellas que puedan implicar pérdidas de confidencialidad.

Por tanto, los hechos acreditados son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

VII
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

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

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

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

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

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

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

VIII
Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

IX
Sanción

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."*

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

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

(…)

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

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

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.

(…)

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."

En el presente caso se estima adecuado sancionar con apercibimiento a la parte reclamada, por infracción del artículo 5.1.f) del RGPD y por la infracción del artículo 32 del RGPD, por la falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad.

X
Medidas

El artículo 58.2 del RGPD dispone*: "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;"

Asimismo, procede imponer la medida correctiva descrita en el artículo 58.2.d) del RGPD y ordenar a la parte reclamada que, en el plazo de un mes, establezca las medidas de seguridad adecuadas para que se adecúen los tratamientos a las exigencias contempladas en los artículos 5.1 f) y 32 del RGPD, impidiendo que se produzcan situaciones similares en el futuro.

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.

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: SANCIONAR con APERCIBIMIENTO al DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE, con NIF S5011001D, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: SANCIONAR con APERCIBIMIENTO al DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE, con NIF S5011001D, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

TERCERO: REQUERIR al DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE, que implante, en el plazo de un mes, las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares, así como que informe a esta Agencia en el mismo plazo sobre las medidas adoptadas.

CUARTO: NOTIFICAR la presente resolución al DEPARTAMENTO DE EDUCACIÓN, CULTURA Y DEPORTE.

QUINTO: 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.

938-181022

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