

- Expediente N.º: EXP202101350

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 07/07/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el SERVICIO PUBLICO DE EMPLEO ESTATAL con NIF **Q2819009H** (en adelante el reclamado). Los motivos en que basa la reclamación son los siguientes: que ha recibido una carta procedente de la reclamada en la que figuran impresos en el sobre (visibles desde el exterior, por tanto) datos personales que no debieran exponerse.

Y aporta fotografía de una de las caras del sobre de la carta recibida. El membrete referencia a la parte reclamada e incluye el nombre, apellidos y dirección de la parte reclamante. Asimismo, incorpora los siguientes datos: “Exp.: *****EXP.1**”, “N.I.F./N.I.E.: *****NIF.1**”

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 24/08/2021 se dio traslado de dicha reclamación al reclamado de conformidad con lo establecido en la LPACAP, 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. No consta respuesta del reclamado.

TERCERO: Con fecha 28/10/2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, teniendo conocimiento de los siguientes extremos:

Con fecha 03/02/2022 tiene entrada escrito de la reclamada señalando que no le consta notificación alguna de la AEPD en relación con los hechos investigados.

Causas del incidente y medidas de reacción

La inspección de servicios del reclamado manifiesta lo siguiente en relación con los hechos objeto de reclamación que: *“En las comunicaciones postales dirigidas por el SEPE a las personas solicitantes y/o beneficiarias de prestaciones por desempleo únicamente son visibles los datos necesarios para la entrega por el operador postal, es decir, el nombre y apellidos y la dirección postal del interesado. En el mes de junio de 2021 se llevó a cabo un cambio en las plantillas de comunicaciones del organismo. Como consecuencia de dicho cambio, se produjo una incidencia que ocasionó que se desplazaran los datos, por lo que se emitió una remesa de comunicaciones erróneas.*

La incidencia se detectó y corrigió con la máxima rapidez posible, sin que se haya tenido constancia de otras quejas al respecto.”

QUINTO: Con fecha 26/04/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción de los artículos 5.1.f) y 32.1 del RGPD, sancionados conforme a lo dispuesto en el artículo 83.5.a) y 83.4.a) del citado RGPD y considerando que la sanción que pudiera corresponder sería de APERCIBIMIENTO. Consta la recepción por el reclamado del acuerdo de inicio del expediente.

SEXTO: Notificado el acuerdo de inicio, el reclamado al tiempo de la presente resolución no ha presentado escrito de alegaciones, por lo que es de aplicación lo señalado en el artículo 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que en su apartado f) establece que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, por lo que se procede a dictar Resolución.

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

HECHOS PROBADOS

PRIMERO. El 07/07/2021 tiene entrada en la AEPD escrito de la reclamante manifestando que ha recibido una carta procedente del reclamado figurando impresos en el sobre (visibles desde el exterior) datos personales que no debieran ser revelados.

SEGUNDO. La reclamante aporta fotografía de una de las caras del sobre de la carta recibida; figuran el membrete de referencia del reclamado; el nombre, apellidos y dirección de la reclamante. También incorpora los siguientes datos: “Exp.: *****EXP.1**”, “N.I.F./N.I.E.: *****NIF.1**”.

TERCERO. El reclamado en escrito de 03/02/2022 ha manifestado que “...*En el mes de junio de 2021 se llevó a cabo un cambio en las plantillas de comunicaciones del organismo. Como consecuencia de dicho cambio, se produjo una incidencia que ocasionó que se desplazaran los datos, por lo que se emitió una remesa de comunicaciones erróneas.*

La incidencia se detectó y corrigió con la máxima rapidez posible, sin que se haya tenido constancia de otras quejas al respecto”

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 reclamados se materializan en el envío por el reclamado de una carta en cuyo sobre figuran datos de carácter personal que podrían vulnerar la normativa en materia de protección de datos personales.

El artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *“integridad y confidencialidad”*.

El citado artículo señala 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»).

(...)

III

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al permitir el acceso a los datos de carácter personal de la reclamante, como consecuencia de la remisión por el reclamado de una carta en cuyo sobre figuran los mismos.

Este deber de confidencialidad, debe entenderse que tiene como finalidad evitar que se realicen accesos a los datos no consentidos por los titulares de los mismos.

Por tanto, 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.

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

En segundo lugar, el 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”.

VI

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 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”.
(...)”*

Los hechos puestos de manifiesto podrían suponer la vulneración de las medidas técnicas y organizativas vulnerando la confidencialidad de los datos y permitiendo el acceso a los mismos incluidos en el sobre de la carta enviada por el Servicio de Empleo.

VII

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 en su sistema permitiendo el acceso a datos personales de la reclamante, con la vulneración de las medidas técnicas 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 deben protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales”.

En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación la AEPD trasladó al reclamado el 24/08/2021 la reclamación presentada para su análisis solicitando la aportación de información relacionada con la incidencia reclamada, sin que remitiera respuesta al respecto.

No obstante, el 19/01/2022 se le envió nuevo requerimiento de información y el 03/02/2022 remitía respuesta señalando que no le constaba notificación alguna de la AEPD y que el incidente reclamado era debido a que *“En el mes de junio de 2021 se llevó a cabo un cambio en las plantillas de comunicaciones del organismo. Como consecuencia de dicho cambio, se produjo una incidencia que ocasionó que se desplazaran los datos, por lo que se emitió una remesa de comunicaciones erróneas”.*

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo

para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

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).

VIII

No obstante lo que antecede, también la LOPDGDD en su artículo 77, Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento, establece lo siguiente:

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

- 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”.

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

Hay que señalar que la LOPDGDD contempla en su artículo 77 la sanción de apercibimiento en relación con los tratamientos de datos personales que no se adecúen a sus previsiones. A este respecto, el artículo 83.7 del RGPD contempla que “Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro”.

En este mismo sentido, el artículo 58 del RGPD, en su apartado 2 d) señala 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...”.

Como se señalaba con anterioridad ha quedado acreditado que el reclamado ha incumplido la normativa de protección de datos, artículos 5.1.f) y 32.1 del RGPD, al posibilitar el acceso a los datos de carácter personal de la reclamante, al remitir el reclamado una carta en cuyo sobre figuran los mismos, vulnerando las medidas técnicas y organizativas.

Sin embargo, en su respuesta a este centro directivo el 03/02/2022 el reclamado ha señalado haber corregido la incidencia producida manifestando “.. *En el mes de junio de 2021 se llevó a cabo un cambio en las plantillas de comunicaciones del organismo. Como consecuencia de dicho cambio, se produjo una incidencia que ocasionó que se desplazaran los datos, por lo que se emitió una remesa de comunicaciones erróneas.*

La incidencia se detectó y corrigió con la máxima rapidez posible, sin que se haya tenido constancia de otras quejas al respecto”.

Por ello, se considera que la respuesta ha sido razonable habiéndose subsanado la incidencia y no procediendo instar la adopción de medidas adicionales.

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 SERVICIO PUBLICO DE EMPLEO ESTATAL, con NIF **Q2819009H**, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: IMPONER al SERVICIO PUBLICO DE EMPLEO ESTATAL, con NIF **Q2819009H**, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de apercibimiento.

TERCERO: NOTIFICAR la presente resolución al SERVICIO PUBLICO DE EMPLEO ESTATAL.

CUARTO: 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