- **Expediente N.º: PS/00587/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 22 de noviembre de 2020, ***A.A.A.*** (en adelante, la parte reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E, (en adelante, la parte reclamada).

La parte reclamante expone que, el día 16 de mayo de 2020, presentó una reclamación ante la Dirección del Hospital Universitario de la Paz donde trabajaba, por el presunto acceso indebido a su historia clínica por parte de una compañera de trabajo ***B.B.B.*** y que únicamente ha recibido respuesta de que se daba traslado de su reclamación a la Dirección Médica del Hospital La Paz para su investigación.

Indica que el día 13 de mayo de 2020, en torno a las 8 horas de la mañana, la citada enfermera, del servicio de quirófano en el edificio general del Hospital Universitario la Paz de Madrid, aprovechándose de su condición de enfermera y utilizando sus claves personales de acceso, entró, sin que mediara relación asistencial ninguna, en su historia clínica, sita en la base de datos "sistema informático HCIS".

Manifiesta que el mismo día 13 de mayo de 2020, informó de los hechos descritos a la supervisión de enfermería del servicio de quirófano donde trabajaba la enfermera, así como a la Dirección de Enfermería del Hospital la Paz.

Aporta escrito de fecha 20/05/2020, donde el jefe del Servicio de Información del Hospital Universitario La Paz comunica a la reclamante el traslado a la Dirección Médica del centro de la notificación sobre “accesos indebidos a su historia clínica” y la reclamación interpuesta ante Salud Madrid.

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 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 contestación al traslado de la reclamación.

TERCERO: En fecha 26 de abril de 2021, 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 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 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos de la parte reclamada:

CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E, con domicilio en C/ MELCHOR FERNÁNDEZ ALMAGRO, N.º 1 - 28029 MADRID (MADRID).

En fecha 24/05/2021, se requiere información a la parte reclamada en el marco del presente expediente de investigación. No recibiendo contestación, se reitera el requerimiento, recibiéndose respuesta con los siguientes resultados:

Sobre los accesos.

Se ha solicitado copia del registro de accesos al sistema de información del Hospital de La Paz del día 13/05/2020 donde consten los accesos realizados por la enfermera citada por la reclamante. Se pide aportar fecha y hora de los accesos, el detalle de la tipología de los datos accedidos, así como documentación acreditativa de la justificación existente para dichos accesos.

Ante ello, la parte reclamada únicamente indica que el Hospital Universitario La Paz ha realizado una investigación de los hechos y ha concluido que se han producido accesos por parte de la enfermera citada por la reclamante, en el tramo de horario en que ésta acude a Urgencias a las 3:46 a.m. hasta que recibe el alta el mismo día a las 10:12 a.m.

Sobre las investigaciones de los accesos.

Se ha solicitado copia de las investigaciones oportunas que se mencionan en el documento del Servicio de Atención al Paciente, así como la contestación final emitida a la reclamante, adjuntando al requerimiento de esta Agencia copia del documento aportado por la reclamante donde el Jefe del Servicio de Información del Hospital Universitario La Paz le comunica el traslado a la Dirección Médica del centro de la notificación sobre *"accesos indebidos a su historia clínica"* para que *"se proceda a realizar las investigaciones oportunas".*

A este respecto la parte reclamada indica que el Hospital de la Paz ha llevado a cabo las oportunas investigaciones para esclarecer los hechos descritos por la denunciante.

No aportan copia de las investigaciones requeridas. Aportan copia de un escrito fechado el 18/12/2020, indicando que es la respuesta final remitida a la reclamante, en el que el Hospital indica que la Dirección no se pondrá en contacto con ella porque *"se*

lleva a cabo una auditoria y se toman las acciones oportunas, pero ello no conlleva que se informe a la interesada".

Indican a esta Agencia que el citado Hospital cuenta con un protocolo según el cual "*si se han producido accesos indebidos, se ha de valorar en el Comité de Protección de Datos (PD) qué información se le daría al interesado, siempre informándole de que el derecho concedido al mismo por la propia LOPD únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de la organización del responsable del fichero han podido tener acceso a dicha información"*.

Adjuntan el citado protocolo titulado Auditorías de verificación del cumplimiento en los accesos a HC (Historia Clínica), cuya copia obra en las presentes actuaciones de inspección.

Sobre las acciones tomadas con objeto de minimizar los efectos adversos y para la resolución final del incidente.

Aportan a este respecto Informe del Hospital la Paz en el que se detalla la secuencia de los hechos, así como copia los informes de la Dirección de Enfermería.

En uno de estos informes de la Dirección de Enfermería del Hospital La Paz consta:

"El jueves día 13 de mayo […la reclamante…] solicita reunión conmigo para informarme de un hecho que se ha producido y que yo, como Supervisora de la Unidad, sea conocedora. Ha pasado la noche en urgencias ya que, estando de guardia en el quirófano, comienza con […]. Durante su estancia en urgencias, recibe un WhatsApp de una compañera suya del quirófano donde pone textualmente "la placa está bien". […la reclamante…] le responde "¿cómo lo sabes? ¿Has mirado mi Historia clínica? Su compañera le responde que efectivamente lo ha consultado en su historia, pidiéndole disculpas en ese mismo momento.

[…la reclamante…]refiere que este hecho atenta gravemente contra su intimidad y que esta compañera (cito palabras textuales) "le ha estado haciendo la vida imposible durante 3 años, y esto es la gota que colma el vaso".

Viendo la gravedad del asunto, aviso a mi Adjunto de Área y […la reclamante…] le manifiesta su deseo de que estos hechos no queden impunes.

Así mismo, hablamos con la compañera que ha entrado en la historia clínica admitiendo de inmediato su error y pidiendo disculpas en reiteradas ocasiones. Manifiesta su deseo de hablar con […la reclamante…] y pedirle disculpas. Una vez hablado con las dos partes implicadas y, ante la demanda de […la reclamante…], se le informa de las vías que dispone en el hospital para hacer las reclamaciones que considere oportunas. También se le comunica que su compañera está interesada en pedirle disculpas personalmente por el hecho de consultar su Historia sin su permiso y por si en algún momento de su relación profesional se ha sentido agraviada con su actitud hacia ella."

Sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

Únicamente hacen mención nuevamente al protocolo de Auditorías de verificación del cumplimiento en los accesos a HC (Historia Clínica) de fecha de edición el 23/03/2021, indicando que se puede observar en el apartado 4 (Desarrollo), un proceso de auditorías reactivas y proactivas siendo estas últimas de carácter mensual y siguiendo una estructura y seguimiento concreto, para atender los requerimientos de la Consejería de Sanidad en caso de accesos indebidos a historias clínicas.

Respecto de la seguridad de los tratamientos de datos personales existente con anterioridad a los hechos.

Se ha pedido detallar las medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado a los riesgos detectados con relación a los accesos por el personal sanitario a los historiales clínicos de los pacientes y la Política de seguridad adoptada por la entidad con relación a ello.

Mencionan al respecto que, en la Política de Seguridad de la Consejería de Sanidad, cuya copia aportan, se incluye un *"Decálogo de buenas prácticas para usuarios de sistemas de información de la Consejería de Sanidad*" que es de obligatorio cumplimiento para todo el personal que preste servicios en la Consejería *(artículo 12.2).*

Respecto al deber de respetar la privacidad de los datos, entre otras obligaciones, en el Decálogo se establecen las siguientes:

- Los usuarios deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la que esté autorizado (3.1).

- En el acceso a esta información los usuarios están obligados a cumplir todas las medidas de seguridad establecidas por la normativa en protección de datos, y demás requisitos aplicables conforme a las normas y procedimientos establecidos en la CSCM (3.2).

- Todas las personas que intervengan en cualquier fase del tratamiento de datos de carácter personal están obligadas al secreto profesional respecto de estos (3.3).

Indican que la referida Política de Seguridad contempla que "*El incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente Decálogo de buenas prácticas podrá dar lugar a la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar, en aplicación de las normas reguladoras del régimen jurídico disciplinario propio del usuario".*

Manifiestan que el Hospital Universitario La Paz cuenta con una serie de medidas establecidas con el fin de mantener y consolidar la seguridad de la información y privacidad, como por ejemplo la conservación de las trazas de acceso y la realización periódica de formaciones dirigidas al personal.

QUINTO: En fecha 3 de enero de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en

adelante, LPACAP), por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD, respectivamente.

El acuerdo de inicio fue enviado, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibido en fecha 5 de enero de 2022, como consta en el certificado que obra en el expediente.

SEXTO: Notificado el acuerdo de inicio, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba:

-que el Hospital Responsable del Tratamiento de los Datos, Hospital Universitario La Paz (HULP), realizó una investigación de los hechos, concluyendo tras la misma que se produjeron accesos indebidos a su historia clínica durante el intervalo en el que la denunciante se encontraba en Urgencias (3:46 a.m. hasta las 10:12 a.m. del mismo día en el que recibe el alta: el 13 de junio de 2020),

-que existen medidas de seguridad adecuadas y suficientes para la gestión de Historias Clínicas, toda vez que se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa, contando el centro con un protocolo establecido a tales efectos, en el que se recoge un proceso de auditorías reactivas y proactivas, siendo estas últimas de carácter mensual y siguiendo una estructura y seguimiento concreto, para atender los requerimientos de la Consejería de Sanidad en caso de accesos indebidos a historias clínicas,

-que cuentan con una Política de seguridad a nivel de la Consejería de Sanidad, que prevé medidas organizativas específicas para el mantenimiento de la confidencialidad de la información a la que acceden los trabajadores de la organización,

-que en el sistema de gestión de historias clínicas existe una segregación de perfiles para la utilización de la herramienta, en base al desempeño del trabajo de cada uno de los puestos.

Se adjunta el documento que establece la asignación de Usuarios y perfiles tipo, en el que exponen que: "*puede comprobarse que se da el debido cumplimiento al principio de mínimo privilegio, de conformidad con lo estipulado en el Anexo II [op.acc.3] del Esquema Nacional de Seguridad limitando a cada usuario a lo mínimo estrictamente necesario para cumplir sus obligaciones. Asimismo, los privilegios se limitan de forma que los usuarios sólo acceden a información necesaria para el cumplimiento de sus funciones.*

Por tanto, existen distintos modelos de usuarios definidos, como son:

- *Usuario Administrativo*
- *Usuario Médico (uno por especialidad)*
- *Usuario Enfermero (matronas, supervisoras, enfermeras)*
- *Usuario Consulta (solo da acceso a ver la información, pero no permite registro)*
- *Usuario para otros colectivos no médicos*

Los modelos de usuarios están compuestos por diferentes perfiles, y cada perfil permite el acceso a determinadas funciones o competencias, teniendo siempre presente que, según la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 16 se indica que la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, es decir, la historia clínica debe ser accesible de forma tal que se pueda asegurar que se presta una adecuada asistencia a cada paciente, teniendo en cuenta la diversidad de profesionales sanitarios existentes en el centro. Por ejemplo, en los supuestos de urgencias, esta historia clínica debe ser accesible para asegurar los intereses vitales de cada ciudadano.

Cuando un profesional se incorpora al centro, se le asigna el usuario modelo establecido, pero si el profesional cambia sus funciones o precisa funciones nuevas, debe tener el visto bueno de la Dirección. En el caso de que un usuario, reclame nuevas funciones y no exista un usuario modelo establecido, la Dirección valora la pertinencia de crear un usuario modelo nuevo.

Así pues, y como podemos observar en el protocolo, no existen usuarios genéricos, sino más bien, son usuarios creados de acuerdo con las funciones que tienen asignadas, siendo el acceso unívoco y nominal por cada profesional con su número de DNI personal."

-que cuentan con la firma de un Compromiso de Confidencialidad, mediante el cual se informa al trabajador en el momento de formalizar su contrato con el hospital, sobre las políticas de seguridad y privacidad de obligado cumplimiento de los trabajadores del Centro Hospitalario,

-que se imparten formaciones respecto a la seguridad de los datos de carácter personal,

-que la parte reclamada reconoció su error y pidió disculpas a la parte reclamante, indicando la falta de intencionalidad al acceder a su información, por lo que entienden que las medidas de seguridad tanto técnicas como organizativas, llevadas a cabo por el responsable del Tratamiento, son óptimas y válidas para garantizar la seguridad y confidencialidad de los datos de los pacientes.

SÉPTIMO: En fecha 11 de marzo de 2022, la instructora del procedimiento emitió propuesta de resolución por infracción a lo dispuesto en el artículo 5.1 f) del RGPD.

La citada propuesta de resolución fue enviada, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibida en fecha 12 de marzo de 2022, como consta en el certificado que obra en el expediente.

OCTAVO: En fecha 28 de marzo de 2022, la entidad reclamada presentó escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, manifestaba en relación con las medidas de seguridad establecidas que, en aplicación del Esquema Nacional de Seguridad, se registran las actividades de los usuarios, reteniendo la infor-

mación necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa, que cuentan con la implantación de un proceso de auditorías reactivas y proactivas siendo estas últimas de carácter mensual y siguiendo una estructura y seguimiento concreto, para atender los requerimientos de la Consejería de Sanidad en caso de accesos indebidos a historias clínicas, que existe una segregación de perfiles para la utilización de la herramienta, en base al desempeño del trabajo de cada uno de los puestos, limitando a cada usuario el acceso a lo mínimo, que por parte de los empleados se firma un Compromiso de Confidencialidad, mediante el cual se le informa al trabajador en el momento de formalizar su relación de sus deberes en esta materia y que aparece un recuadro informativo (banner) que advierte que el acceso a la plataforma debe realizarse con fines asistenciales.

Y en relación con otras consideraciones, afirma que la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, es decir, la historia clínica debe ser accesible de forma tal que se pueda asegurar que se presta una adecuada asistencia a cada paciente, que se imparten formaciones respecto a la seguridad de los datos de carácter personal, que se realizaron las oportunas investigaciones, las cuales derivaron en las acciones necesarias para solventar los hechos ocurridos, pudiendo identificar en todo momento la persona que realizó el acceso indebido a la historia y que las medidas mitigantes efectuadas por el Hospital, atendiendo a la solicitud de la afectada, han consistido en un apercibimiento

Finalmente menciona el procedimiento Sancionador de la AEPD Procedimiento Nº: AP/00056/2014. En dicha resolución emitida el 9 de febrero de 2021, la AEPD tuvo ocasión de pronunciarse sobre el posible acceso indebido e injustificado a la historia clínica de un paciente trabajador del Servicio Madrileño de Salud. La AEPD, afirma el interesado, habría llegado a la conclusión de que el SERMAS tenía establecidas medidas de seguridad suficientes.

NOVENO: A la vista de los hechos considerados probados y de acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) y en uso de la facultad prevista en el artículo 90.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en fecha 23 de agosto de 2022, se notifica a la parte reclamada la consideración de que, de los hechos probados, se extrae no sólo la infracción del artículo 5.1.f) del RGPD, sino también la del artículo 32 del mismo texto legal.

DÉCIMO: Notificada la Propuesta de Resolución, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que una adecuada prestación de la asistencia sanitaria implica la participación de varios servicios del mismo centro para la consecución del fin último del bienestar y salud del paciente, que, de hecho, en la práctica sanitaria, es habitual que un servicio de urgencias pueda derivar en un servicio de quirófano, en el que se haría estrictamente necesario para preservar los intereses vitales del afectado, el que el personal sanitario de ambos servicios tenga acceso inmediato a la historia clínica del paciente para poder prestar una adecuada asistencia sanitaria de urgencia.

Aportan informe emitido por el Hospital Universitario de La Paz en el que se indica, en relación con la medida propuesta por la AEPD de que cada uno de los profesionales pudiera tener acceso a las historias clínicas únicamente de aquellos pacientes sobre los cuales despliegan su actividad, que dicha medida es sumamente compleja y difícil de aplicar tanto a nivel técnico como organizativo, y sobre todo desde el punto de vista asistencial , y ello porque los profesionales sanitarios y en especial el área de enfermería, están sujetos a continuos cambios de turnos; pueden desempeñar su actividad de forma rotatoria, pasando del turno de mañana a tarde o noche. De igual modo, y respecto a la unidad, servicio o especialidad médica, tampoco se podría aplicar criterios de exclusión ya que el personal sanitario puede cambiar de ubicación. Un profesional puede desempeñar su actividad en una planta o especialidad y al día siguiente o turno siguiente en otra diferente.

Consideran por tanto que el personal sanitario debe tener acceso a las diferentes pruebas diagnósticas realizadas o consultar informes de otros especialistas y/o profesionales que puedan influir en la patología que está tratando. Añaden además que los pacientes pueden ejercer su derecho de Libre Elección de Especialista, Libre Elección de Centro Sanitario, solicitar una según opinión o ser canalizado a petición facultativa a diferente centro para llevar a cabo una prueba o tratamiento no incluido en la cartera de servicio del centro de origen. Ante estas situaciones, los profesionales sanitarios, tienen que poder tener acceso al historial clínico íntegro del paciente para ofrecer una adecuada atención al enfermo.

Por último, estiman necesario que los perfiles del sistema de configuración vengan configurados como se encuentran hasta ahora puesto que es la mejor forma de preservar la salud de los pacientes que acuden al hospital donde se les presta asistencia sanitaria e indican que ya existe una fuerte segregación de perfiles para la utilización de la herramienta, en base al desempeño del trabajo de cada uno de los puestos, limitando a cada usuario el acceso a lo mínimo.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: En fecha 22 de noviembre de 2020, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, por el presunto acceso indebido a su historia clínica, por parte de una compañera de trabajo.

SEGUNDO: El Hospital Responsable del Tratamiento de los Datos, realizó una investigación de los hechos, concluyendo tras la misma que se produjeron accesos indebidos a su historia clínica durante el intervalo en el que la denunciante se encontraba en Urgencias (3:46 a.m. hasta las 10:12 a.m. del mismo día en el que recibe el alta: el 13 de junio de 2020).

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada

autoridad de control y según lo establecido en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento, la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

En respuesta a las alegaciones presentadas por la entidad reclamada al Acuerdo de inicio del procedimiento sancionador, se debe señalar lo siguiente:

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra 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."*

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, como consecuencia de la exposición a tercera persona ajena, de los datos personales relativos a la salud de la parte reclamante.

El artículo 32 del RGPD señala lo siguiente:

"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.".

El citado artículo contempla que "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".* En consecuencia, no adopta una relación cerrada de medidas técnicas y organizativas, sino que éstas deberán ser las apropiadas en función del nivel de riesgo previamente analizado.

Dicho lo anterior, el artículo 32.1 recoge una obligación de medios y no una obligación de resultado. En efecto, indica que *"el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo,*". Es decir, impone la obligación de establecer un nivel de seguridad, y ese nivel debe estar en función del análisis de riesgos que todo responsable debe efectuar conforme al apartado 2 de dicho artículo:

> *"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."*

La evolución tecnológica y sofisticación de los sistemas de acceso no autorizado a sistemas de datos hace que la normativa no pueda imponer de manera incondicionada un aseguramiento total de la ausencia de brechas de integridad o confidencialidad. Pero sí obliga a que los responsables de los tratamientos deban realizar un análisis de riesgos y a la implantación de un "nivel de seguridad adecuado" a los mismos.

Se caracteriza por lo tanto este deber como una obligación de medios. Así lo ha declarado el Tribunal Supremo en su reciente sentencia de 15 de febrero de 2022:

> *"La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.*
>
> *En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su*

consecución, por ello se las denomina obligaciones "de diligencia" o "de comportamiento".

La diferencia radica en la responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

En estas últimas, la suficiencia de las medidas de seguridad que el responsable ha de establecer ha de ponerse en relación con el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados, pero no se garantiza un resultado. Como establece el art. 17.1 de la Directiva 95/46/CE respecto a la seguridad del tratamiento el responsable del tratamiento tiene la obligación de aplicar las medidas técnicas y organizativas adecuadas «Dichas medias deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de aplicación, un nivel de seguridad apropiados en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse». Y en el mismo sentido se pronuncia en la actualidad el art. 31 del Reglamento de la Unión Europea 2016/679, del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, al establecer respecto a la seguridad del tratamiento que las medidas técnicas y organizativas apropiadas lo son «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 […]».

Ya hemos razonado que la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado."

Fijado lo anterior, esto es, que la obligación de medios impuesta por el artículo 32 del RGPD consiste en adoptar las medidas de seguridad en el tratamiento, tendentes a evitar la producción de una brecha de seguridad en el mismo. Estas obligaciones deben ser establecidas en función de los riesgos que hayan sido analizados, y teniendo en cuenta el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados.

En consecuencia, el análisis debe realizarse para determinar si se ha producido el incumplimiento consiste en la determinación de si las medidas eran suficientes para evitar el riesgo de brecha de seguridad. En este caso, se debe comprobar si las medidas eran adecuadas para garantizar que no se produjese un acceso no autorizado a la his-

toria clínica de la reclamante como el que se produjo en este supuesto. Ello con independencia de que dicho acceso se produjera efectivamente, o no.

Procede analizar las alegaciones aportadas en este procedimiento por la CONSEJERÍA DE SANIDAD. En relación con las medidas de seguridad establecidas:

- En aplicación del Esquema Nacional de Seguridad se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa

- Implantación de un proceso de auditorías reactivas y proactivas siendo estas últimas de carácter mensual y siguiendo una estructura y seguimiento concreto, para atender los requerimientos de la Consejería de Sanidad en caso de accesos indebidos a historias clínicas

- Existe una segregación de perfiles para la utilización de la herramienta, en base al desempeño del trabajo de cada uno de los puestos, limitando a cada usuario el acceso a lo mínimo.

- Por parte de los empleados se firma un Compromiso de Confidencialidad, mediante el cual se le informa al trabajador en el momento de formalizar su relación de sus deberes en esta materia.

- Aparece un recuadro informativo (banner) que advierte que el acceso a la plataforma debe realizarse con fines asistenciales

Y en relación con otras consideraciones afirma:

- La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, es decir, la historia clínica debe ser accesible de forma tal que se pueda asegurar que se presta una adecuada asistencia a cada paciente

- Se imparten formaciones respecto a la seguridad de los datos de carácter personal

- Se realizaron las oportunas investigaciones, las cuales derivaron en las acciones necesarias para solventar los hechos ocurridos, pudiendo identificar en todo momento la persona que realizó el acceso indebido a la historia.

- Las medidas mitigantes efectuadas por el Hospital, atendiendo a la solicitud de la afectada, han consistido en un apercibimiento

Finalmente menciona el procedimiento Sancionador de la AEPD Procedimiento Nº: AP/00056/2014. En dicha resolución emitida el 9 de febrero de 2021, la AEPD tuvo ocasión de pronunciarse sobre el posible acceso indebido e injustificado a la historia clínica de un paciente trabajador del Servicio Madrileño de Salud. La AEPD, afirma el interesado, habría llegado a la conclusión de que el SERMAS tenía establecidas medidas de seguridad suficientes.

En relación con estas alegaciones, debe significarse lo siguiente:

De las cinco medidas de seguridad descritas, ya de principio puede descartarse que cuatro de ellas puedan ser eficaces para la prevención de un acceso no autorizado. En primer lugar, el registro de accesos o la realización de auditorías son medidas para reaccionar a posteriori, una vez el acceso se hubiera producido. En segundo, el banner tiene únicamente efectos informativos, sin que impida continuar al profesional en caso de que el acceso no estuviera justificado. Finalmente, el compromiso de confidencialidad tampoco evita, de por sí, un acceso no autorizado.

Únicamente la segmentación de perfiles de acceso a las historias clínicas podría considerarse una herramienta válida y eficaz para la evitación de sucesos como el presente caso. La CONSEJERÍA DE SANIDAD aporta un muy detallado anexo con los perfiles de cada uno de los tipos de categoría profesional, distinguiendo entre personal administrativo y sanitario, y dentro de esta última categoría, por tipos y especialidades de personal.

Ahora bien, no viene reflejada en el documento una medida que sería básica, y es que cada uno de los profesionales sanitarios pudiera tener acceso a las historias clínicas únicamente de aquellos pacientes sobre los cuales despliegan su actividad asistencial.

En este sentido, el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica dispone que "1*. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.*
2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten" (el subrayado es nuestro).

De la lectura de este precepto se infiere con claridad que, si bien la historia clínica es el instrumento para prestar la asistencia sanitaria al paciente, lo que debe quedar debidamente garantizado, también lo es el hecho de que sólo puede producirse el acceso a la historia clínica por los profesionales que le asisten, no con carácter general, sino con carácter particular realizando la diagnosis o el tratamiento del paciente.

Recordemos que el supuesto de hecho que ha dado lugar a este procedimiento consiste en el acceso por parte de una persona de enfermería del Servicio de Quirófanos respecto a una paciente que recibió asistencia médica en el Servicio de Urgencias.

Es cierto que, como afirma el interesado, "la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, es decir, la historia clínica debe ser accesible de forma tal que se pueda asegurar que se presta una adecuada asistencia a cada paciente", pero no lo es menos que pueden implantarse medidas, en función de los pacientes asignados a cada profesional, del servicio en que se desempeñen las labores sanitarias, y de los turnos de trabajo de cada profesional, que eviten que por parte de un profesional pueda accederse a datos médicos res-

pecto de un paciente sobre el cual no se tiene encomendada actividad asistencial alguna. La fuerte segregación de perfiles que dicen que tienen implantada no ha impedido el acceso a la historia clínica de una paciente, por parte de una enfermera que no tenía encomendado el tratamiento de la paciente. Ello denota la ausencia de medidas de seguridad adecuadas.

La falta de adopción de una medida como la descrita hace que no pueda considerarse que existan unas medidas de seguridad que aporten un nivel de protección adecuado a los riesgos existentes. De hecho, la propia CONSEJERÍA DE SANIDAD reconoce la antijuridicidad de la conducta, toda vez que tramitó un expediente disciplinario contra la persona que realizó el acceso indebido, y que concluyó con la imposición de un apercibimiento.

En relación con el precedente invocado (exp. AP/00056/2014), es preciso señalar que se trata de un procedimiento sancionador que se llevó a cabo por hechos muy anteriores a la entrada en vigor del RGPD. Este último entró en vigor en mayo de 2018, mientras que los hechos sucedieron en mayo de 2013. En dicho expediente, se llevó a cabo un archivo de actuaciones basado en que la CONSEJERÍA DE SANIDAD acreditó tener en práctica las medidas exigidas por el ya derogado Real Decreto 1720/2007, de 21 diciembre, (RLOPD) por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal. (LOPD)

El sistema establecido por la anterior LOPD difiere sustancialmente del instaurado por el vigente RGPD. Mientras que aquella establecía un sistema de medidas de seguridad establecidas normativamente (en conjunción con el RLOPD) para entenderse cumplidas las obligaciones en materia de seguridad, el vigente RGPD se basa en los principios de responsabilidad proactiva y protección de datos desde el diseño, esto es, en el establecimiento de las medidas que sean necesarias en función de los riesgos apreciados inherentes a un determinado tratamiento. No existe, por lo tanto, un *numerus clausus* de medidas que el responsable de un tratamiento deba adoptar, sino que estas deben ser establecidas caso a caso, en función del análisis de riesgo y de los datos que están siendo objeto de tratamiento.

A este respecto, el artículo 5.2 RGPD establece, tras la enumeración de los principios relativos a la protección de datos personales, lo siguiente:

> *"2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."*

Y en cuanto al principio de protección de datos desde el diseño, el RGPD exige:

> *"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en*

el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados"

Por todo ello, la referencia al precedente constituido por el expediente AP/00056/2014 carece de toda virtualidad, toda vez que fue tramitado al amparo de una normativa radicalmente diferente a la actual.

Por lo demás, el criterio de la AEPD en relación con este tipo de accesos no autorizados tiene un precedente claro, producido en un procedimiento sancionador tramitado tras la entrada en vigor del RGPD. Se trata del expediente referencia PS/00250/2021, en que se sancionó al SERVICIO EXTREMEÑO DE SALUD por un problema idéntico al que nos ocupa en este expediente. En la narración de los hechos figura:

"Las actuaciones de inspección se inician por la recepción de un escrito de reclamación de A.A.A. (en adelante, el reclamante), en el que manifiesta que se han producido accesos indebidos a su historia clínica por parte de una trabajadora del Servicio Extremeño de Salud (en adelante SES), con categoría profesional de enfermera. Los accesos se realizan sin la autorización del reclamante y sin que medie una relación que lo justifique."

Este procedimiento debería concluir con la imposición de dos sanciones por estos hechos: una por la vulneración del artículo 5.1.f) RGPD, en los términos explicitados en la propuesta de resolución y otra por la del artículo 32 Reglamento. Ese es el criterio de esta Agencia en relación con este tipo de supuestos.

III

En respuesta a las últimas alegaciones presentadas por la entidad reclamada, se debe señalar lo siguiente:

En primer lugar, nos encontramos ante una categoría especial de datos personales (artículo 9.1 RGPD) a la que es aplicable el principio de prohibición de tratamiento, salvo que concurra alguna de las circunstancias previstas en su apartado 2. Por tanto, incorporan un peligro innato, y deben someterse a un estándar de protección más elevado.

El considerando 51 dispone, sobre las categorías especiales de datos personales, que:

"*Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. […] Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma*

explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales".

Resulta prioritario determinar el papel desempeñado por la Consejería de Sanidad.

Se deduce que el responsable del tratamiento de los datos que forman parte de la historia clínica es el centro sanitario, público o privado; éstos tienen la obligación de elaborarla, custodiarla e implantar las medidas de seguridad necesarias para que no se extravíe, no se comunique a partes no interesadas o pueda accederse por terceros no autorizados.

El RGPD introduce explícitamente el principio de responsabilidad (artículo 5.2 RGPD), es decir, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 del artículo 5 y ha de ser capaz de demostrarlo "responsabilidad proactiva".

El Informe 0064/2020 del Gabinete Jurídico de la AEPD ha expresado con rotundidad que "*El RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)".*

La parte reclamada, en su condición de responsable de dicho tratamiento, debería haber adoptado e implementado, en forma proactiva, las medidas técnicas y organizativas que resultasen apropiadas para evaluar y garantizar un nivel de seguridad adecuado a los probables riesgos de diversa naturaleza y gravedad vinculados a los tratamientos de datos de salud realizados.

A estos efectos, el artículo 24 del RGPD bajo el epígrafe "Responsabilidad del responsable del tratamiento" dispone:

> *"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*
> *2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. (…)"*

Por su parte, el artículo 25 del RGPD bajo el epígrafe "Protección de datos desde el diseño y por defecto" dispone:

> *"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de di-*

versa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. (…)"

Asimismo, la LOPDGDD en el artículo 28.1 señala que:

"Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable."

En consecuencia, debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el RGPD, incluida la eficacia de las medidas (RGPD considerando 74).

En síntesis, este principio exige una actitud consciente, diligente, comprometida y proactiva por parte del responsable frente a todos los tratamientos de datos personales que lleve a cabo.

En el presente caso, se imputa a la entidad reclamada la falta de implementación de las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo derivado del tratamiento de datos de salud de los pacientes (categoría especial de datos personales conforme a lo dispuesto en el artículo 9.1 del RGPD), en orden a impedir la vulneración del principio de confidencialidad, tal y como se desprende de la valoración del conjunto de hechos analizados.

Con carácter general, debe señalarse que en el tratamiento de historias clínicas no debe esperarse a que se haya producido el acceso indebido para reaccionar después (lo que desplazaría la responsabilidad al trabajador en lugar de al responsable del tratamiento) sino, en función de los mencionados principios de responsabilidad proactiva y protección de datos desde del diseño, evitar que los accesos indebidos se produzcan.

De lo expuesto, se evidencia que el reclamado, como responsable del tratamiento objeto de estudio, no ha mostrado la diligencia que le resultaba exigible para establecer las medidas de seguridad que resultan necesarias para evitar la filtración o difusión de este tipo de datos a terceros. En este sentido, la configuración de las medidas técnicas y organizativas debe realizarse para que, con carácter previo a la realización de los tratamientos de datos personales, se garantice que únicamente pueda tener acceso a las historias aquel personal que desarrolle su actividad asistencial sobre el titular de estas.

En caso de que la aplicación informática que controle el acceso a las historias clínicas estuviera correctamente programada, podría determinar, en el momento en que se solicita el acceso, si quien lo solicita (en función de su especialidad, turno o actividad en ese momento) debe estar legitimado para acceder a ella.

Por último, la protección de datos desde el diseño debe complementarse con la realización periódica de auditorías, de modo que puedan detectarse fallos en el sistema que, a su vez, aconsejen modificar los protocolos de acceso en caso de accesos indebidos.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

Se imputa a la entidad reclamada la comisión de una infracción por vulneración del artículo 5.1.f) del RGPD, que rige el principio de confidencialidad e integridad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento y artículo 32 del RGPD.

IV

Sobre el dato de salud señala el considerando 35 del RGPD lo siguiente:

"Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro."

Por su parte, el artículo 4 del RGPD define:

"2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;"

V

El tratamiento de datos de las historias clínicas se encuentra regulado en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Su artículo 3 señala:

"Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

En el artículo 16, se establecen los usos de la historia clínica:

"*1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.*

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten."

VI
Artículo 5.1.f) del RGPD

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

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»)."

En relación con este principio, el Considerando 39 del referido RGPD señala que:

"[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Hay que añadir que, en relación con la categoría de datos a la que tercera persona ajena ha tenido acceso, se encuentran en la categoría de especiales según lo dispuesto en el art. 9 del RGPD, circunstancia que supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

En consecuencia, se considera que los hechos acreditados son constitutivos de infracción, imputable a la parte reclamada, por vulneración del artículo 5.1.f) del RGPD.

VII
Tipificación de la infracción del artículo 5.1.f) del RGPD

El artículo 83.5 del RGPD dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del

volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "Infracciones" determina lo siguiente:

"*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica."*

A efectos del plazo de prescripción de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente:

"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."

VIII

Artículo 32 del RGPD

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

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 (El subrayado es de la AEPD).

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En el presente caso, tal y como consta en los hechos y en el marco del expediente E/05028/2021, la AEPD solicitó aportar fecha y hora de los accesos, el detalle de la tipología de los datos accedidos, así como la documentación acreditativa de la justificación existente para dichos accesos. En la documentación aportada, el reclamado sólo reconoce la existencia de dichos accesos si bien no se pronuncia sobre la legitimidad de estos ni aporta copia de la investigación requerida.

La consecuencia de esta implantación de medidas deficientes de seguridad fue la exposición a tercera persona ajena de los datos personales relativos a la salud de la parte reclamante. Es decir, la afectada se ha visto desprovista del control sobre sus datos personales relativos a su historial clínico.

Hay que añadir que, en relación con la categoría de datos a la que tercera persona ajena ha tenido acceso, se encuentran en la categoría de especiales según lo dispuesto en el art. 9 del RGPD, circunstancia que supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por el responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

Por tanto, los hechos acreditados son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

IX

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica"*.

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679"

X

Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

XI
Sanción

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

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."*

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

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

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

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.

(…)

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."

En el presente caso se estima adecuado sancionar con apercibimiento a la parte reclamada, por infracción del artículo 5.1.f) del RGPD y por la infracción del artículo 32 del RGPD, por la falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad.

XII
Medidas

El artículo 58.2 del RGPD dispone*: "Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

d) 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;"

Asimismo, procede imponer la medida correctiva descrita en el artículo 58.2.d) del RGPD y ordenar a la parte reclamada que, en el plazo de un mes, establezca las medidas de seguridad adecuadas para que se adecúen los tratamientos a las exigencias contempladas en los artículos 5.1 f) y 32 del RGPD, impidiendo que se produzcan situaciones similares en el futuro.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y 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: SANCIONAR con APERCIBIMIENTO a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

SEGUNDO: SANCIONAR con APERCIBIMIENTO a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

TERCERO: REQUERIR a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, que implante, en el plazo de un mes, las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares, así como que informe a esta Agencia en el mismo plazo sobre las medidas adoptadas.

CUARTO: NOTIFICAR la presente resolución a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E.

QUINTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-120722

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