- **Expediente N.º: PS/00293/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 3 de marzo de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra ***SERVICIO DE SALUD DE CASTILLA LA MANCHA*** con NIF ***Q4500146H*** (en adelante, la parte reclamada).

La reclamación se basa en que el reclamante, que trabaja como profesional sanitario en el centro hospitalario ***HOSPITAL.1, denuncia que ******PUESTO.1*** ha enviado por e-mail a varios trabajadores del servicio una tabla con su información personal (nombre, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral)

- El afectado aporta copia del correo electrónico, recibido el 3 de junio de 2020, y captura de pantalla de la tabla adjunta al mismo.

Fecha en la que tuvieron lugar los hechos reclamados: 3 de junio de 2020.

Documentación relevante aportada por la parte reclamante:

- copia del correo electrónico, recibido el 3 de junio de 2020, y captura de pantalla de la tabla adjunta al mismo.

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 23 de marzo de 2021 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.

El traslado, que se practicó 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), fue recogido en fecha 24 de marzo de 2021 como consta en el acuse de recibo que obra en el expediente.

Con fecha 17 de mayo de 2021 se recibe en esta Agencia escrito de respuesta haciendo referencia a varios documentos supuestamente incorporados al escrito.

Sin embargo, al no encontrarse incorporados dichos documentos al escrito de respuesta de la parte reclamada, estos le son requeridos, sin que hasta la fecha estos hayan sido remitidos.

TERCERO: Con fecha 11 de junio de 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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados 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:

Con fecha 20 de abril de 2022, se solicitó información a la reclamada por notificación postal y al Delegado de Protección de Datos de la misma, por notificación electrónica.

Ambos recibieron las notificaciones sin dar respuesta a los requerimientos efectuados, por lo que, en fecha 18 de mayo de 2022 se reitera la solicitud de información que es atendida en fecha 30 de mayo de 2022.

El contenido de la información facilitada, en esencia, es el siguiente:

"Sin perjuicio de lo que corresponda informar a la Gerencia de Coordinación e Inspección SESCAM, teniendo en cuenta el conocimiento de los hechos adquiridos por ese órgano a través de la "información reservada" tramitada por dicha Gerencia en su día (de la que nos consta que existió propuesta de archivo por parte de la Inspectora Instructora del expediente), paso a exponer la información que nos consta siguiendo el orden de los puntos propuesto por la propia AEPD:

1.- Informe de todas las actuaciones que han sido llevadas a cabo como consecuencia del incidente descrito.

(…)

Dicho lo anterior, los jefes de servicio y/o sección de los 44 servicios médicos que suman más de 570 facultativos especialistas de área vinculados a esta Gerencia, tienen la obligación de organizar sus respectivos servicios médicos tomando las correspondientes decisiones asistenciales y organizativas. En esta línea y ya en el periodo inmediatamente posterior a la declaración del estado de alarma en el Estado por la existencia de la pandemia provocada por la COVID-19, los jefes y jefas de servicio médicos adoptaron medidas en sus respectivos servicios con una doble finalidad:

a) Garantizar en lo posible pero con total rigor, la prevención de riesgos laborales de los profesionales médicos, sanitarios y no sanitarios de los empleados-as públicos del Servicio, evitando los contagios por COVID.

b) Garantizar la continuidad asistencial no demorable y minimizar el riesgo de contagio por COVID de pacientes. Este es el caso de los pacientes del Servicio de Oncología radioterápica que por tratarse de pacientes en tratamiento por cáncer no solo no son demorables, sino que precisan de un cuidado especial en la prevención, en este caso, del contagio por COVID-19.

En este sentido y por la finalidad expresada, debería valorase en el contexto y situación crítica generada por la pandemia en que se produjo este hecho, debería valorarse si, como entiende esta Gerencia, existió justificación legal para remitir el correo electrónico con las instrucciones y/o documentos adjuntos que pudiera llevar (según se dice) o tratamiento de los datos, a tenor de lo previsto en el artículo 6.1 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

(…)

Véase la obligación impuesta a esta Gerencia por los artículos 14 y 15 de la ley 31/1995, de prevención de riesgos laborales, así como la función del servicio público de salud respecto de la población atendida, a tenor de lo fijado por la ley 14/1986, General de Sanidad y ley 8/2000 de Ordenación sanitaria de Castilla-La Mancha; es decir, deberá contemplarse la necesidad de protección de los empleados públicos y de los pacientes atendidos.

*Pues bien, de la existencia de un correo electrónico dirigido por B.B.B. como ***PUESTO.1 a los médicos del servicio y a la supervisora de enfermería, esta Gerencia tuvo conocimiento a través de un escrito fechado el 21 de julio de 2020 firmado por la Sra. Presidenta de la Junta de Personal del Área de Salud de ***LOCALIDAD.1 dando cuenta de la existencia del mismo y de un documento adjunto en el que se dice que aparecen nombres de empleados y empleadas del Servicio de Oncología radioterápica y los resultados de un estudio de seroprevalencia,*

(…)

No obstante, esta Gerencia nunca tuvo conocimiento ni del correo electrónico y su contenido, ni del documento con datos de salud que se dice entregado por C.C.C. a la Junta de Personal;

(...)

2.- Descripción detallada de los siguientes puntos:

*a) Según la información verbal facilitada a esta Gerencia por ***PUESTO.1, **B.B.B.**, el correo electrónico, es utilizado como media de hacer llegar instrucciones de servicio y en este caso, siempre según su manifestación fue dirigido exclusivamente a los médicos y a la supervisora de enfermería, pues de una parte los médicos son los que deben conocer con que profesionales trabajan y su situación respecto al COVID para prevenir el contagio de los pacientes al ser el medico el responsable directo del paciente durante la realización de las pruebas y tratamiento de los pacientes; y la*

supervisora al ser la jefa y responsable del personal de enfermería destinado en el servicio de oncología radioterápica.

No obstante, como se ha indicado, desconocemos el contenido del correo electrónico.

b) De haber sido remitido el correo electrónico sin ocultar las direcciones del correo electrónico del resto de profesionales destinatarios, ello podría obedecer a las siguientes razones:

- Tratarse de la dirección de correo electrónico profesional, es decir, la que se utiliza para emitir instrucciones de servicio, organización del servicio, novedades existentes en el mismo, no siendo una dirección privada de correo electrónico.

- Posible necesidad de que todos los destinatarios conozcan que el resto de destinatarios también son conocedores del mensaje para mejor organización y trabajo en equipo propio de la profesión médica y sanitaria.

- Porque si bien la dirección privada de correo electrónico puede considerarse que contiene datos personales, en el ámbito del SESCAM las direcciones corporativas de correo electrónico deben ser conocidas por la necesidad de su uso entre los distintos profesionales médicos y sanitarios para comunicarse entre ellos.

*c) Es de suponer que la "tabla" a la que se alude cuyo contenido desconoce esta Gerencia, no ha sido objeto de tratamiento alguno posterior a su uso, sino que sería eliminada una vez cumplida su finalidad. Así nos ha sido informado por ***PUESTO.1 con carácter previo a la emisión de este documento.*

d) No se han adoptado medidas de seguridad específicas para un hecho que no nos consta, más allá de la información periódica que se traslada a todos los profesionales sobre la regulación normativa de los tratamientos de datos.

3) En su caso, motivo por el cual no se ha notificado la brecha de seguridad a esta Agenda.

Como se infiere de lo expuesto y en especial de lo referido en el punto 1 de este documento, esta Gerencia no tuvo conocimiento de la existencia de la supuesta brecha de seguridad ni de incidentes que la sustenten según la regulación legal existente, sino en todo caso, como se informó a la Presidenta de la Junta de Personal, de actuaciones en el ámbito de gestión del servicio médico.

(…)

4.- En su caso, información sobre si se han producido otros envíos de correos similares sin copia oculta de los destinatarios, con o sin documento adjunto con datos personales.

Esta Gerencia tiene informado a los empleados dependientes de la misma que deben extremar las precauciones para no desvelar por ninguna vía datos personales, desconociendo en este momento si existió con posterioridad correos similares sin

copia oculta de los destinatarios, ni desde luego ha llegado a nuestro conocimiento denuncia derivada de hechos similares.

5- Medidas técnicas y organizativas adoptadas para evitar, en lo posible, incidentes de seguridad coma el sucedido.

Los hechos que la AEPD dice haberse producido, no pueden extrapolarse a una situación al margen de la grave crisis producida en todos los hospitales del país que supuso su colapso y casi imposibilidad de prestar la asistencia sanitaria. Por tanto y al margen de la información transmitida desde nuestras estructuras centrales, los hechos que se dicen ocurridos no pueden volver a producirse pues se produjeron como ya se ha indicado íntimamente vinculados y derivados a la pandemia y al colapso hospitalario.

6.- Plan de formación del personal sanitario en materia de protección de datos y descripción del procedimiento establecido para la remisión de este tipo de comunicaciones. Copia de las instrucciones dirigidas al personal encargado de su envió.

En el ámbito del SESCAM existe un comité de seguridad de la información que marca directrices y medidas a adoptar, comunicadas a través de reuniones periódicas celebradas con todas las Gerencias.

*En esta línea, en la Gerencia de Atención Integrada de ***LOCALIDAD.1 se ha elaborado un curso propio en modalidad on line sobre seguridad en la información ("Seguridad en la Información. Accesos indebidos"), cuyo plazo de presentación de instancias ya se ha iniciado estando previsto el inicio del curso en los primeros días del mes de junio de 2022 y deberá ser cursado de forma obligatoria como jornada de trabajo por los más de 5.000 empleados que en este momento dependen de esta Gerencia.*

Con carácter previo, desde hace algunos años desde nuestros Servicios Centrales se organiza un curso denominado "LA PROTECCION DE LOS DATOS PERSONALES EN EL SESCAM", de 25 horas de duración, con más de seis ediciones y de acceso para todo el personal del SESCAM."

En relación con la contestación de la reclamada evacuada en el seno de las presentes actuaciones de investigación y que ha sido parcialmente transcrita en los párrafos precedentes, es preciso destacar que:

En la información facilitada no se han incorporado los documentos anexos al escrito procedente de la Gerencia de Atención Integrada de ***LOCALIDAD.1, con el que supuestamente se contesta al traslado de la reclamación.

La reclamada insiste en el desconocimiento tanto del correo electrónico enviado, y que motiva la reclamación que ahora se investiga, como del anexo adjunto al mismo en el que se contienen datos de varios trabajadores del servicio: nombre, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral.

Del correo analizado se ha constatado la siguiente información:

La dirección desde la que se envió es ***EMAIL.1**.

El correo tenía como destinatario a ***EMAIL.2**

Los destinatarios en copia del correo fueron:

***EMAIL.3**
***EMAIL.4**
***EMAIL.5**
***EMAIL.6**
***EMAIL.7**
***EMAIL.8**

Ninguna de las direcciones destinatarias del correo electrónico son correos corporativos de la reclamada. Solamente la dirección desde la que se envió el correo es corporativa.

La tabla Anexa al correo contiene los datos de 40 personas relativos a: Empleado (con nombre); PCR test serológico; Síntomas; Baja laboral; Categoría.

Los datos contenidos en la tabla afectan a personal de distintas categorías: Recepcionista, Administrativos, Caladores, Auxiliares DUE, DUE, TERT, Radiofísicos y Médicos.

De las actuaciones anteriormente descritas se desprenden dos aspectos relevantes:

1.- Ha quedado acreditado que en fecha 3 de junio de 2020 a las 16:20 horas, el Servicio de Oncología Radioterápica del centro hospitalario ***HOSPITAL.1** envió por e-mail a varios trabajadores del servicio una tabla con su información personal (nombre, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral).

La dirección desde la que se envió es ***EMAIL.1**.

El correo tenía como destinatario a ***EMAIL.2**

Los destinatarios en copia del correo fueron:

***EMAIL.3**
***EMAIL.4**
***EMAIL.5**
***EMAIL.6**
***EMAIL.7**
***EMAIL.8**

Ninguna de las direcciones destinatarias del correo electrónico son correos corporativos de la reclamada. Solamente la dirección desde la que se envió el correo es corporativa.

La tabla Anexa al correo contiene los datos de 40 personas relativos a: Empleado (con nombre); PCR test serológico; Síntomas; Baja laboral; Categoría.

2.- Respecto a la brecha de confidencialidad se constata que no ha sido notificada a la Agencia Española de Protección de Datos. No se dispone de evidencias suficientes sobre el resto de información referente a la brecha y en concreto el destino que se ha dado a los datos contenidos en la tabla y si éstos has sido suprimidos o no.

QUINTO: Con fecha 2 de junio de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD, artículo 9 del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD.

SEXTO: Con fecha 24 de junio de 2022, la entidad reclamada en respuesta al acuerdo de inicio de este procedimiento sancionador, reitera las manifestaciones realizadas el 30 de mayo de 2022, señaladas en el antecedente cuarto, con motivo del requerimiento de información realizado en fase de actuaciones previas al inicio de este procedimiento, estableciendo las siguientes matizaciones sobre las presuntas sanciones que se le imputan:

En relación con la presunta sanción del artículo 5.1 f) del RGPD, la entidad reclamada considera que la incorporación de los datos, tenía por finalidad garantizar la seguridad de los pacientes y la del resto de empleados del servicio de oncología y radioterápica.

Respecto de la presunta sanción del artículo 9 del RGPD, la entidad reclamada considera que la información desvelada no indica ningún dato de salud, sólo si los trabajadores como consecuencia de haber padecido la enfermedad COVID, habían generado o no anticuerpos.

En lo relativo a la presunta sanción del artículo 32 del RGPD, la entidad reclamada manifiesta que no ha declarado la brecha de seguridad pues no se tuvo conocimiento de ella hasta que ha tenido conocimiento de la presente denuncia.

SEPTIMO: Con fecha 8 de julio de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento al ***SERVICIO DE SALUD DE CASTILLA LA MANCHA***, con NIF ***Q4500146H***, por una infracción del artículo 5.1.f) del RGPD, una segunda infracción del artículo 9 del RGPD tipificadas ambas en el artículo 83.5 del RGPD y una tercera infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

OCTAVO: Con fecha 27 de julio de 2022 se presentan alegaciones a la propuesta de resolución, en el mismo sentido que en las alegaciones al acuerdo de inicio, afirmando concretamente que los hechos imputados se ven fundamentados en lo siguiente:

".-Que existía obligación legal de actuar en la forma que se hizo, por razones de seguridad y salud de pacientes y trabajadores del Servicio de Radioterapia.

- Que la información fue dada al grupo reducido de médicos del Servicio y Supervisora de enfermería que tienen la responsabilidad de cumplir tales cometidos.

- Que el documento en cuestión se usó para una sola finalidad y que fue destruido después sin quedar incorporado a una base de dalos con vocación de permanencia.

- Que el documento quedó bajo la custodia de la Junta de Personal sin que a esta Gerencia se le diera traslado del mismo, no pudiendo por ello adoptar ninguna medida ni comunicar la supuesta brecha de seguridad. de existir.

- Que no existió brecha de seguridad."

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: El 3 de junio de 2020, se remite correo electrónico por la entidad reclamada a varios trabajadores en los cuales aparecía información personal (nombre, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral)

SEGUNDO: El 24 de junio de 2020, la entidad reclamada presenta alegaciones manifestando que su actuación se justifica por razones de seguridad, que los datos eran relativos a si los pacientes habían generado anticuerpos por haber padecido COVID, y que no se declaró la brecha de seguridad por no tener conocimiento de la misma.

FUNDAMENTOS DE DERECHO

I

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

II

Los principios relativos al tratamiento de datos de carácter personal, se regulan en el artículo 5 del RGPD donde se establece que *"los datos personales serán:*

"a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en

interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

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

La infracción del art. 5.1.f) se tipifica en el artículo 83.5 del RGPD que dispone:

“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; (…)”

El artículo 72.1 a) de la LOPDGDD señala que “*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”.

III

Hemos de tener en cuenta además que el artículo 9 del RGPD establece lo siguiente:

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o

tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

La infracción del artículo 9 del RGPD, está prevista en el artículo 83.5 del RGPD donde se establece que:

"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."

A su vez, la LOPDGDD en su artículo 72.1.e) califica de infracción muy grave, a efectos de prescripción, "*El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE)2016/679 sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo de esta Ley Orgánica."*

IV

La seguridad en el tratamiento de datos personales viene regulada en el artículo 32 del RGPD donde se establece 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."*

La infracción del artículo 32 del RGPD se tipifica 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."

El artículo 73.f) de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves dispone:

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

V

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".

VI

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

b) dirigir a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

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;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

VII

Se presenta reclamación por la remisión de correo electrónico por la entidad reclamada a varios trabajadores en los cuales aparecía información personal (nombre, categoría profesional, resultados de las pruebas de COVID-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral)

En escrito de alegaciones tanto en el acuerdo de inicio como de propuesta de resolución, la entidad reclamada justifica los hechos imputados alegando razones de seguridad pública, y que la información remitida versaba únicamente sobre si unos trabajadores habían generado o no anticuerpos tras haber padecido COVID-19, así como la imposibilidad de comunicar la brecha de seguridad por desconocimiento.

En concreto justifica su actuación alegándose lo siguiente:

".-Que existía obligación legal de actuar en la forma que se hizo, por razones de seguridad y salud de pacientes y trabajadores del Servicio de Radioterapia.

- Que la información fue dada al grupo reducido de médicos del Servicio y Supervisora de enfermería que tienen la responsabilidad de cumplir tales cometidos.

- Que el documento en cuestión se usó para una sola finalidad y que fue destruido después sin quedar incorporado a una base de dalos con vocación de permanencia.

- Que el documento quedó bajo la custodia de la Junta de Personal sin que a esta Gerencia se le diera traslado del mismo, no pudiendo por ello adoptar ninguna medida ni comunicar la supuesta brecha de seguridad de existir.

- Que no existió brecha de seguridad."

De conformidad con las evidencias de las que se dispone, se constata que el email objeto de conflicto contenía una tabla con su información personal (nombre, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad, y si esto había conllevado una baja laboral), lo cual contraviene el artículo 9 del RGPD, ya que la entidad reclamada ha procedido al tratamiento de datos de salud del reclamante, sin encontrarse en alguno de los supuestos indicados en el artículo 9.2 del RGPD, tal y como se ha indicado en el fundamento de derecho III.

Se considera, asimismo, la comisión de la infracción del artículo 5.1 f) del RGPD, que rige el principio de integridad y confidencialidad, para que los datos sean 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.

Respecto a la brecha de confidencialidad producida, se constata que no ha sido notificada a la Agencia Española de Protección de Datos.

No se dispone de evidencias suficientes sobre el resto de información referente a la brecha y en concreto el destino que se ha dado a los datos contenidos en la tabla y si éstos han sido suprimidos o no.

Esta Agencia considera que las medidas de seguridad de la entidad reclamada no eran adecuadas en el momento de producirse el incidente objeto de reclamación y deben ser mejoradas porque queda constatado que no han sido suficientes para evitar los hechos denunciados.

Así las cosas, esta Agencia considera que la entidad reclamada, ha infringido los artículos 9, 5.1 f) y 32 del RGPD, al tratar datos de salud, especialmente protegidos, en segundo lugar por violar el principio de integridad y confidencialidad, y finalmente por no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de su personal.

VIII

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: IMPONER al ***SERVICIO DE SALUD DE CASTILLA LA MANCHA***, con NIF ***Q4500146H***, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: IMPONER al ***SERVICIO DE SALUD DE CASTILLA LA MANCHA***, con NIF ***Q4500146H***, por una infracción del artículo 9 del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

TERCERO: IMPONER al ***SERVICIO DE SALUD DE CASTILLA LA MANCHA***, con NIF ***Q4500146H***, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de apercibimiento.

CUARTO: QUE el ***SERVICIO DE SALUD DE CASTILLA LA MANCHA*** adopte las medidas necesarias para un debido tratamiento de los datos de salud, así como medidas que garanticen la integridad, confidencialidad y seguridad de los datos personales tratados, así como la aportación de medios de prueba acreditativos del cumplimiento de lo requerido en el plazo de un mes desde la notificación de la presente resolución.

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

SEXTO: NOTIFICAR la presente resolución al ***SERVICIO DE SALUD DE CASTILLA LA MANCHA***.

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