Ref. Consulta DPD 3-2021

INFORME DEL DELEGADO DE PROTECCIÓN DE DATOS-INSPECCIÓN GENERAL DE SERVICIOS SOBRE LA CONSULTA REALIZADA POR LA CONSEJERÍA DE SALUD RELATIVA AL TRATAMIENTO Y CESIÓN DE DATOS PERSONALES RELATIVOS AL PROCESO DE VACUNACIÓN.

ANTECEDENTES

Con fecha 29 de enero de 2021 se ha recibido por comunicación interior escrito de consulta remitida por la Secretaría General de la Consejería de Salud en la que solicita informe a este Delegado de Protección de Datos sobre el tratamiento y cesión de datos personales relativos al proceso de vacunación en la Región de Murcia.

La consulta, en síntesis, plantea que *en lo referente a la vacunación del personal de los órganos centrales del Servicio Murciano de Salud (SMS) y de la Consejería de Salud, se considera necesario, en aras a la transparencia de las actuaciones practicadas, dar publicidad general a los listados de las personas que han sido vacunadas en el conjunto de la Región de Murcia, por lo que solicita conocer su viabilidad jurídica y, en su caso, con qué criterios y pautas se debería llevar a cabo la difusión de la información sin vulnerar la normativa reguladora en materia de protección de datos, así como, de modo específico, para los datos vinculados a la historia clínica en la Ley 14/1986, de 25 de abril, General de Sanidad y 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.*

Este Delegado de Protección de Datos en ejercicio de las funciones atribuidas por el artículo 39.1 del *Reglamento (UE) 2016/679 de 27 de abril de 2016 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* (en adelante RGPD), de asesoramiento al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de aquellas obligaciones que les incumben en virtud de la normativa de protección de datos, emite el siguiente informe en respuesta a la consulta formulada.

CONSIDERACIONES

I

La consulta plantea, en aras de la transparencia, dar publicidad a los listados de personas que han sido vacunadas, en especial, el personal de los órganos centrales del SMS y de la Consejería de Salud.

Dicha actividad consistente en la cesión, difusión o comunicación de datos de una persona implica un tratamiento de datos personales, y por tanto está sujeta a la normativa sobre protección de datos y a sus principios, esto es, al RGPD y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD).

El artículo 4.1) del RGPD recoge la **definición de datos personales**, estableciendo que se entenderá por tales:

"«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"

Respecto a las comunicaciones o cesiones de datos personales, el RGPD permite las cesiones de datos personales a terceros. Ahora bien, la cesión de datos personales debe realizarse cumpliendo con los principios y las condiciones legales establecidas en el RGPD, las cuales serán objeto de análisis posteriormente.

Conviene señalar, que, según el RGDP, **la comunicación o cesión de datos consiste en una actividad de "tratamiento" de datos,** pues el artículo 4.2) del RGPD define "tratamiento" como cualquier operación sobre datos personales como la recogida, registro, comunicación, difusión o cualquier otra forma de acceso.

"«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;"

A este respecto, el tratamiento (o la cesión) de datos para ser legítimo, únicamente puede realizarse si está fundamentado en alguno de los supuestos o condiciones previstas en el artículo 6.1 del RGPD, que establece las causas de licitud del tratamiento.

Ahora bien, para el tratamiento (o la cesión) de datos de salud, objeto de análisis en el presente informe, debemos acudir al **artículo 9 del RGPD que regula el tratamiento de las "categorías especiales de datos personales", gozando de esta naturaleza, entre otros, los datos de salud.**

"Artículo 9.Tratamiento de categorías especiales de datos personales

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 orientación sexuales de una persona física."*

Respecto a los datos de salud, están definidos en el artículo 4.15) del RGPD:

*"«**datos relativos a la salud**»: datos personales **r**elativos a la salud física o mental de una persona física,* ***incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud****;"*

El **Considerando 35 del RGPD** precisa más la cuestión sobre **dato relativo a la salud,** al considerar que *«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».*

En este sentido, mencionamos también la definición dada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal[1], que en su artículo 5.1 g) establece:

"Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. "

En este **concepto amplio de datos relativos a la salud** consideramos que están incluidos los datos de vacunación de una persona.

Dado que los datos de vacunación son datos relativos a la salud de una persona, y tienen la condición de "categoría especial de datos personales", debe aplicarse para su tratamiento o cesión el régimen establecido en el artículo 9 del RGPD, que examinamos a continuación.

II

Ya hemos mencionado anteriormente respecto a la legitimación para el tratamiento de datos que las condiciones para su licitud están establecidas en el artículo 6.1 del RGPD. Entre las bases jurídicas que legitiman el tratamiento de datos personales establecidas en el artículo 6.1 del RGPD, destacamos las siguientes:

"a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;"

Sin embargo, en el presente caso, no es suficiente con que exista un supuesto habilitante del artículo 6.1 RGPD, sino que debido a la naturaleza de los datos personales objeto de cesión o tratamiento, es decir, por tratarse de datos de

[1] Dicho Real Decreto 1720/2007, según lo establecido en la Disposición derogatoria única de la LOPD 3/2018, se considera vigente en lo que no contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD y en la LOPD 3/2018.

salud los cuales tienen la condición de "categoría especial de datos personales", debe aplicarse el régimen establecido en el artículo 9 del RGPD.

El artículo 9 del RGPD establece lo siguiente:

"Artículo 9. Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos (…) relativos a la salud de una persona física.

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

El tratamiento de las categorías especiales de datos está prohibido por el artículo 9.1 del RGPD. No obstante, el artículo 9.2 RGPD establece el listado tasado de circunstancias que pueden concurrir para poder llevar a cabo el tratamiento o cesión de las categorías especiales de datos. **Únicamente en el caso de que concurra alguna de las circunstancias previstas en el artículo 9.2 del RGPD, se excepciona la prohibición del tratamiento o cesión de datos de salud.**

Entre las circunstancias del 9.2, las mencionadas en las **letras g) h) e i)** pueden referirse a datos de salud:

"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."

Conviene recordar que cuando el RGPD se refiere a la base del Derecho de la Unión o de los Estados miembros, debemos entender una **norma con rango de ley**.

En este sentido, el artículo 9.2 de la LOPD, referido a las categorías especiales de datos, establece que "*los tratamientos de datos contemplados en las letras g) h) e i) del 9.2 RGPD deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad."*

Además, la Disposición adicional 17 (relativa a los tratamientos de datos de salud) de la LOPD, establece que se encuentran amparados en las letras g) h) e i) del 9.2 RGPD, los tratamientos de datos relacionados con la salud que estén regulados en las leyes citadas en dicha **Disposición adicional 17**. **Listado de leyes y sus disposiciones de desarrollo todas pertenecientes a la legislación sectorial de ámbito sanitario**.

"*Disposición adicional decimoséptima. Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) 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.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre."

A este respecto, en concreto, **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**, **reconoce en su artículo 7 el derecho a la intimidad y en el artículo 16 regula los usos de la historia clínica**, en los siguientes términos:

"Artículo 7. El derecho a la intimidad.

1. ***Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley****.*

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes."

El artículo 16 regula los usos de la historia clínica, estableciendo en el apartado 3 el acceso a la historia clínica[2], en los siguientes términos:

"Artículo 16. 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

[2] La redacción vigente del artículo 16.3 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, procede de la modificación efectuada por la Disposición final novena de la Ley Orgánica 3/2018, de Protección de Datos y garantías de derechos digitales.

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.

3. ***El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos****.*

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los ***supuestos de investigación de la autoridad judicial*** *en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.*

Cuando ello sea necesario para la ***prevención de un riesgo o peligro grave para la salud de la población****, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso,* ***por un profesional sanitario sujeto al secreto profesional*** *o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.*

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

*6. El **personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto**.*

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso."

De lo expuesto en la consulta se deduce que **si los datos de vacunación forman parte de la historia clínica**, hay que tener en cuenta que **entre las finalidades señaladas en el apartado 3 que permiten el acceso a la historia clínica no se incluye la difusión de la misma a la ciudadanía en aras de la transparencia**.

Por tanto, según lo establecido en el RGPD únicamente si concurriese alguna de las circunstancias señaladas en las letras g) h) e i), sobre la base de una norma con norma con rango de ley, y en los términos señalados por la legislación sectorial de ámbito sanitario, el responsable del tratamiento[3] podría realizar el tratamiento o la cesión de datos personales de salud. De lo manifestado en la consulta no parece deducirse que el hecho de dar publicidad a la ciudadanía en aras de la transparencia, esté comprendido en alguna de estas circunstancias.

Ahora bien, a las anteriores circunstancias **añadimos las señaladas en las letras a) y e) del 9.2 RGPD, referidas respectivamente, al consentimiento del interesado y a que el interesado hubiera hecho manifiestamente públicos los datos.**

"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;

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

[3] Responsable del tratamiento entendiendo como tal el órgano de la Consejería de Salud que tenga atribuidas las competencias o funciones para determinar los fines y medios del tratamiento de los datos de vacunación. Según artículo 4.7) del RGPD "*«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".*

Por lo que **si se prestara el consentimiento explícito del afectado, o bien, si éste hubiera hecho manifiestamente públicos sus datos de salud, el responsable del tratamiento estaría legitimado para el tratamiento (o cesión) de dichos datos de salud**.

Respecto a cómo debería manifestarse el consentimiento, recordamos lo dispuesto en el artículo 4.11) del RGPD (definición de consentimiento), y en el artículo 7 del RGPD relativo a las condiciones del consentimiento.

"4.11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;"

"Artículo 7. Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo."

En términos similares se pronuncia la LOPD en su artículo 6 respecto al consentimiento:

"Artículo 6. Tratamiento basado en el consentimiento del afectado.

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas."

III

Por otro lado, dado que la consulta plantea dar publicidad a los datos en aras de la transparencia, consideramos que debe hacerse una referencia al **marco normativo relativo a la transparencia de la información pública**, esto es, la Ley 19/2013, de 9 de diciembre, de trasparencia, acceso a la información pública y buen gobierno; y la Ley 12/2014, de 16 de diciembre, de Transparencia y Participación Ciudadana de la Comunidad Autónoma de la Región de Murcia.

Efectivamente la información relativa a listados de personas que han recibido una vacuna **no se especifica expresamente como uno de los extremos objeto de publicidad activa** recogidos en la Ley 19/2013 o en la Ley 12/2014, no obstante esta última, prevé en el artículo 20 que "*con independencia de las obligaciones de publicidad activa señaladas en los artículos anteriores, se fomentará la publicación de cualquier otra información pública que se considere de interés para la ciudadanía".* Por tanto, si la Administración Regional considera, tal como dice en la consulta, que son datos a los que debe darse publicidad en aras de la transparencia, estimamos conveniente mencionar aquí los límites a la publicidad contenidos en la legislación sobre transparencia.

Así, ante la posible colisión entre la publicidad de la información pública y la protección de datos personales, debemos tener en cuenta lo dispuesto en el artículo 5.3 y en el artículo 15 de la Ley 19/2013, diferenciando los supuestos de categorías especiales de datos, de aquellos que no tienen dicho carácter.

El artículo 5.3 establece:

*"3. Serán de aplicación, en su caso, los **límites al derecho de acceso a la información pública** previstos en el artículo 14 y, especialmente, el derivado de la **protección de datos de carácter personal**, regulado en el artículo 15. A este respecto, **cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación** de los mismos."*

Y el artículo 15. 1 establece para los datos de salud que el acceso solo se podrá autorizar en el caso de que el afectado manifieste su consentimiento expreso, o si el acceso estuviera amparado por una norma con rango de ley.

"Artículo 15. Protección de datos personales.

1. *(…) Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley."*

Según dicho precepto, **para la cesión de datos de salud es necesario contar con el consentimiento expreso del afectado, o bien, que exista una norma con rango de ley que lo ampare**.

Por otro lado, añade el artículo 15 en su apartado 4, que **no es aplicable** el límite establecido en el apartado anterior **si el acceso a los datos se efectúa previa disociación de los datos de carácter personal de manera que se impida identificar a las personas**. Por lo que **cabe la posibilidad de proporcionar la información de forma disociada, desvinculada de datos identificativos**.

"15.4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas."

IV

En otro orden de cosas, y a pesar de que no se especifica en la consulta, en aras de dar una visión completa, añadimos aquí un comentario respecto al supuesto de que se solicitara información a la Administración Regional en el marco de la acción de control al Ejecutivo por el Legislativo. Advirtiendo que, en este ámbito, este Delegado de Protección de Datos se limita únicamente a exponer el marco jurídico que permita compatibilizar el derecho de los diputados a obtener información de la Administración necesaria para el ejercicio de su función de control, con el respeto al derecho fundamental a la protección de datos, sin que pueda interferir este Delegado en las funciones propias de la Cámara Legislativa.

De modo que si se **solicitara información en el marco de las relaciones del Legislativo-Ejecutivo**, y en concreto, por los diputados en el ejercicio de las funciones de control parlamentario, el marco normativo vendría establecido por el **Reglamento de la Asamblea Regional de Murcia**, en concreto el artículo 13, que señala lo siguiente:

"*Artículo 13. Derecho a solicitar información.*

1. *Para el mejor cumplimiento de sus funciones parlamentarias, las diputadas y diputados, por conducto de la Presidencia de la Asamblea, tendrán derecho a recabar de la Administración de la Comunidad Autónoma los datos, informes o documentos, consecuencia de actuaciones realizadas por dicha Administración y todos sus organismos dependientes, que obren en su poder, siempre que su conocimiento no conculque las garantías legalmente establecidas para la protección de datos de carácter personal.*

   En caso de no indicar el tipo de soporte de los datos, se entenderá que es en soporte informático.

   En el supuesto de que los datos, informes o documentos solicitados afecten al contenido esencial de los derechos fundamentales o libertades públicas constitucionalmente reconocidos, la Administración comunicará a la Mesa el carácter reservado de estos. En tal caso, la Mesa podrá declarar el carácter no público de las actuaciones, disponiendo el acceso directo a los documentos y pudiendo la diputada o el diputado tomar notas, pero no obtener copia ni actuar acompañado de ningún asesor, ni divulgar la información.

   El incumplimiento del deber de reserva establecido en este punto podrá dar lugar a la aplicación de las normas de disciplina parlamentaria establecidas en la sección primera del capítulo VI del título VI de este Reglamento.

   La normativa de protección de datos de carácter personal será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de información de los diputados y diputadas."

Según lo dispuesto en el artículo 13.1 del Reglamento de la Asamblea, los diputados, por conducto de la Presidencia de la Asamblea, tienen derecho a recabar datos procedentes de la Administración, siempre que "*su conocimiento*

no conculque las garantías legalmente establecidas para la protección de datos de carácter personal."

Añade a lo anterior "*en el supuesto de que los* ***datos afecten al contenido esencial de los derechos fundamentales o libertades públicas constitucionalmente reconocidos****",* la aplicación de un límite al derecho de información de los diputados que tiende a que en caso de colisión con un derecho fundamental, se produzca un **acceso limitado** a la información consistente en **tomar notas, sin posibilidad de obtener materialmente la documentación**.

V

Por otra parte, abundando en el tema anteriormente citado sobre aportar la **información de forma disociada**, desvinculada de datos identificativos, procedemos analizar esta opción con más profundidad. Así, para mitigar los eventuales daños que pudieren producirse a los interesados, podría anonimizarse la información o, tal como menciona el RGPD, podría procederse a la seudonimización de datos. Así el considerando 28 del RGPD establece que:

"(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos."

Antes, debemos diferenciar técnicamente entre **datos anonimizados y datos seudonimizados,** ya que los efectos jurídicos de uno y otro son diferentes.

- La **anonimización** es el resultado de un tratamiento de datos personales realizado para evitar de forma irreversible su identificación a todos los actores (incluido el responsable del tratamiento). A los datos anónimos no le es de aplicación la normativa de protección de datos. La anonimización consiste en un tratamiento de los datos de tal manera que no puedan usarse para identificar a una persona física mediante el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por terceros. De ahí que los procesos de anonimización deban garantizar que

tampoco el responsable del tratamiento pueda reidentificar a los individuos de un fichero anonimizado.

- La **seudonimización**, definida en el artículo 4.5) del RGPD, consiste en "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".* Correspondiendo al responsable del tratamiento determinar quién tiene acceso a la información adicional. Dado su carácter reversible le resulta de aplicación la normativa de protección de datos.

De la consulta no se deduce que el objeto de la anonimización afecte al responsable, ya que no nos encontramos con una información que ha sido previamente facilitada al responsable del tratamiento de manera anonimizada, sino que parece limitarse al sistema de difusión o cesión de la información a terceros, pues se trata de una información disponible en sus bases de datos de manera completa, ya que el responsable tendrá acceso a los datos personales de vacunación asociados a la persona física identificada, siendo de aplicación el RGPD y la seudonimización a la que se refiere en el artículo 4.5) del RGPD.

En este sentido el *Grupo de trabajo sobre protección de datos del artículo 29 en su Dictamen*[4] *05/2014, sobre técnicas de anonimización de 10 de abril de 2014*, analiza la anonimización y la seudonimización, así como las técnicas de ambas.

Respecto a la **seudonimización**, el Dictamen 05/2014 refiere que *"la seudonimización consiste en la sustitución de un atributo por otro en un registro. (…) La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado, se trata de una medida de seguridad útil, pero no es un método de anonimización."*

En este sentido, el Dictamen 05/2014 recomienda el uso de las técnicas de seudonimización[5], entre ellas, las más utilizadas son: cifrado con clave secreta;

[4] Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014 por el Grupo de trabajo sobre protección de datos del artículo 29. Accesible en: https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

[5] Técnicas de seudonimización:

• Cifrado con clave secreta: En esta técnica, el poseedor de la clave puede reidentificar al interesado con suma facilidad. Para ello, le basta con descifrar el conjunto de datos, ya que este

función hash; función con clave almacenada; cifrado determinista o función hash con clave con borrado de clave; y descomposición en tokens.

---

contiene los datos personales, aunque sea en forma cifrada. Si se aplican los sistemas de cifrado más avanzados, tan solo es posible descifrar los datos si se conoce la clave.

• Función hash: Se trata de una función que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño (esta entrada puede estar formada por un solo atributo o por un conjunto de atributos). Esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Sin embargo, si se conoce el rango de los valores de entrada de la función hash, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado. Por ejemplo, si se aplica la función hash al número de identificación nacional para seudonimizar un conjunto de datos, dicho atributo se puede obtener simplemente ejecutando la función con todos los posibles valores de entrada y comparando los resultados con los valores del conjunto de datos. Habitualmente, las funciones hash se diseñan para poder ejecutarse de manera relativamente rápida, por lo que están sujetas a ataques de fuerza bruta[16]. También se pueden crear tablas precalculadas para lograr una reversión masiva de un gran número de valores hash. El uso de una función hash «con sal» (en la que se añade un valor aleatorio, conocido como «sal», al atributo al que se aplica la función hash) puede reducir la probabilidad de obtener el valor de entrada. No obstante, usando medios razonables, todavía existe la posibilidad de calcular el valor original del atributo que se oculta tras el resultado de e oculta tras el resultado de una función hash con sal[17].

• Función con clave almacenada: Se trata de un tipo de función hash que hace uso de una clave secreta a modo de valor de entrada suplementario (lo cual la diferencia de una función hash con sal, ya que, normalmente, la sal no es secreta.) El responsable del tratamiento puede reproducir la ejecución de la función con el atributo y la clave secreta. Sin embargo, los atacantes, que no conocen la clave, lo tendrían mucho más difícil: el número de combinaciones que habría que probar sería tan grande, que convertiría este procedimiento en impracticable.

• Cifrado determinista o función hash con clave con borrado de clave: Esta técnica equivale a generar un número aleatorio a modo de seudónimo para cada atributo de la base de datos y, posteriormente, borrar la tabla de correspondencia. Esta solución18 reduce el riesgo de vinculabilidad entre los datos personales contenidos en el conjunto de datos y los datos personales relativos a la misma persona contenidos en otro conjunto de datos en el que se usa un seudónimo diferente. Si se ejecutan los algoritmos más avanzados, el esfuerzo de cálculo que debería realizar un atacante para descifrar o reproducir la ejecución de la función sería muy grande, ya que tendría que probar cada posible clave, puesto que esta se desconoce. • Descomposición en tokens: Esta técnica se usa típicamente en el sector financiero (aunque no exclusivamente en él) para reemplazar los números de identificación de tarjetas por valores que son de poca utilidad para los atacantes. Tiene su origen en las técnicas anteriormente mencionadas, y suele basarse en la aplicación de mecanismos de cifrado unidireccionales, o bien en la asignación, mediante una función de índice, de un número de secuencia o un número generado aleatoriamente que no derive matemáticamente de los datos originales.

[16] Estos ataques consisten en probar todas las posibles entradas para crear tablas de correspondencia.

[17] Especialmente si se conoce el tipo de atributo (nombre, número de seguridad social, fecha de nacimiento, etc.). Para añadir dificultad computacional, se podría recurrir a una función hash de derivación de clave, en la que al valor computado se le aplica varias veces la función hash con poca sal.

Tal como menciona el Dictamen 05/2014, la seudonimización ofrece una serie de garantías, entre ellas, la "*singularización: es posible singularizar registros de las personas, ya que la persona queda identificada por un atributo único, que es el resultado de la función de seudonimización".* Es decir, con la seudonimización es posible singularizar la información ya que detrás de un atributo seudonimizado sabemos que habría una persona identificada.

En resumen, de la normativa analizada podemos deducir que salvo que el interesado haya dado su consentimiento explícito al responsable del tratamiento para publicar sus datos de salud, o si el interesado los hubiera hecho manifiestamente públicos con anterioridad, conforme establece el artículo 9.2 letras a) y e) del RGPD, y entendiendo que el responsable del tratamiento tampoco apreciara que concurre alguna otra de las circunstancias previstas en las letras g) h) e i) del artículo 9.2 RGPD para la cesión de los datos de salud, se recomienda publicar la información seudonimizando los datos personales identificativos contenidos en el listado del personal vacunado, utilizando alguna de las técnicas de seudonimización a las que hace referencia el Dictamen 05/2014. De manera que **con el fin de conciliar la necesidad de mitigar los eventuales daños que pudieren producirse en los interesados como consecuencia de la publicación de sus datos personales y de dotar de transparencia al proceso de vacunación podría ponderarse la realización de una publicación desvinculada de la identidad del interesado o**, como señala el RGPD, **llevar a cabo una seudonimización previa de los datos identificativos de los vacunados**, máxime tratándose de datos de salud.

Por lo que se refiere, en especial, a la vacunación del personal de los órganos centrales del Servicio Murciano de Salud y de la Consejería de Salud objeto de la consulta, **podría estudiarse por el responsable del tratamiento proporcionar datos estadísticos desvinculados de la identidad, que considerase de interés para la ciudadanía y que contribuyan a la transparencia.** Así, sin ánimo de interferir en la decisión por el responsable respecto a qué tipo de información estimase de interés, y, a título de ejemplo, podríamos señalar los siguientes: datos de vacunados por gerencias o áreas de salud; distinguiendo en su caso, entre clases de personal estatutario; entre categorías, cuerpos, y opciones estatutarias; entre personal sanitario y no sanitario vacunado; o incluso la fecha de vacunación; o el rango de edad; etc., así como aquellos otros datos que se considerasen relevantes para el ejercicio de la transparencia. Lo anterior con la cautela de que esa información no permita reidentificar a las personas, de manera que usando los valores de otros atributos por agregación de datos se revele la identidad de personas concretas.

VI

Finalmente, recordamos que en relación con el tratamiento de datos personales debemos tener siempre presente la aplicación de todos los principios contenidos en el artículo 5 del RGPD.

Especial atención dedicamos al **principio de licitud y limitación de la finalidad** (los datos personales recogidos con fines determinados, explícitos y legítimos nos serán tratados ulteriormente con finalidades distintas); y al **principio de minimización de datos** (el dato tiene que ser pertinente, adecuado y limitado a lo estrictamente necesario en relación con el fin para el que es tratado). Así como al **principio de confidencialidad** (protección contra el tratamiento no autorizado o ilícito).

"Artículo 5. Principios relativos al tratamiento

1. 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; («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»);"

VII

A modo de **C O N L U S I Ó N**:

1. Todo tratamiento, cesión, difusión o publicación de información que contenga datos de carácter personal debe respetar la normativa reguladora en materia de protección de datos y sus principios.

2. Respecto al régimen establecido en la normativa sobre protección de datos, el RGPD determina que el tratamiento (o cesión) de datos para ser legítimo únicamente puede realizarse si se fundamenta en alguno de los supuestos

previstos en el artículo 6.1 del RGPD, el cual establece las causas de licitud del tratamiento.

En el presente caso, no es suficiente con que exista un supuesto del artículo 6.1 del RGPD, sino que debido a la naturaleza de los datos personales objeto de tratamiento o cesión, es decir, por tratarse de datos de salud los cuales tienen la condición de "categoría especial de datos personales", debe aplicarse el régimen establecido en el artículo 9 del RGPD.

El tratamiento de las "categorías especiales de datos" está prohibido por el artículo 9.1 del RGPD. No obstante, el artículo 9.2 RGPD establece el listado tasado de circunstancias que pueden concurrir para poder llevar a cabo el tratamiento o cesión de estas categorías especiales de datos.

Únicamente en el caso de que concurra alguna de las circunstancias previstas en el artículo 9.2 del RGPD se excepciona la prohibición del tratamiento o cesión de datos de salud. Para los datos de salud hay que tener en cuenta las circunstancias previstas en las letras g) h) e i), además de las letras a) y e) estas últimas referidas al consentimiento del interesado, y a datos que el interesado haya hecho manifiestamente públicos.

El responsable del tratamiento para llevar a cabo la publicación o cesión de los datos de salud, debe valorar si concurre alguna de las circunstancias previstas en las letras g) h) e i) del artículo 9.2 del RGPD sobre la base de una norma con rango de ley. De lo expuesto en la consulta no parece deducirse que concurra alguna de estas circunstancias.

La legislación sectorial sanitaria, en concreto 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, regula en su artículo 16.3 el acceso a la historia clínica aludiendo a la finalidades que justifican su acceso (*fines judiciales, epidemiológicos, salud pública, investigación, prevención de un riesgo grave para la salud*, etc.) sin que se cite entre ellas la comunicación de datos a la ciudadanía en aras de la transparencia como se alude en la consulta.

En cualquier caso podrían concurrir las circunstancias previstas en las letras a) y e) del 9.2 RGPD para el tratamiento o la cesión, si los interesados dan su consentimiento explícito o si los interesados hacen manifiestamente públicos sus datos de salud.

3. Por otro lado, la legislación en materia de transparencia no desconoce los límites a la publicación de información que contenga datos de carácter personal, sino que establece que en caso de colisión se aplica el limite contenido en el artículo 15 de la Ley 19/2013 de transparencia, el cual establece que para el acceso a datos de salud se requiere consentimiento del afectado o que el acceso al dato esté amparado en una norma con rango de ley.

4. En otro orden de cosas, si se solicitara información por un diputado en ejercicio de la función de control parlamentario se aplicaría el régimen establecido en el Reglamento de la Asamblea. En el artículo 13 establece que se recabará el dato siempre que su conocimiento no conculque las garantías legalmente establecidas para la protección de datos de carácter personal.

   Y en caso de afectar a un derecho fundamental, establece un acceso limitado a tomar notas.

5. En cualquier caso, todo tratamiento de datos habrá de respetar los principios contenidos en el artículo 5 del RGPD, en especial, el principio de licitud y limitación de la finalidad (los datos personales recogidos con fines determinados, explícitos y legítimos nos serán tratados ulteriormente con finalidades distintas); el principio de minimización de datos (el dato tiene que ser limitado a lo estrictamente necesario en relación con el fin para el que es tratado), y el principio de confidencialidad (protección contra el tratamiento no autorizado o ilícito).

6. Finalmente, cabría tomar en consideración la posibilidad de proporcionar información desvinculada de datos identificativos. Con el fin de conciliar la necesidad de mitigar los eventuales daños que pudieran producirse en los interesados como consecuencia de la publicación de sus datos personales, y de dotar de transparencia al proceso de vacunación podría ponderarse la realización de una publicación anonimizada de la información o, como señala el RGPD, aplicar como medida de seguridad y garantía la seudonimización. Esta publicación de datos de vacunados debería realizarse de forma tal que su proporción no permitiese identificar a persona física alguna, máxime tratándose de datos de salud, por lo que se recomienda el uso de las técnicas de seudonimización previstas en el *Dictamen 05/2014 sobre técnicas de anonimización de 10 de abril de 2014*. Así mismo, a título de ejemplo, y por lo que se refiere en especial a la vacunación del personal de los órganos centrales del Servicio Murciano de Salud y de la Consejería de Salud objeto

de la consulta, podría estudiarse por el responsable de tratamiento proporcionar datos estadísticos de vacunados por gerencias o áreas de salud; distinguiendo, en su caso, entre clases de personal estatutario; entre categorías, cuerpos, y opciones estatutarias; entre personal sanitario y no sanitario vacunado, etc., así como aquellos otros datos disociados que se considerasen relevantes para el ejercicio de la transparencia.

EL DELEGADO DE PROTECCIÓN DE DATOS-INSPECCIÓN GENERAL DE SERVICIOS

(En Murcia, documento fechado y firmado electrónicamente al margen)