- Expediente N.º: EXP202207643

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 parte reclamante) con fecha 31/05/2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la TESORERIA GENERAL DE LA SEGURIDAD SOCIAL, con NIF ***Q2827003A*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: la reclamante manifiesta que una trabajadora que presta servicios para la parte reclamada ha efectuado accesos indebidos a sus datos personales con ánimo de perjudicarla; señala que el 03/05/2022 solicitó la apertura de una investigación al respecto; el 27/05/2022 la Inspección de Servicios del reclamado comunicó a la reclamante que habían detectado varias consultas no justificadas realizadas el 23/03/2022, razón por la cual se ha iniciado una averiguación interna para esclarecer los hechos.

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 12/07/2022 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 13/07/2022 como consta en el acuse de recibo que obra en el expediente.

TERCERO: El 10/08/2022 tras el análisis de la documentación obrante en el expediente se dictó resolución por la Directora de la Agencia Española de Protección de Datos, acordando la no admisión a trámite de la reclamación.

La resolución fue notificada a la reclamante el 10/08/2022, según consta acreditado en el expediente.

CUARTO: El 09/09/2022 la reclamante interpuso recurso potestativo de reposición contra la resolución recaída en el expediente, en el que mostraba su disconformidad con la misma, solicitando la admisión a trámite la reclamación inicialmente presentada.

El 10/04/2023 se remitió el recurso interpuesto a la reclamada en el marco de lo establecido en el artículo 118.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) a los efectos de que formulase alegaciones y presentase los documentos y justificantes que

estimase procedentes, lo que se ha verificado mediante escrito de respuesta de 20/04/2023.

El reclamado reiteró la información aportada con anterioridad confirmando los accesos no justificado a los datos de la recurrente

QUINTO: El 10/05/2023 por la Directoria de la Agencia resolvía ESTIMAR el recurso de reposición interpuesto contra la resolución de esta Agencia dictada en fecha 10/08/2022 y, admitir a trámite la reclamación formulada de acuerdo con lo establecido en el artículo 65 de la LOPDGDD.

SEXTO: Con fecha 05/07/2023, 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 el artículo 83.5.a) y 83.4.a) del RGPD.

SEPTIMO: Notificado el acuerdo de inicio en fecha 05/07/2023, el reclamado no presentó escrito de alegaciones al citado acuerdo.

OCTAVO: Con fecha fue emitida Propuesta de Resolución en el sentido de que por la Directora de la AEPD se declarara la infracción por el reclamado de los artículos 5.1.f) y 32.1 del RGPD, tipificados en los artículos 83.5.a) y 83.4.a) del RGPD.

En fecha 04/09/2023 el reclamado presento escrito de alegaciones a la Propuesta de Resolución manifestando, en síntesis, lo siguiente: las dificultades técnicas a la hora de realizar envíos y comunicaciones con la AEPD a través de su Registro electrónico; disculpas por el error cometido en el envío de 17/07/2023 relativo a la documentación que formaban parte de las alegaciones al acuerdo de inicio olvidando, por error, anexar el oficio de alegaciones firmado por el Secretario General de la TSGG; que se reitera en las alegaciones de 14/07/2023 y la documentación de 17/07/2023 y, además, que al contrario de lo señalado en la Propuesta "*la situación acontecida no es imputable a un tercero, sino que constituye una conducta irregular imputable a una empleada de esta Entidad*" y que *"no cabe apreciar la existencia de una brecha de seguridad ya que no estamos ante un error o fallo generalizado de nuestro sistema de seguridad, sino ante un uso indebido e impredecible por parte de una funcionaria de unas transacciones a cuyo acceso estaba autorizada para el desempeño de sus funciones profesionales"* y que en relación con lo señalado en el oficio de 14/07/2023 que hubo *"acuerdo de 22/06/2022 de incoación de expediente disciplinario contra la funcionaria implicada, si bien fue suspendido a expensas del fallo judicial (Diligencias Previas Nº XXXXXX/2022 incoadas por el Juzgado de Instrucción (...)de Valencia), al tener por objeto ambos procedimientos los mismos hechos".*

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

HECHOS PROBADOS

PRIMERO. Con fecha 31/05/2022 tiene entrad en la AEPD escrito de la reclamante en la que manifiesta que se ha accedido a su expediente personal por parte de una funcionaria del reclamado usando sus datos de carácter personal para una finalidad

distinta de su actividad laboral; (…); todos estos hechos han sido puestos en conocimiento del reclamado y ha solicitado que se protejan sus datos ante su situación de vulnerabilidad, que además constata que ha habido consultas a su expediente no justificadas.

SEGUNDO. El 10/08/2022 se dictó resolución acordando la no admisión a trámite de la reclamación.

TERCERO. El 09/09/2022 la reclamante interpuso recurso potestativo de reposición mostrando su disconformidad con la resolución recaída, solicitando la admisión a trámite la reclamación inicialmente presentada. En el curso del mismo el reclamado en alegaciones durante el trámite de audiencia reiteraba la información aportada con anterioridad confirmando los accesos no justificados a los datos personales de la reclamante.

CUARTO. El 10/05/2023 por la Directoria de la Agencia resolvía estimar el recurso de reposición interpuesto, admitiendo a trámite la reclamación formulada.

QUINTO. Consta aportado por la reclamante *Formulario de Solicitud de Ejercicio de Derechos* en solicitud del derecho de acceso a sus datos de carácter personal ante el reclamado, de fecha 03/05/2022, consecuencia de los hechos expuestos con anterioridad.

SEXTO. Consta *Oficio* de respuesta del reclamado de fecha 25/05/2022 en el que se señala *"En respuesta a su escrito de 3 de mayo de 2022, por el que solicitó apertura de investigación sobre posibles accesos, sin su consentimiento, a sus datos personales, esta Inspección de Servicios de la Tesorería General de la Seguridad Social (TGSS) le informa que dentro de la cadena de rastros se han detectado varias consultas no justificadas a sus datos realizadas en la Dirección provincial de Valencia con fecha 23 de marzo de 2022. Por este motivo, le comunicamos que desde esta unidad comenzaremos a realizar las actuaciones vía interna que procedan en relación con el personal investigado.*
(…)".

SEPTIMO. Consta aportada *Nota Interior* del reclamado con destino la *Secretaria general, Subdirección General Adjunta, Unidad de Régimen Disciplinario*, *Expte.* ******EXPEDIENTE.1***, de fecha 02/06/2022 en el que se señala lo siguiente: *"(…) El pasado 26 de mayo la Directora provincial de Valencia nos envió diferente documentación, entre la que se incluye un oficio de la Dirección provincial confirmando la existencia de los rastros detectados e indicando las funciones de la trabajadora, y una declaración de la funcionaria, en la que alega no haber realizado ningún acceso a datos personales más allá de los necesarios para las tareas que le competen.*
Después de analizar todos los documentos, desde esta unidad no se puede considerar suficiente para justificar las consultas efectuadas por los siguientes motivos:
- En primer lugar, hay que tener en cuenta la particularidad de este caso, puesto que la denunciante se encuentra inmersa en un procedimiento judicial en curso y, asimismo, esta persona tenía una relación de parentesco por afinidad con la denunciada.

- Por otro lado, en la documentación enviada por la D.P. de Valencia no se hace mención a ningún expediente concreto en el que se fundamenten los accesos realizados por esta funcionaria, y además las fechas de los mismos no coinciden con un periodo de actividad de la denunciante, que en ese momento se encontraba en situación de desempleo.
(…)"

OCTAVO. Con fecha registro de entrada 22/06/2022, consta requerimiento del Juzgado de Instrucción nº XX de Valencia procedimiento Diligencias Previas nº XXXXXX/2022 en el que se indica que *"dirijo a Vd. el presente a fin de que respecto al expediente* ******EXPEDIENTE.1*** *apertura en esa Inspección, intereso remitan informe e identificación de las consultas no justificadas a los datos personales de* la reclamante"

NOVENO. En su respuesta al Juzgado, de fecha 23/06/2022, el reclamado señala que:
"(…)
Tras analizar la documentación enviada, desde esta unidad no se ha podido considerar justificados estos accesos en base a los siguientes motivos:
No se ha aportado ningún expediente administrativo relacionado con la denunciante en el que se pueda fundamentar estos accesos.
Además, tras analizar nuestros ficheros, se ha comprobado que en la fecha en la que se realizan dichos accesos, la Sra. ***A.A.A.*** *se encontraba en situación de desempleo, por lo que una consulta a su perfil en el fichero de afiliación hecha en ese momento desde la Tesorería General no es posible vincularla con una finalidad profesional (aunque debe señalarse también que no es infrecuente que usuarios autorizados accedan de buena fe a nuestros sistemas y faciliten datos a terceros que los han solicitado verbalmente)".*

E identifica el usuario que efectuó las consultas a los datos personales de la reclamante, así como día y hora de las mismas.

DECIMO. Consta aportado por el reclamado la respuesta ofrecida al requerimiento de la AEPD en el que reitera lo ya expuesto en los escritos anteriores.

UNDECIMO. El reclamado en escrito de 17/07/2023 ha aportado copia de *Circular sobre la regulación y desarrollo de los controles y auditorías sobre accesos a los ficheros y bases de datos informáticos gestionados por la Tesorería General de la Seguridad Social; Política de uso seguro de los sistemas de información de la Seguridad Social; Gestión de incidentes de seguridad; Gestión de acceso y autorizaciones* e *Informe del Director Provincial de Valencia.* En este informe se advierte a la funcionaria de su conducta irregular y de la iniciación de expediente disciplinario.

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 materializan en los accesos no justificados a los datos de carácter personal de la reclamante por funcionaria al servicio del reclamado, lo que podría constituir vulneración a la normativa de protección de datos de carácter personal.

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

"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

En primer lugar, dicho tratamiento 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»).
(…)"

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 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.
(…)"

V

1. La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, principios relativos al tratamiento, al posibilitar el acceso a los datos carácter personal de la reclamante por una funcionaria al servicio de la entidad, accesos que no estaban justificados al no estar vinculados con finalidades profesionales.

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

El propio reclamado en escrito de 25/05/2022 en respuesta al ejercicio de derechos llevado a cabo por la reclamante le informaba *"…que dentro de la cadena de rastros se han detectado varias consultas no justificadas a sus datos…"*

También en Nota Interior del reclamado remitido a la Secretaria general, Subdirección General Adjunta, Unidad de Régimen Disciplinario, se indicaba que *"(…) El pasado 26 de mayo la Directora provincial de Valencia nos envió diferente documentación, entre la que se incluye un oficio de la Dirección provincial confirmando la existencia de los rastros detectados e indicando las funciones de la trabajadora, y una declaración de la funcionaria, en la que alega no haber realizado ningún acceso a datos personales más allá de los necesarios para las tareas que le competen.*

Después de analizar todos los documentos, desde esta unidad no se puede considerar suficiente para justificar las consultas efectuadas por los siguientes motivos:

- En primer lugar, hay que tener en cuenta la particularidad de este caso, puesto que la denunciante se encuentra inmersa en un procedimiento judicial en curso y, asimismo, esta persona tenía una relación de parentesco por afinidad con la denunciada.

- Por otro lado, en la documentación enviada por la D.P. de Valencia no se hace mención a ningún expediente concreto en el que se fundamenten los accesos realizados por esta funcionaria, y además las fechas de los mismos no coinciden con

un periodo de actividad de la denunciante, que en ese momento se encontraba en situación de desempleo.

(…)"

Ese deber de confidencialidad 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.

Por tanto, la actuación llevada a cabo supone la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del citado Reglamento.

VI

En segundo lugar, se atribuye al reclamado la posible 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, 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".*

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32.1 del RGPD, al producirse un incidente de seguridad, con vulneración de medidas técnicas y organizativas implantadas.

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 la AEPD trasladó al reclamado 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.

El reclamado ha confirmado los accesos producidos y que los mismos no están justificados, a pesar de lo manifestado por la funcionaria a su servicio de que se realizaron en el ámbito de su relación laboral, puesto que no existía expediente abierto a la reclamante y que cuando se realizaron los accesos la reclamante se encontraba en situación de desempleo.

Además, se hace necesario hacer referencia a la peculiaridad del caso ya que la reclamante tenía una relación de parentesco por afinidad con la funcionaria responsable de los accesos.

Por otra parte, el reclamado ha manifestado que, si bien el nivel de seguridad actual, la diligencia y la buena fe con la que trabaja el personal a su servicio, hacen que en muy pocas ocasiones surjan incidentes como el producido, a pesar de ello, se trabaja continuamente con el fin de evitar cualquier infracción de la normativa de

protección de datos, de manera que se puedan salvaguardar los derechos de los ciudadanos, adoptándose una serie de medidas enfocadas con dichos fines.

Hay que señalar, que en ocasiones no resulta suficiente el diseño e implantación de las medidas técnicas y organizativas adecuadas, aunque también resulta necesaria además de su correcta implantación, su utilización de forma apropiada.

La responsabilidad del reclamado viene determinada porque las medidas implantadas, en la medida de lo posible deben evitar errores e incidencias como el producido, ya que es el responsable de tomar decisiones destinadas a implementar y adecuar de manera efectiva medidas que garanticen un nivel de seguridad adecuado al riesgo y reforzando la confidencialidad de los datos, restaurando su disponibilidad e impidiendo 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:

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

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

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

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

En el caso examinado, el procedimiento sancionador trae causa en que el reclamado, tal y como se expone en los hechos, ha vulnerado 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 establecidas.

De conformidad con las evidencias de las que se dispone 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 declarar la infracción y establecer las medidas que procedan 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 manifestado que hechos como los producidos son escasos y que *"Aun así tales incidentes ocurren en algunas ocasiones, motivando la intervención de esta Inspección de Servicios con la consiguiente adopción de las*

medidas oportunas para corregir el problema y evitar o reducir las consecuencias que se puedan producir, tales como:

A. Un mayor control en el perfilado de los accesos a nuestras bases de datos por nuestro personal, para asignarle únicamente los estrictamente necesarios para el desempeño de sus tareas profesionales.

B. La retirada del acceso a las transacciones utilizadas de manera irregular.

C. La propuesta de apertura de expediente disciplinario (si se trata de nuestro personal).

D. El apercibimiento sobre la prohibición taxativa de cualquier acceso realizado fuera del ejercicio de sus tareas profesionales. En este sentido, cualquier acceso de nuestro personal a los datos contenidos en los ficheros del Sistema de Información de la Seguridad Social exige la introducción de una contraseña personal e intransferible, advirtiendo al usuario de que tal contraseña equivale a su firma electrónica y sobre la posibles actuaciones y responsabilidades (administrativas, civiles y penales) ante un acceso y uso indebidos de los datos contenidos en los mismos.

E. Aumentar la información y formación en materia de protección de datos impartida a todo el personal, para que sean más conscientes de la importancia de dicha materia, el compromiso de esta entidad con respecto a la misma, o de los perjuicios que puede suponer para el ciudadano un incidente en la seguridad de sus datos personales.

F. El refuerzo de los sistemas de auditorías periódicas y control de accesos a los ficheros y bases de datos informáticos gestionados por la TGSS.

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 TESORERIA GENERAL DE LA SEGURIDAD SOCIAL, con NIF ***Q2827003A***, ha infringido lo dispuesto en los artículos 5.1.f) y 32.1 del RGPD, tipificadas en el artículo 83.5.a) y 83.4.a) del RGPD, respectivamente.

SEGUNDO: NOTIFICAR la presente resolución a TESORERIA GENERAL DE LA SEGURIDAD SOCIAL.

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