- Expediente Nº: PS/00033/2022

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 20/04/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra CONSEJERÍA DE SANIDAD con NIF ***S7800001E*** (en adelante, la parte reclamada). Los motivos en que se basa la reclamación son los siguientes: la reclamante manifiesta que, en contestación a una queja interpuesta ante el Servicio de Atención al Paciente del hospital de la CAM, ha recibido respuesta a la que se adjunta informe médico relativo a una tercera persona.

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 14/05/21 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. No consta en esta Agencia respuesta del reclamado.

TERCERO: Con fecha 06/09/2021, 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, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 58.1 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:

Consta escrito procedente de la Consejería con fecha de 23/09/2021, firmado por el Comité Delegado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid.

En relación con el traslado de la reclamación referido en el apartado antecedentes (realizado en el contexto del expediente E/05274/2021), señala el escrito del reclamado que *"no es hasta el pasado 27/09/2021 cuando este Comité ha tenido conocimiento del mismo, dado que han existido incidencias de distinta índole en el Registro de entrada"*.

Con relación a los hechos objeto de reclamación el escrito del reclamado facilita la siguiente información:

Cronología y naturaleza del incidente:
Se anexa informe realizado por el Hospital en relación con los hechos reclamados (Anexo 1).

Este informe, fechado el 22/09/2021, incluye la siguiente descripción de hechos:

"*1.- Con fecha 26 de marzo de 2021, tuvo entrada en el registro del Servicio de Atención al Paciente del Hospital Universitario de La Princesa, con número* ******RECLAMACIÓN.1****, reclamación presentada por Dña.* ***A.A.A.****.*

*Con motivo de la citada reclamación, con fecha 6 de abril de 2021, se remitió escrito del ***CARGO.1, adjuntando copia del informe realizado por el ***CARGO.2, donde se daba contestación a las cuestiones planeadas por la paciente.*
Es relevante destacar que esta contestación a la ahora reclamante ante la AEPD fue remitida correctamente a la dirección que facilitó la propia paciente en su escrito, esto es, a la ******DIRECCIÓN.1****. Así se puede constatar en la reclamación y contestación.*

2.- Con posterioridad, el siguiente 30 de marzo de 2021, tuvo entrada en el registro del Servicio de Atención al Paciente, una reclamación presentada por la paciente Dña. ***B.-B.B.****, con número* ******RECLAMACIÓN.2****.*

La contestación a esta reclamación fue remitida con fecha 13 de abril de 2021, adjuntando el informe del Servicio (…), donde se daba respuesta a las cuestiones planteadas por la paciente Dña. ***B.B.B.****.*

No obstante, efectivamente, debido a un error al indicar la dirección y destinatario de la contestación, ésta fue remitida a Dña. ***A.A.A.****, motivo por el cual ha presentado reclamación ante la AEPD, manifestando su preocupación de que su informe se haya remitido a otra persona. Sin embargo, cabe indicar que la contestación dirigida a Dña.* ***B.B.B.****, y que recibe la reclamante Dña.* ***A.A.A.****, fue enviada a la misma dirección a la que se envió el escrito de 6 de abril de 2021 que daba contestación a su reclamación.*

Por tanto, conviene remarcar que los datos personales de la reclamante, Dña. ***A.A.A.****, no han sido afectados al no haber remitido la contestación a su reclamación a ninguna dirección errónea. Esta información se constata también en la reclamación y contestación de Dña.* ***B.B.B.****, que se acompañan como documento 2.*

3. Esta Dirección Gerencia no ha tenido constancia de ninguna reclamación presentada en este sentido por parte de Dña. ***A.A.A.*** *hasta el pasado 6 de septiembre de 2021, cuando se ha recibido directamente la reclamación y solicitud de información de la AEPD."*

En relación con las causas que habrían propiciado que se enviara el informe al destinatario incorrecto, el Hospital señala en su informe que se debió a *"un error al elaborar la contestación dirigida a Dña.* ***B.B.B.****, al transcribir una dirección y destinatario que eran incorrectos, de forma que la misma fue enviada equivocadamente a Dña.* ***A.A.A.****."* Asimismo, la Consejería en su escrito lo califica de *"error humano puntual".*

Se adjuntan al escrito del reclamado, documentos 1 y 2 referidos en el Anexo 1:

- El documento 1 incluye:

- La copia de la reclamación presentada por la parte reclamante ante el Hospital con fecha de 26/03/2021. En ella, la dirección consignada para la parte reclamante es ******DIRECCIÓN.1***.
- Escrito de remisión de la reclamación al servicio (…) del hospital desde el servicio de atención al paciente.
- Escrito dirigido con fecha de 06/04/2021 por el Hospital a la parte reclamante con número de registro de salida ******RECLAMACIÓN.1*** que señala, en relación con la queja presentada con anterioridad, que se remite copia del *"informe realizado por el Dr.* ***C.C.C.****".*
  - Informe de fecha 06/04/2021 firmado por el Dr. ***C.C.C.*** que refiere la respuesta a la reclamación de la parte reclamante.

- El documento 2 incluye:

- La copia de la reclamación presentada por la tercera persona (Dña. ***B.B.B.***) ante el Hospital con fecha de 30/03/2021.
- Escrito de remisión de la reclamación de esta tercera persona al servicio (…) del hospital desde el servicio de atención al paciente.
- Escrito dirigido con fecha de 13/04/2021 por el Hospital a la parte reclamante que señala, en relación con la queja presentada con anterioridad, que se remite copia del *"informe realizado por la Dra.* ***D.D.D.****".*
- Informe de fecha 08/04/2021 firmado por la Dra. ***D.D.D.*** que incluye sello del Hospital y refiere la respuesta a una reclamación de un tercero sobre una intervención médica relacionada con *(…)* efectuada por la doctora. Los datos personales del tercero que figuran en el informe son su nombre y apellidos, e información de detalle de la técnica médica utilizada en la intervención.

Número de afectados, categorías de los datos personales expuestos y uso posterior:
Señala el Hospital que la incidencia ha tenido una única afectada (la tercera persona sobre la que versaba el informe recibido por la parte reclamante). Así, cita expresamente que *"únicamente se han visto afectados los datos personales reflejados en el Informe de doña* ***B.B.B.*** *y los mismos han sido revelados a una única persona (doña* ***A.A.A.****)"*. Asimismo, apunta que no tiene constancia de que esta información haya sido utilizada por otros.

Comunicación a los afectados:

Manifiesta el Hospital en su informe que la afectada (Dña. ***B.B.B.***) *"fue informada verbalmente de que la contestación se había enviado a otra dirección cuando acudió personalmente al Servicio de Atención al Paciente del Hospital."*

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

Manifiesta el Hospital en su informe que *"es la primera vez que se tiene conocimiento de una reclamación de este tipo, sin que la paciente Dña.* ***A.A.A.*** *se dirigiera en ningún momento al Hospital para informar de esta incidencia.*"

Medidas de reacción al incidente:

Expresa el Hospital en su informe que *"cuando se recibió la reclamación, de forma inmediata se recopiló toda la información relativa a los hechos, de cara a poder identificar las causas del incidente y prevenir que puedan volver a repetirse en un futuro. Además, se recordará al personal la importancia de extremar al máximo el cuidado en las contestaciones remitidas, debiendo comprobar en más de una ocasión que los datos personales introducidos son los correctos, dada la relevancia y sensibilidad de los datos personales de los pacientes y su especial protección."* Cita además su compromiso con la normativa conforme a la *"Guía de pacientes y usuarios de la Sanidad"* elaborada por la AEPD.

El reclamado en su escrito expresa además que *"la Consejería de Sanidad de la Comunidad de Madrid tiene implementadas medidas para preservar la seguridad de la información y los derechos y libertades de los ciudadanos, entre las que se incluyen medidas de naturaleza organizativa que comprenden la formación regular y periódica del personal de los centros asistenciales del Servicio Madrileño de Salud (SERMAS) que se considera como una medida idónea para prevenir errores humanos como el acaecido. Si bien esta medida se considera adecuada, no impide que los mismos ocurran, no obstante, tal y como puede apreciarse y se ha manifestado, se trata del primer error del que se tiene constancia. En cualquier caso, este CDPD procederá a revisar el plan de formación del centro para valorar si se requiere una formación adicional en su centro de trabajo."*

Notificación a la AEPD:

En relación con la no notificación a la AEPD, manifiesta el reclamado que los hechos *"no se han valorado como una brecha de seguridad y sí como un incidente de seguridad."*

Añade al respecto la siguiente explicación: *"Es indiscutible que la dimensión de la seguridad asociada a confidencialidad se ha visto vulnerada, sin embargo se han valorado los parámetros de volumen de datos, tipología del incidente y su impacto, determinado que su riesgo tiene un perjuicio limitado a los efectos de considerarlo como una brecha de seguridad que deba ser objeto de notificación a esta Agencia, puesto que no supone un alto riesgo en los derechos de la única ciudadana afectada, teniendo en cuanta asimismo el contenido de los informes remitidos por causa de un error humano puntual.*

No obstante, a pesar de no calificarse como brecha de seguridad que deba ser objeto de comunicación a esta Agencia, en atención a lo previsto en el artículo 33 RGPD, sí puede considerarse la actividad del HPRI como proactiva en relación con lo previsto en el art. 34 RGPD, dado que se informó a la afectada de que sus datos habían sido remitidos a otra persona por error."

QUINTO: Con fecha 17/03/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción de los artículos 32.1 y 5.1.f) del RGPD, tipificadas en el artículo 83.4.a) y 83.5.a) del RGPD, con apercibimiento.

SEXTO: Notificado el acuerdo de inicio, el reclamado al tiempo de la presente resolu-

ción 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 20/04/2021 la afectada interpuso reclamación ante la Agencia Española de Protección de Datos, manifestando que, en respuesta a una queja interpuesta ante el Servicio de Atención al Paciente de hospital perteneciente al sistema público de la CAM, ha recibido adjunto informe médico relativo a una tercera persona.

SEGUNDO: Consta aportada escrito de respuesta a la reclamación interpuesta por la reclamante ante el Servicio de Atención al Paciente de hospital público de la CAM de 13/04/2021.

TERCERO: Al anterior escrito se adjunta Informe de 08/04/2021 firmado por Facultativo especialista si bien correspondiente a una tercera persona.

CUARTO: El reclamado en escrito de 23/09/202 ha manifestado que:

"El día 30/03/2021 doña …, (persona distinta) presentó una reclamación (nº ******RECLAMACIÓN.2****) que fue atendida el 13/04/2021 pero que, por culpa de un error humano puntual fue remitida a* la reclamante*, …*

Los datos de la reclamante *no han sido revelados a ninguna persona…"*

Y que *"..., únicamente se han visto afectados los datos personales reflejados en el Informe de doña …* (persona distinta a la reclamante) *y los mismos han sido revelados a una única persona (*la reclamante*), esto es, los datos personales que se han visto afectados se corresponden con los datos identificativos de nombre, apellidos y datos de salud de una única persona.*

En relación con el problema que causó el incidente, el Hospital *señala en su informe que se corresponde con un "error al elaborar la contestación dirigida a* la reclamante*, al transcribir una dirección y destinatario que eran incorrectos".*

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

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 materializan en el acceso a datos de tercero como consecuencia de la respuesta ofrecida a una queja presentada por la reclamante ante el Servicio de Atención al Paciente del hospital integrante del sistema sanitario público de la CAM, a la que se adjunta informe médico relativo a una tercera persona.

El RGPD se ocupa en su artículo 5 de los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *integridad y confidencialidad*, señalando:

"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

La infracción que se le atribuye a la reclamada se encuentra tipificada en el artículo 83.5 a) del RGPD, que 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 Reglamento.

La LOPDGDD en su artículo 71, *Infraccione*s, 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 72, considera a efectos de prescripción, que son: *"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

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, al permi-

tir el acceso a los datos carácter personal pertenecientes a una tercera persona al serle remitido a la reclamante en el ámbito de una queja informe médico de dicho tercero.

VI

En segundo lugar, hay que señalar que la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD.

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".

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 volu-

men 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".
(…)"

VIII

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 del RGPD, al producirse un incidente de seguridad al serle remitido a la reclamante como consecuencia de queja interpuesta ante el servicio de atención al cliente de un hospital del sistema público sanitario de la CAM informe médico conteniendo datos de una tercera persona, quebrantando 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 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".

En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación E/05274/2021 la AEPD trasladó al reclamado el 14/05/2021 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, sin que diera respuesta al citado requerimiento.

No obstante, el reclamado ha señalado en escrito de **(...)** que *"no es hasta el pasado 27/09/2021 cuando este Comité ha tenido conocimiento del mismo, dado que han existido incidencias de distinta índole en el Registro de entrada".* En este escrito facilita información detallada de la incidencia producida y decisiones adoptadas.

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. En este caso, si bien la parte reclamada afirma que disponía de medidas de seguridad tendentes a evitar incidentes como este, lo cierto es que no se cumplieron, propiciando la brecha de seguridad

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del artículo 32.1 del RGPD, 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:

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 infracción a lo dispuesto en los artículos 5.1.f) y 32.1 del RGPD.

Hay que señalar que la LOPDGDD, en coherencia con lo establecido en su artículo 83 RGPD, 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.

El Hospital perteneciente a la red sanitaria pública perteneciente a la CAM donde se produjo la incidencia ha señalado en el informe presentado que *"cuando se recibió la reclamación, de forma inmediata se recopiló toda la información relativa a los hechos, de cara a poder identificar las causas del incidente y prevenir que puedan volver a repetirse en un futuro. Además, de recordar al personal la importancia de extremar al máximo el cuidado en las contestaciones remitidas, debiendo comprobar en más de una ocasión que los datos personales introducidos son los correctos, dada la relevancia y sensibilidad de los datos personales de los pacientes y su especial protección"* Cita su compromiso con la normativa conforme a la *"Guía de pacientes y usuarios de la Sanidad"* elaborada por la AEPD y que todo se debió a *"un error al elaborar la contestación dirigida a* la reclamante, *al transcribir una dirección y destinatario que eran incorrectos…"*

Por su parte el reclamado en su escrito ha señalado que todo se debió a un error humano puntual y que "*la Consejería de Sanidad de la Comunidad de Madrid tiene implementadas medidas para preservar la seguridad de la información y los derechos y libertades de los ciudadanos, entre las que se incluyen medidas de naturaleza organizativa que comprenden la formación regular y periódica del personal de los centros asistenciales del Servicio Madrileño de Salud (SERMAS) que se considera como una medida idónea para prevenir errores humanos como el acaecido. Si bien esta medida se considera adecuada, no impide que los mismos ocurran, no obstante, tal y como puede apreciarse y se ha manifestado, se trata del primer error del que se tiene constancia. En cualquier caso, este CDPD procederá a revisar el plan de formación del centro para valorar si se requiere una formación adicional en su centro de trabajo".*

Por tanto, se considera que la respuesta del reclamado ha sido razonable, habiéndose subsanando la incidencia que había afectado a una sola persona, no proce-

diendo instar la adopción de medidas adicionales, al haber adoptado medidas de carácter técnico y organizativas de conformidad con la normativa en materia de protección de datos para evitar que se vuelvan a producirse situaciones como la que dio lugar a la presente reclamación, que es la finalidad principal de los procedimientos respecto de aquellas entidades relacionadas en el artículo 77 de la LOPDGDD.

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 CONSEJERÍA DE SANIDAD de la CAM, con NIF ***S7800001E*** por infracción de los artículos 32.1 y 5.1.f) del RGPD, tipificadas en el artículo 83.4.a) y 83.5.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a CONSEJERÍA DE SANIDAD de la CAM.

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