- **Expediente N.º: PS/00020/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, LA PARTE RECLAMANTE) con fecha 27 de abril de 2021 interpuso reclamación ante la AEPD. La reclamación se dirige contra el INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL con NIF Q2827002C (en adelante, INSS). Los motivos en que basa la reclamación son los siguientes:

LA PARTE RECLAMANTE manifiesta que, junto con su pareja, solicitó la prestación de
paternidad/maternidad ante el INSS y el 17 de marzo de 2021, el INSS le remitió un correo electrónico en el que se le requería la subsanación de la petición.

Dicho correo se remitió a una dirección incorrecta que no pertenece al reclamante.

Junto a la reclamación aporta una copia del correo remitido por el INSS ***(…).***

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 al INSS, 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 se remitió con fecha 20 de mayo de 2021 a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, siendo notificado ese mismo día.

TERCERO: Con fecha 20 de julio de 2021, y de conformidad con lo dispuesto en el art. 65 de la LOPDGDD se produjo la admisión a trámite de la reclamación interpuesta por LA PARTE RECLAMANTE.

CUARTO: En fechas 26 y 30 de julio de 2021 respectivamente, se reciben en la AEPD dos notificaciones del INSS una de ellas inicial y otra adicional, comunicando la brecha de seguridad sufrida como consecuencia de la remisión de documentación personal de un interesado a un tercero.

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección

de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

- ***(…)***

Respecto de las causas que hicieron posible la brecha

(…)

Respecto de las medidas que se van a implantar

- ***(…)***

SEXTO: Con fecha 21 de marzo de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD, respectivamente.

SÉPTIMO: 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 que, en síntesis, manifestaba que "…al igual que el resto de las entidades gestoras y servicios comunes que integran la Administración de la Seguridad Social, está sometida a la norma que aprueba y revisa periódicamente el Comité de Seguridad de los Sistemas de Información de la Seguridad Social (CSSISS), en las normas de uso seguro de los sistemas de información de la Seguridad Social (se adjunta última versión de estas)…existiendo un documento expreso referido al uso del correo electrónico corporativo por parte de los funcionarios destinados en la Administración de la Seguridad Social, y un especial celo en cuanto a las medidas de seguridad diseñadas e implementadas por la Gerencia de Informática de la Seguridad Social, encargada de tratamientos a efectos de los sistemas informáticos, para salvaguardar la integridad, confidencialidad, disponibilidad y trazabilidad de los sistemas, incluido el correo corporativo, medidas que han sido revisadas y actualizadas tras los ciberataques sufridos recientemente a los servidores informáticos de distintos departamentos de la AGE, como ha sido el caso del Ministerio de Inclusión, Seguridad Social y Pensiones…"

Si bien es cierto que el INSS, como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos, dichas medidas no solo son medidas de los sistemas informáticos sino también medidas de organizativas de factor humano.

Es evidente que las medidas de seguridad implantadas fueron insuficientes; ya que, la existencia de ese documento expreso referido al uso del correo electrónico corporativo por parte de los funcionarios, no impidió que se remitiera por el INSS (******EMAIL.1***) un

correo electrónico a una dirección incorrecta que no pertenecía al reclamante, en el que se incluían los datos personales del reclamante: Nombre y Apellidos, DNI, teléfono, dirección de correo electrónico, provincia y código postal.

En este mismo sentido, el INSS aportó mayor información, a efectos de valorar la posible existencia de medidas previas de seguridad en relación a la programación formativa de los trabajadores.

Resaltándose por parte de esta Agencia, que la formación de los empleados públicos que tienen acceso o disponibilidad a datos personales disponibles en sus bases de datos es un control esencial que toda organización diligente debe poder acreditar y no sólo mencionar.

También se hizo referencia por parte del INSS que, dentro de la programación formativa acordada en la mesa de diálogo social con los sindicatos más representativos de los trabajadores, tiene establecido la impartición de dos tipos de cursos de protección de datos, uno a realizar por parte de las direcciones provinciales, y otro organizado por la dirección general; si bien, dicha medida viene a reforzar las medidas técnicas y organizativas existentes en el momento de producirse la brecha de seguridad.

El INSS en su escrito de alegaciones señalaba textualmente que "…si bien es cierto que es un evidente ejemplo de la pérdida de confidencialidad de la información, no se ha visto afectada la integridad y disponibilidad de los sistemas y servicios del tratamiento, toda vez que los datos personales remitidos en el correo electrónico, ya constaban en el correspondiente aplicativo informático así como en los servidores informáticos de la entidad (con las medidas de seguridad establecidas por el Centro Criptológico Nacional CCN-CERT y los requisitos del Esquema Nacional de Seguridad) .

Es evidente que en el presente caso, consta una brecha de seguridad de datos personales, categorizada como una brecha de confidencialidad, al haberse remitido por el INSS (******EMAIL.1***) un correo electrónico a una dirección incorrecta que no pertenece al reclamante, en el que se incluyen datos personales del reclamante: Nombre y Apellidos, DNI, teléfono, dirección de correo electrónico, provincia y código postal.

Cuando en el acuerdo de inicio se dice "…La remisión a la dirección de correo electrónico de un tercero de la documentación correspondiente a una solicitud de la prestación de nacimiento, para que el interesado subsanara los defectos de la misma, no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento…", nos estábamos refiriendo a la obligación del responsable y del encargado del tratamiento de aplicar la medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:.. b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

Por último, el INSS en sus alegaciones hacía referencia al déficit de personal y al incremento exponencial de la carga de trabajo asignada; si bien, que el incidente fuera debido a un error humano, a la sobrecarga de trabajo que viene soportando la

administración, así como a la limitación de recursos humanos, en ningún caso, justifican la vulneración de la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento así como el incumplimiento de la normativa vigente en materia de protección de datos como responsable del tratamiento de datos.

OCTAVO: Con fecha 17 de mayo de 2022 se formuló propuesta de resolución, proponiendo que se sancione al INSS, por una infracción de los artículos 5.1.f) del RGPD y 32 del RGPD, tipificada en los artículos 83.5 y 83.4 del RGPD con un APERCIBIMIENTO para cada una de las dos infracciones.

La propuesta de resolución se notificó a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, siendo notificada ese mismo día 17 de mayo.

NOVENO: Con fecha 31 de mayo de ese mismo año, el INSS presenta alegaciones a la propuesta de resolución notificada.

HECHOS PROBADOS

PRIMERO: Consta acreditado que el INSS remitió a LA PARTE RECLAMANTE un correo electrónico en el que se le requería la subsanación de la petición de paternidad/ maternidad previamente solicitada.

SEGUNDO: Consta acreditado que dicho correo electrónico, ***(...) ,*** se remitió a una dirección incorrecta que no pertenece al reclamante.

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 y 48.1 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

Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el INSS realiza, entre otros tratamientos, la recogida, registro, conservación de datos personales de los afiliados tales como nombre, apellidos, número de identificación, domicilio etc.

III
Alegaciones aducidas

En relación con las alegaciones presentadas a la propuesta de resolución el INSS, se procede a dar contestación a las mismas según el orden expuesto.

> PRIMERA. – –El Instituto Nacional de la Seguridad Social (INSS) está plenamente comprometido con el cumplimiento de la normativa vigente en materia de protección de datos personales y con el principio de responsabilidad proactiva, que rige la actuación de esta Administración.
>
> Con anterioridad al incidente acaecido que ha motivado la propuesta de resolución de procedimiento sancionador a esta Entidad, el INSS ya había realizado una campaña informativa sobre la detección y comunicación de brechas de seguridad (julio de 2020), que sigue estando publicada actualmente en la intranet institucional (Anexo I).
>
> Con carácter anual, el INSS viene realizando cursos de formación en materia de protección de datos, donde se desarrolla en concreto el concepto de brecha de seguridad y la concienciación sobre la importancia de las medidas preventivas (Anexo II).
>
> Asimismo, se imparte una sesión formativa sobre estos conceptos a los funcionarios de nuevo ingreso. A modo de ejemplo acreditativo, adjuntamos el programa de la formación impartida en febrero de 2021 a los funcionarios del cuerpo de gestión de la Seguridad Social, así como la impartida en mayo del 2022 a los funcionarios del cuerpo superior de Técnicos de la administración de la Seguridad Social (Anexo III).

En este sentido debemos mencionar que, no sólo en INSS sino toda la Administración Pública debe estar plenamente comprometida con el cumplimiento de la normativa en materia de protección de datos personales.

Las Administraciones Públicas actúan como responsables de tratamientos de datos de carácter personal y, en algunas ocasiones, ejercen funciones de encargados de tratamiento, por lo que les corresponde, siguiendo el principio de responsabilidad proactiva, atender las obligaciones que la normativa en materia de protección de datos personales les impone.

El INSS insiste en la formación dirigida a los funcionarios del cuerpo de gestión de la Seguridad Social.

El INSS, como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

Dentro de dichas medidas técnicas y organizativas de obligado cumplimiento, se encuentra la formación de los empleados públicos que tienen acceso o disponibilidad a datos personales disponibles en sus bases de datos.

En consecuencia, la programación en formación a la que se hace referencia viene a reforzar las medidas técnicas y organizativas existentes en el momento de producirse la brecha de seguridad.

> SEGUNDA. –. Este Instituto ha seguido adoptando diversas medidas en materia de Protección de Datos:
>
> Se han llevado a cabo múltiples acciones de concienciación, publicaciones, instrucciones, acciones formativas, elaboración de material de consulta…
>
> Cabe destacar el reciente objetivo institucional (del segundo semestre de 2021), que consistió en realizar una acción de comunicación dirigida a todo el personal del INSS, a través de las direcciones provinciales, para informar y sensibilizar sobre el concepto de brecha de seguridad y la necesidad de comunicarlo a la Subdelegada de Protección de Datos del INSS. (Anexo IV).
>
> En cuanto a las medidas concretas adoptadas para intentar evitar este tipo de sucesos y concienciar a los tramitadores sobre la importancia de revisar los destinatarios de las comunicaciones, así como su correspondencia con la documentación o información que contiene datos personales y que es enviada al exterior, esta Entidad ha elaborado y dado difusión a una píldora informativa que actualmente se encuentra publicada en su intranet corporativa (Anexo V).
>
> Por otro lado, y como consecuencia del proceso de actualización continua de los procedimientos de actuación realizados por el INSS, aprovechando las posibilidades técnicas disponibles en cada momento y, salvaguardando las políticas de privacidad y uso seguro, de conformidad con el 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; y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y garantía de los derechos digitales (LOPDGDD), se están analizando los procesos en los que es posible evitar la intervención del factor humano para que sean desarrollados de forma automatizada y reducir, en la medida de lo posible, las probabilidades de estos fallos humanos.
>
> A este respecto, cabe precisar que recientemente, se ha procedido a la automatización de la mayoría de las comunicaciones emitidas por este Instituto, de manera que, las notificaciones a comunicar a la ciudadanía han sido centralizadas en la imprenta de la que dispone la Gerencia de Informática de la Seguridad Social (servicio común de apoyo al INSS). De este modo, se está realizando de forma centralizada, a través de los aplicativos informáticos de

> gestión utilizados en la tramitación de sus prestaciones, tanto la impresión como el ensobrado de las comunicaciones emitidas por direcciones provinciales del INSS, así como por sus respectivos Centros de Atención e Información (CAISS) , sin intervención directa de personal adscrito a esta entidad (tren de impresión de SARTIDO-gestor documental del INSS), con la consiguiente disminución de la probabilidad de que se produzcan errores humanos.

En este sentido debemos resaltar que, las medidas mencionadas permitirán a dicho organismo público reforzar y contar con las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

En el momento de producirse la brecha de seguridad, ha quedado probado en el expediente que el INSS no disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

> TERCERA. – Atendiendo al aforismo “Errare humanum est”, podemos señalar que se ha tratado de un error humano puntual sobre los que esta Entidad ya adopta multitud de medidas tanto preventivas como reparadoras. Sin embargo, la producción eventual de estos sucesos aislados es, lamentablemente, inevitable ya que es consustancial a la esencia del ser humano. No obstante, como se ha señalado, el INSS trabaja permanentemente en la adopción de nuevos procesos de automatización para reducir al máximo la producción de este tipo de suceso.

El INSS insiste en que el incidente fue debido a un error humano; si bien, que el incidente fuera debido a un error humano, la sobrecarga de trabajo que viene soportando la administración, así como la limitación de recursos humanos en ningún caso, justifican la vulneración de la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento.

Destacando que la automatización de los procedimientos permitirá reforzar y contar con unas medidas de seguridad razonables en función de los posibles riesgos estimados, reduciendo al mínimo el error humano.

> CUARTA. – No se prevé que se produzcan nuevas violaciones de seguridad como consecuencia de este incidente concreto.

Dadas las medidas alcanzadas es imprevisible nuevas violaciones de seguridad como consecuencia de este incidente.

Si bien, en todo momento, estamos hablando de una previsión, hecho que puede suceder o no.

Circunstancia esta que no desvirtúa los hechos ocurridos ni la vulneración de la normativa de protección de datos cometida.

IV

Se imputa al INSS la comisión de una infracción por vulneración del artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

La infracción figura referenciada en el RGPD, artículo 83:

"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. (…)"

En el presente caso, ha quedado probado que los datos personales de la PARTE RECLAMANTE, obrantes en la base de datos del INSS, fueron indebidamente difundidos a terceros, vulnerándose el principio de confidencialidad; si bien, consta en el expediente la comunicación enviada a ese tercero que por error había recibido la documentación de los anteriores, con indicación expresa de la prohibición de utilizar la información facilitada por error, y las consecuencias administrativas, civiles y penales que acarrearía el incumplir dicha prohibición.

VI

Se imputa al INSS la comisión de una infracción por vulneración del artículo 32 del RGPD.

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y 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".

La infracción figura referenciada en el RGPD, 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:

5) 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.*

En el presente caso, ha quedado probado que, en el momento de producirse la brecha de seguridad, no consta que el INSS dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

El INSS manifiesta que el incidente pudo ser debido a un error humano (el funcionario que remitió el correo electrónico al tercero, intentó sustituir la dirección del correo anterior, cuyo objeto o contenido era muy similar, a pesar de haber copiado la dirección de correo electrónico correcta, o bien no pulsó el "intro" o la opción "pegar" para añadirla en el apartado de destinatario, o bien, si lo pulsó, el programa informático no sustituyó la anterior dirección por la nueva, por lo que se mantuvo la incorrecta).

Si bien, que el incidente fuera debido a un error humano, la sobrecarga de trabajo que viene soportando la administración, así como la limitación de recursos humanos en ningún caso, justifican la vulneración de la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento.

Por lo demás, la manera de actuar del funcionario, tal y como está descrita, comporta un cierto riesgo de que errores como este puedan producirse.

La remisión a la dirección de correo electrónico de un tercero de la documentación correspondiente a una solicitud de la prestación de nacimiento, para que el interesado subsanara los defectos de la misma, no garantiza la confidencialidad, integridad y disponibilidad de los sistemas y servicios del tratamiento.

VIII

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

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se pue-

de, 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…

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. (…)"

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 al INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL, con NIF Q2827002C, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

IMPONER al INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL, con NIF Q2827002C, por una infracción del artículo del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a INSTITUTO NACIONAL 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.

938-050522

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