

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Dña. **A.A.A.** (en adelante, la reclamante) con fecha 25/11/2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA con NIF **Q2826000H** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: la reclamante considera que la reclamada ha vulnerado la normativa en materia de protección de datos de carácter personal al remitir sus datos fiscales (declaración de la renta del año 2019) a un tercero sin que conste que ostenta su representación.

El 14/10/22 la afectada se dirigió a la reclamada mediante escrito indicándole que su liquidación tributaria había sido remitida incorrectamente a su sobrino, con el que no mantiene relación alguna, no siendo su representante.

El 17/10/22 el tercero notificado por la reclamada presentó escrito en el que informaba que no representa a la reclamante.

El 28/10/22 la reclamada remitió una notificación a la reclamante, donde se indicaban los antecedentes y se acordaba la rectificación del acto administrativo tratado, de manera que se anulaba la liquidación objeto de impugnación y se anulaba el expediente sancionador asociado al mismo.

Junto a la reclamación se aportan copia de los documentos anteriores.

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 30/01/2023 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 30/01/2023 como consta en el acuse de recibo que obra en el expediente.

TERCERO: Con fecha 25/02/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 19/04/2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por las presuntas infracciones de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a)

y 83.4.a) del RGPD, sancionando con apercibimiento conforme a lo dispuesto en el artículo 77 de la LOPDGDD.

QUINTO: Notificado el acuerdo de inicio, el reclamado en fecha 03/05/2023 presentó escrito de alegaciones manifestando, en síntesis: aseguramiento de la seguridad del sistema de notificaciones y comunicaciones: que el error cometido se produjo en un momento anterior a la notificación cuando se dio de alta en el registro de sucesores; protocolo de alta den el registro de sucesores: describe el reclamado el incidente producido y como todo fue debido a un error humano puntual y que en cuanto a las medidas de seguridad vienen establecidas de acuerdo con los análisis de riesgos realizados y acordes al riesgo detectado; admisión a trámite de la reclamación: no se entiende por qué se admitió a trámite cuando aún no se había recibido respuesta por parte de la AEAT y aún estaba dentro de plazo para el envío de dicha respuesta; que los errores humanos puntuales no pueden controlarse.

SEXTO: Con fecha 23/05/2023 se inició 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 por los Servicios de Inspección que forman parte del expediente.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que a ellas acompaña.

SEPTIMO: Con fecha 11/07/2023 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancionara al reclamado por infracción de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del citado RGPD, con sendos apercibimientos.

Con fecha 24/07/2023 el reclamado presento escrito de alegaciones manifestando, en síntesis: que el RGPD no exige la seguridad absoluta sino que se apliquen las medias apropiadas que garanticen un nivel de seguridad adecuado; que el reclamado cuenta con análisis de riesgo que son revisados y actualizados constantemente; que en cuanto se tuvo conocimiento del error se acuto con la máxima diligencia dando de baja la relación; que el incidente se debió a un error humano y no a la falta de diligencia en las medidas implantadas considerando necesario incidir en la concienciación para evitar este tipo de errores.

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

#### HECHOS PROBADOS

PRIMERO. La reclamante mediante escrito de 25/11/2022 interpuso reclamación ante el reclamado, manifestado que la entidad reclamada ha vulnerado la normativa en materia de protección de datos de carácter personal al remitir sus datos fiscales (declaración de la renta del año 2019) a un tercero y sobrino de la reclamante sin que conste que ostenta su representación.

SEGUNDO. Consta aportado escrito de D. **B.B.B.**, sobrino de la reclamante, de 03/10/2022 dirigido al reclamado en el que le informa haber recibido notificación *tramite de alegaciones y propuesta de liquidación provisional* en concepto de IRPF 2019, en calidad de representante de la reclamante en la que se contienen datos de carácter personal y adjunta la notificación por dicho concepto tributario.

TERCERO. La reclamante aporta copia del escrito remitido al reclamado el 14/10/2022 en el que informa de los hechos sometidos al conocimiento de la AEPD, sin que según la afectada haya habido respuesta del reclamado.

CUARTO. Consta Acuerdo de iniciación y comunicación del trámite de audiencia de expediente sancionador motivado por no haber respondido a la propuesta de liquidación provisional en concepto de IRPF 2019, que fue remitida a D. **B.B.B.**.

QUINTO. Consta aportada *Acuerdo de Resolución de Rectificación de Errores* de 28/10/2022 en cuya parte resolutive se señala que la notificación efectuada fue cursada erróneamente a otro contribuyente en calidad de representante de la reclamante por lo que se procedía a la anulación de la notificación, se rectificaban el acto de la notificación, se anulaba la liquidación provisional y el procedimiento sancionador.

SEXTO. El reclamado en escrito de 03/03/2023 ha manifestado que *"En el momento de enviar la información a la que hace referencia la reclamante ("Nota informativa" que contenía la "Notificación del trámite de alegaciones y propuesta de liquidación provisional"), el tercero involucrado (...) constaba como sucesor de la reclamante en el registro de sucesores de la Agencia Tributaria, de manera, tal y como establece la normativa, le fue enviada la documentación a dicho sucesor"*.

## 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

Los hechos denunciados se concretan en la notificación llevada a cabo por el reclamado dirigida a un tercero dándole traslado de documentación fiscal correspondiente a la reclamante sin que conste autorización o consentimiento alguno ni que ostenta su representación.

El artículo 58 del RGPD, *Poderes*, señala:

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

*(...)*

*b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;*

*(...)*

*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;*

*(...)”*

### III

El tratamiento llevado a cabo es constitutivo de 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»).*

*(...)”*

### IV

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 otro lado, 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.*

*(...)”*

## V

1. La documentación obrante en el expediente evidencia que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al permitir el acceso a los datos carácter personal por un tercero al que le fue notificada liquidación tributaria de la reclamante sin que conste que ostentara su representación, ni que constara su autorización para ello.

El deber de confidencialidad debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

Por tanto, ese deber es una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional.

2. El reclamado ha reconocido que *“En el momento de enviar la información a la que hace referencia la reclamante (“Nota informativa” que contenía la “Notificación del trámite de alegaciones y propuesta de liquidación provisional”), el tercero involucrado (B.B.B.) constaba como sucesor de la reclamante en el registro de sucesores de la Agencia Tributaria, de manera, tal y como establece la normativa, le fue enviada la documentación a dicho sucesor.*

Que *“El 17 de octubre de 2022, entró por registro de la Agencia Tributaria, el escrito del tercero involucrado (B.B.B.), donde indica que no representaba a la reclamante. Tras analizar los hechos y las posibles causas del error, el día 18 de octubre de 2022, se subsanó el registro de sucesores.*

*El error se había debido a que, ..., se había dado de alta en el registro de sucesores, siguiendo el protocolo interno, la relación entre el tercero involucrado y la reclamante (tía del tercero involucrado), en lugar de entre el tercero involucrado y la madre fallecida de la reclamante (C.C.C., abuela del tercero involucrado), al confundir el DNI de la madre fallecida con el de la hija.*

*El tercero involucrado era nieto de la fallecida y sucesor de la misma, puesto que el padre del tercero involucrado e hijo de la fallecida también había fallecido”.*

Y que *“Aunque no puede controlarse un error humano puntual, se prevé enviar un recordatorio sobre el protocolo de alta en el registro de sucesores, haciendo hincapié en el cotejo y revisión de toda la información incluida antes de dar el alta”.*

La actuación del reclamado evidencia la vulneración del principio de confidencialidad, de conformidad con lo establecido en el artículo 5.1.f), infracción tipificada en el artículo 83.5.a) del citado Reglamento.

## VI

En segundo lugar, se 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”.*

## VII

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:*

*(...)*

*g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679”.*

*(...)”*

## VIII

1. El RGPD define las violaciones de seguridad de los datos personales 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”*.

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad, con vulneración de las medidas de carácter técnico y organizativas.

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”.*

2. En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación la AEPD trasladó al reclamado el 31/01/2023 la reclamación presentada para que procediese a su análisis e informase a esta Agencia de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos; aunque el reclamado manifestaba en escrito de alegaciones al acuerdo de inicio de 03/05/2023 no entender por qué se admitió a trámite la reclamación cuando aún no se había recibido respuesta por parte de la AEAT, lo cierto es que la misma fue recibida fuera del plazo establecido, el 03/03/2023.

Como consta en el Antecedente tercero, la reclamación fue admitida el 25/02/2023, transcurrido el plazo de respuesta y de conformidad con el artículo 65 de la LOPDGDD.

Por otra parte, en el citado escrito el reclamado manifestaba que se habían revisado los hechos ocurridos y que la notificación enviada atendía a la normativa establecida, ya que el envío se realizó a una persona que constaba como sucesor en el registro de sucesores y, aunque todo se había debido a un error humano puntual, el cambio en el registro de sucesores en el momento en el que se tiene conocimiento del mismo también es el adecuado.

Ahora bien, el propio reclamado continúa señalando que *“El error se había debido a que, ..., se había dado de alta en el registro de sucesores, siguiendo el protocolo interno, la relación entre el tercero involucrado y la reclamante (tía del tercero involucrado), en lugar de entre el tercero involucrado y la madre fallecida de la reclamante (... , abuela del tercero involucrado), al confundir el DNI de la madre fallecida con el de la hija.*

*El tercero involucrado era nieto de la fallecida y sucesor de la misma, puesto que el padre del tercero involucrado e hijo de la fallecida también había fallecido (...).”*

Asimismo, el reclamado ha manifestado que prevé enviar un recordatorio sobre el protocolo de alta en el registro de sucesores, haciendo hincapié en el cotejo y revisión de toda la información incluida antes de dar el alta.

En alegaciones a la Propuesta el reclamado ha aportado un Recordatorio de las consideraciones a tener en cuenta para evitar incidencias cuando se procede al



alta en el Registro de Sucesores con las pautas a seguir antes de proceder al alta en el Registro.

Por otra parte, hay que señalar que la responsabilidad del reclamado viene determinada al no haberse adoptado medidas que eviten errores como el producido, ya que es el responsable de tomar decisiones destinadas a implementar y adecuar de manera efectiva las medidas técnicas y organizativas apropiadas a fin de 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.

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

## IX

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:*

- a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
- b) Los órganos jurisdiccionales.*
- c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
- d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
- e) Las autoridades administrativas independientes.*
- f) El Banco de España.*
- g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*
- h) Las fundaciones del sector público.*
- i) Las Universidades Públicas.*
- j) Los consorcios.*
- k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.*

*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.*

*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”.*

*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 trae causa de que el reclamado, como consta en los hechos probados, ha vulnerado la normativa en materia de protección de datos de carácter personal tanto del principio de confidencialidad de los datos como las medidas de seguridad implantadas.

Dicha conducta constituye, por parte del reclamado, 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 acudir a la sanción de apercibimiento 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, contempla 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, el reclamado ha señalado que cuenta con análisis de riesgo TI que son revisados actualizados constantemente; que las medidas técnicas y organizativas a aplicar son el resultado de planes de proyectos anuales, los cuales se nutren, tanto del resultado del análisis y gestión de riesgos TI especificado, como de los Mapas de Riesgos de la organización, normativa aplicable, así como de proyectos que se vea necesario abordar.

Y que si bien la incidencia fue debida a un error humano considera necesario incidir en la concienciación para mitigar y evitar en lo posible los mismos, aportando como se ha señalado *Recordatorio de las consideraciones a tener en cuenta para evitar incidencias en el alta del Registro de Sucesores* con las pautas a seguir antes de proceder al alta en el Registro.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

La Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: IMPONER a la AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA, con NIF **Q2826000H**, por infracciones de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, con sanción de apercibimiento para cada una de ellas.

SEGUNDO: NOTIFICAR la presente resolución a la AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA.

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