- **Expediente Nº: E/04664/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: ***Dª. A.A.A. (***en adelante, la parte reclamante) con fecha 17 de diciembre de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra Consejería de Sanidad de la Comunidad de Madrid con NIF S7800001E (en adelante, la Consejería). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante expone que en fecha 15/12/20 acude al servicio de urgencias del Centro de Salud Jaime Vera, de Leganés, donde recibió la pertinente asistencia sanitaria. Si bien, su médico de cabecera no pudo registrar la información en su historial clínico, porque tanto su historial como su perfil como paciente y usuaria de la Atención Primaria no constaba en las bases de datos del sistema informático del Servicio Madrileño de Salud.

En consecuencia, declara una brecha de seguridad y duda sobre si se podrá recuperar la información extraviada y que no consta.

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 a la Consejería, 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 constando contestación al traslado de la reclamación.

TERCERO: Con fecha 22 de abril de 2021 se admitió a trámite la reclamación presentada por la parte reclamante, al amparo de lo establecido en el artículo 65.5 de la LOPDGDD.

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

De conformidad con la información remitida por el Comité Delegado de Protección de Datos (en adelante CDPD) de la Consejería de Sanidad de la Comunidad de Madrid, ***Dª A.A.A. con DNI: ***NIF.1 con ***DIRECCION.1*** y adscrita al Centro de salud Jaime Vera, constaba de alta inicial en la base poblacional el 01/06/1997 y de baja en la base poblacional CIBELES del 03/11/2020 hasta el 12/01/2021.
Es de resaltar que el Sistema de Información Poblacional CIBELES se configura como el registro básico de los datos de los usuarios del Sistema Sanitario Público Madrileño y como el instrumento básico de gestión sanitaria de la Comunidad de Madrid, que permite la planificación de recursos humanos, infraestructuras y la inclusión de las

prestaciones sanitarias y los recursos tanto de Atención Primaria como Hospitalaria, favoreciendo una gestión sanitaria eficaz, eficiente e integral.

En consecuencia, la Historia Clínica Electrónica no era accesible por parte de los profesionales sanitarios, debido a la situación de baja de la interesada en el sistema.

Tras alta el día 12/01/2021 en la Base de Datos Poblacional, consta en la Historia Clínica Electrónica de la ciudadana toda la información que existía hasta la fecha del 03/11/2020.

Con fecha 20 de octubre de 2021 y en el marco de las actuaciones practicadas por la Subdirección General de Inspección de Datos con objeto de aclarar los hechos ocurridos, se solicitó a la Consejería información relativa a:

(…)

En contestación a dicha solicitud de información se formulan las siguientes consideraciones:

- La reclamante consta dada de alta en la base poblacional el día 01/06/1997.
- La reclamante figura de baja en la base poblacional del sistema CIBELES desde el día 03/11/2020 hasta el 12/01/2021, debido a la necesidad de acreditación del derecho de asistencia en el Instituto Nacional de la Seguridad Social (INSS).
- La Base de datos poblacional CIBELES que utiliza la Comunidad de Madrid para la prestación de los servicios que le son propios, proviene de la base del INSS y está sincronizada con la misma.

Por tanto, cuando el INSS observa alguna discrepancia, solicita regularizar dicha situación, y mientras no se solvente su incidencia, el ciudadano figura como baja en la base de datos poblacional de la Comunidad de Madrid CIBELES.

Tras regularizar la ciudadana su situación en el INSS, cursa alta el día 12/01/2021 en la Base de Datos Poblacional, y consta en la HCE de la ciudadana toda la información que existía hasta la fecha del 03/11/2020.

(…)

A lo cual se hace la siguiente consideración:

La Base poblacional CIBELES es un requisito para poder acceder a la Historia Clínica Electrónica, y depende de que el ciudadano se encuentre dado de alta en el Instituto Nacional de la Seguridad Social (INSS).
Existe un procedimiento general de atención en urgencias en el que se establece la posibilidad de realizar un alta transitoria para reflejar la asistencia sanitaria, pudiendo acceder a la información que conste en la base de datos.

El día 15/12/2020 no consta que esta ciudadana recibiese esa alta provisional.

Tras contactar en el Centro de Salud, nos informan que no existe ningún documento en papel de esta ciudadana en las fechas en que no estuvo de alta en la base de datos, no existen constancia de citas el día 15/12/2020, ni existe constancia de registro en su historia clínica el día 15/12/2020.

Tras alta el día 12/01/2021 en la Base de Datos Poblacional, consta en la HCE de la ciudadana toda la información que existía hasta la fecha del 03/11/2020.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) 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."*

Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.

III

El Artículo 32 del RGPD establece:

"Seguridad del tratamiento

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".

En el presente caso, se reclama por una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de disponibilidad, al no haber podido acceder a la información del historial clínico y registrar la información de la última asistencia médica recibida.

No obstante, de la documentación aportada por la Consejería se desprende que no ha existido brecha de seguridad alguna, dado que la Historia Clínica Electrónica (HCE) no era accesible por parte de los profesionales sanitarios, debido a la situación de baja de la interesada en el sistema. Sin embargo, tras alta el día 12/01/2021 en la Base de Datos Poblacional, consta en la HCE de la ciudadana toda la información que existía hasta la fecha del 03/11/2020.

IV

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***Dª. A.A.A.*** y a la Consejería de Sanidad de la Comunidad de Madrid,

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

940-051121

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