Procedimiento Nº: PS/00327/2019

- **RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR**

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, el reclamante) con fecha 13/02/2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***CONSEJERIA DE SANIDAD Y POLITICAS SOCIALES DE LA JUNTA DE EXTREMADURA*** con NIF ***S0611001I*** (en adelante, el reclamado). Los motivos en que basa la reclamación son: la ausencia de seguridad en el acceso al solicitar cita previa para consultas de atención primaria desde sus webs, ya que cualquier persona puede acceder con facilidad a datos de los usuarios de la sanidad de la comunidad y gestionarlos.

Adjunto captura de pantalla página web e imágenes.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 01/04/2019 fue trasladada al reclamado la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.
- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.
- Cualquier otra que considere relevante.

En la misma fecha se le comunicaba al reclamante la recepción de la reclamación y su traslado a la entidad reclamada.

El reclamado en fecha 01/07/2019 alegaba, en síntesis: Que el Servicio Extremeño de Salud (SES), en el cumplimiento de sus fines y con el objetivo de facilitar al ciudadano las relaciones con la administración sanitaria creo un servicio de la gestión sanitaria del ciudadano estableciendo dos niveles distintos: un nivel de gestión de citas en atención primaria y otro de gestión de información clínica relacionada con la atención especializada.

Este servicio denominado “centro de salud online” permite acceder a la gestión de las citas con su centro de atención primaria, limitando la información a fecha hora y lugar de la cita; asimismo, el servicio permite al ciudadano solicitar una cita, modificarla o anularla. Para la gestión de la información médica del ciudadano el sistema obliga a una autenticación compleja, reforzada con elementos tales como DNI electrónico, etc.

Que no están conforme con la visión presentada por el reclamante ya que si bien es cierto que para el área de citas es suficiente con introducir fecha de nacimiento y DNI, la información a la que se puede acceder es simplemente la relacionada con la cita en Atención Primaria, pero en ningún caso se puede acceder a otro tipo de información, como historial médico, tratamientos, datos de salud o citas de Atención Especializada, para la cual se necesitaría una autenticación más compleja (DNI, certificado electrónico, etc.).

No obstante, el SES ha valorado la modificación de algunos aspectos de seguridad en relación con la reclamación recibida, señalando entre otros la modificación de las condiciones de uso y la aceptación previa de las condiciones de uso del servicio.

TERCERO: El 25/07/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: Con fecha 10/12/2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 5.1.f) del RGPD, sancionada conforme a lo dispuesto en el artículo 83.5.a) del citado RGPD.

QUINTO: Notificado el citado acuerdo de inicio, el reclamado no presentó escrito de alegaciones dentro del plazo legal establecido para ello, 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..

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

HECHOS PROBADOS

PRIMERO: Con fecha 13/02/2019 el reclamante presento escrito en la AGPD motivada por la ausencia de seguridad al solicitar cita previa para consultas de atención primaria desde su web, ya que cualquier persona puede acceder con facilidad a los datos de los usuarios de la sanidad de la comunidad y gestionarlos.

SEGUNDO: Consta aportada copia del DNI del reclamante nº ******NIF.1***

TERCERO: El SES en escrito de 17/05/2019 manifiesta *"que el uso del servicio está sujeto a unas normas de uso, disponibles de un enlace accesible una vez se ha accedido, visible en la parte inferior de la web y que puede consultarse en la dirección https://saludextremadura.ses.es/onilne/publico/infoLegal.xhtml",* y que para el caso de producirse accesos no autorizados ni consentidos, como el supuesto planteado por el reclamante *"debe entenderse que no se produce una brecha de seguridad en el sistema de información sino, más bien, la comisión de un delito por parte de quien accede a datos no autorizados"* y que ha valorado la modificación de algunos aspectos relacionados con la seguridad como:

"- Modificación de las condiciones de uso, adecuando las mismas a la prevención de la comisión de los delitos que se ha hechos referencia previamente, con especial incidencia sobre los delitos relacionados con el descubrimiento y la revelación de secretos.

- Aceptación previa de las condiciones de uso del servicio: si bien es cierto que el uso del servicio CSOnline esta sujeto a unas condiciones de uso a las que ya se ha hecho referencia en este documento y, que según se acaba de indicar, se modificarán en el sentido de la reclamación, se propone incluir una aceptación previa expresa (opt in) de las condiciones de uso. Con esta modificación, el usuario declara ser conocedor de las condiciones de uso. Con esta modificación, el usuario declara ser conocedor de las condiciones de uso y, concretamente, de la posibilidad de la comisión de un delito en so de acceder a datos de terceros".

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 64 *"Acuerdo de iniciación en los procedimientos de naturaleza sancionadora",* dispone:

"1. El acuerdo de iniciación se comunicará al instructor del procedimiento, con traslado de cuantas actuaciones existan al respecto, y se notificará a los interesados, entendiendo en todo caso por tal al inculpado.

Asimismo, la incoación se comunicará al denunciante cuando las normas reguladoras del procedimiento así lo prevean.

2. El acuerdo de iniciación deberá contener al menos:

a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Identificación del instructor y, en su caso, Secretario del procedimiento, con expresa indicación del régimen de recusación de los mismos.

d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.

e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.

f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como indicación de 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.

3. Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados".

En aplicación del anterior precepto y teniendo en cuenta que no se han formulado alegaciones al acuerdo de inicio, procede resolver el procedimiento iniciado.

III

Los hechos denunciados se concretan en la ausencia de medidas de seguridad en la web destinada por el SES para gestionar las solicitudes de cita previa de atención primaria en los centros o servicios de salud extremeños, ya que para concertar cita solo es necesario introducir DNI y fecha de nacimiento, lo cual permitiría el acceso a otros datos vinculados al paciente por terceros vulnerando el deber de confidencialidad.

El 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»).

(…)"

El artículo 5, *Deber de confidencialidad*, de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), señala que:

"1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

IV

La documentación obrante en el expediente evidencia que el SES vulnera el artículo 5 del RGPD, *principios relativos al tratamiento*, en relación con el artículo 5 de la LOPGDD, *deber de confidencialidad,* en relación con la web destinada por el citado organismo en la gestión de las solicitudes de cita previa de atención primaria en los centros de salud extremeños, como además lo justifica el que se haya reforzado el aviso legal recordando que el acceso no autorizado a datos o información de terceros es un hecho delictivo y un mecanismo de opt-in para aceptar las condiciones, entendiendo que antes de acceder a la sección de citas o registrarse en ella

Este deber de confidencialidad, con anterioridad deber de secreto, 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 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.

El propio reclamado estima que aunque para la cita es suficiente con introducir el DNI y fecha de nacimiento, la información a la que se podría acceder es la relacionada con la cita de Atención primaria sin que se pueda acceder a otro tipo de información como historial médico, datos de salud, etc., necesitando una autenticación más compleja reforzada con otros elementos; sin embargo, no es menos cierto que a raíz de la reclamación ha valorado la modificación de algunos aspectos relacionados con la seguridad como las condiciones de uso, adecuando las mismas a la prevención de la comisión de los delitos y la inclusión previa expresa (opt in) de las condiciones de uso, lo que lo que vendría a corroborar la endeblez de las medidas técnicas y organizativas implantadas siendo adecuado la aplicación de una modificación del procedimiento de acceso al sistema.

V

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, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, *"con multas administrativas de 20.000.000€ 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".*

La LOPDGDD en su artículo 72, a efectos de prescripción, 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.

(…)"

IV

No obstante, 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".

En el supuesto que nos ocupa, en el presente procedimiento sancionador consta acreditado que, en relación con el servicio instaurado para la gestión de citas previas de los centros de atención primaria, se ha vulnerado la normativa sobre protección de datos de carácter personal.

De conformidad con las evidencias de las que se dispone, dicha conducta constituye por parte del reclamado la infracción de lo dispuesto en el artículo 5.1.f) 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.

Asimismo, se contempla que la resolución que se dicte establecerá las medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido, la adecuación del tratamiento a las exigencias contempladas en el artículo 5 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Como se señalaba con anterioridad ha quedado acreditado que el reclamado no tiene adoptadas medidas pertinentes que garanticen un nivel de seguridad adecuado capaz de asegurar la confidencialidad e integridad de los datos evitando accesos no autorizados e inconsentidos, no siendo suficiente la solución incorporada por el reclamado de reforzar el aviso legal en su página web para recordar que el acceso no autorizado a información es un delito, así como el mecanismo *opt-in* para aceptar las condiciones antes de acceder a la sección de citas o registrarse en ella.

Se hace necesario señalar que de no corregir dichas deficiencias adoptando las medidas adecuadas conforme a lo señalado en el artículo 5.1.f) del RGPD a fin de garantizar 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 o bien reiterar la conducta puesta de manifiesto en la reclamación y que es causa del presente procedimiento, así como no informar seguidamente a esta AEPD de las medidas adoptadas podría dar lugar al ejercicio de posibles actuaciones ante el responsable del tratamiento a fin de que se apliquen de manera efectiva las medidas apropiadas para garantizar y no comprometer la confidencialidad de los datos de carácter personal y el derecho a la intimidad de las personas.

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 CONSEJERIA DE SANIDAD Y POLITICAS SOCIALES DE LA JUNTA DE EXTREMADURA (Servicio Extremeño de Salud), con NIF ***S0611001I***, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: REQUERIR a la CONSEJERIA DE SANIDAD Y POLITICAS SOCIALES DE LA JUNTA DE EXTREMADURA (Servicio Extremeño de Salud), con NIF ***S0611001I*****,** para que en el plazo de un mes desde la notificación de esta resolución, acredite: la adopción de las medidas necesarias y pertinentes de conformidad con la normativa en materia de protección de datos de carácter personal a fin de evitar que en el futuro vuelvan a producirse incidencias como las que han dado lugar a la reclamación corrigiendo los efectos de la infracción, adecuando las citadas medidas a las exigencias contempladas en el artículo 5.1.f) del RGPD.

TERCERO: NOTIFICAR la presente resolución a CONSEJERIA DE SANIDAD Y POLITICAS SOCIALES DE LA JUNTA DE EXTREMADURA (Servicio Extremeño de Salud), con NIF ***S0611001I.***

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