

0047/2024

El proyecto remitido tiene por objeto la regulación del Sistema de Información de Vacunaciones e Inmunizaciones (SIVAIN) que se integra en el Sistema de Información en Salud Pública, de conformidad con lo establecido en el artículo 40 de la Ley 33/2011, de 4 de octubre, General de salud Pública.

La disposición final tercera del Real Decreto 568/2024, de 18 de junio, por el que se crea la Red Estatal de Vigilancia en Salud Pública, creó el Sistema de Información de Vacunaciones e Inmunizaciones dependiente del Ministerio de Sanidad, con la finalidad de recoger la información de las vacunaciones e inmunizaciones de todas las personas que residen en España, cuyo funcionamiento se desarrolla a través de la norma proyectada que ahora se somete a informe.

De acuerdo con el artículo 2 del proyecto, la finalidad del SIVAIN *es disponer de los datos de las vacunas y otros fármacos específicos, utilizados para la inmunización pasiva preexposición y posexposición frente a las enfermedades inmunoprevenibles administrados en España, así como los no administrados, pero sí registrados en España, para el seguimiento y evaluación de los programas de vacunación e inmunización.*

Y en su artículo 6 dispone que el SIVAIN (...) *incorporará la información mínima contenida en el Anexo I de las vacunas (...)*

En consecuencia, de la aplicación de la norma proyectada se va a someter a tratamiento (artículo 4.2 RGPD), con carácter general, información susceptible de ser calificada como dato de carácter personal (artículo 4.1 RGPD), y en particular, categorías especiales de datos (artículo 9 RGPD), entre los que se encuentran datos relativos a la salud (artículo 4.15 RGPD).

En efecto, el citado precepto define «datos relativos a la salud» como datos personales relativos 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 concepto de “dato relativo a la salud” del art. 4.15) RGPD es un concepto autónomo de derecho europeo que ha de ser objeto de interpretación uniforme en toda la UE.

Tal y como expresa el TJUE (véanse apartados 81 y ss. de la STJUE de 22 de junio de 2021, C-439/19),

81 A este respecto, procede recordar que el tenor de una disposición de Derecho de la Unión que no contenga una remisión expresa al Derecho de los Estados miembros para determinar su sentido y su alcance debe normalmente ser objeto de una interpretación autónoma y uniforme en toda la Unión (sentencias de 19 de septiembre de 2000, Linster, C 287/98, EU:C:2000:468, apartado 43, y de 1 de octubre de 2019, Planet49, C 673/17, EU:C:2019:801, apartado 47).

El RGPD no contiene ninguna remisión al derecho nacional acerca del concepto de “datos relativos a la salud”, por lo que el alcance de este habrá de ser objeto de interpretación uniforme en el seno de la UE. Por ello, la interpretación acerca del concepto y el alcance de “datos relativos a la salud” no puede ser diferente en un Estado miembro que en otro.

De manera algo más extensa, el Considerando (35) establece:

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.

Acoge pues, el RGPD, un concepto amplio de “dato relativo a la salud”, incluyendo el “riesgo” de padecer enfermedades (futuras), y, por lo tanto, aunque no exista tal enfermedad hoy, o ni siquiera llegue a materializarse efectivamente ese “riesgo” (sujeto, como tal riesgo de salud, a una probabilidad) en el futuro.

Sobre la necesidad de interpretar dicho concepto de una manera amplia, véase STJUE de 1 de agosto de 2022, C-184/20, apartados 124 a 128). Así:

125 Además, una interpretación amplia de los conceptos de «categorías especiales de datos personales» y de «datos sensibles» se ve respaldada por el objetivo de la Directiva 95/46 y del RGPD, a que se ha hecho mención en el apartado 61 de la presente sentencia, de asegurar un alto nivel de protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, de su intimidad, en relación con el tratamiento de los datos personales que las afectan (véase, en este sentido, la sentencia de 6 de noviembre de 2003, Lindqvist, C 101/01, EU:C:2003:596, apartado 50).

126 Más aún, la interpretación contraria se opondría a la finalidad del artículo 8, apartado 1, de la Directiva 95/46 y del artículo 9, apartado 1, del RGPD, que consiste en garantizar una mayor protección frente a tales tratamientos, que, en atención a la particular sensibilidad de los datos objeto de ellos, pueden constituir, como se desprende del considerando 33 de la Directiva 95/46 y del considerando 51 del RGPD, una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados por los artículos 7 y 8 de la Carta [véase, en este sentido, la sentencia de 24 de septiembre de 2019, GC y otros (Retirada de enlaces a datos sensibles), C 136/17, EU:C:2019:773, apartado 44].

Por consiguiente, resultarán de aplicación a las previsiones del Reglamento (UE) 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, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

I

En primer lugar, debe partirse de la naturaleza reglamentaria del proyecto informado y de la vigencia, en relación con las limitaciones al derecho fundamental de protección de datos personales, del principio de reserva de ley exigido por el artículo 53.1 de la Constitución y el artículo 8 de la LOPDGDD, que, conforme a reiterada jurisprudencia del Tribunal Constitucional, requiere, por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal “*ha de reunir todas aquellas características*

indispensables como garantía de la seguridad jurídica”, esto es, “ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención” (STC 49/1999, FJ 4). En otras palabras, “no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites” (STC 292/2000, FJ 15). Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

En este sentido, la importante sentencia 292/2000 de 30 de noviembre señala, en su Fundamento Jurídico 14, y se pronuncia respecto del alcance de las normas reglamentarias en los siguientes términos:

14. Pese a la importancia que para garantizar el ejercicio del derecho fundamental poseen los derechos del interesado a ser informado y a consentir la cesión de sus datos personales, como antes se ha declarado, sin embargo, es suficiente según el art. 21.1 LOPD [norma cuya constitucionalidad se estaba discutiendo en el proceso ante el TC] que la comunicación de tales datos entre Administraciones Públicas, para el ejercicio de competencias diferentes o que versen sobre materias distintas, sea autorizada por una norma reglamentaria. Al respecto, ya hemos dicho [STC 127/1994, FJ 5, con remisión a la STC 83/1984, FJ 4, y 99/1987, FJ 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar

ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino "deferir a la normación del Gobierno el objeto mismo reservado" (STC 227/1993, de 9 de julio, FJ 4, recogiendo la expresión de la STC 77/1985, de 27 de junio, FJ 14).

La remisión a la regulación reglamentaria de materia ligada a la reservada a la Ley es preciso, pues, que se formule en condiciones tales que no contraría materialmente la finalidad de la reserva, de la cual se derivan, según la STC 83/1984, "ciertas exigencias en cuanto al alcance de las remisiones o habilitaciones legales a la potestad reglamentaria, que pueden resumirse en el criterio de que las mismas sean tales que restrinjan efectivamente el ejercicio de esa potestad a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley". Es en este segundo plano en el que se encuentra el núcleo argumental del recurso interpuesto por el Defensor del Pueblo que es acogido en esta Sentencia, el cual considera que al establecer el art. 21.4 LOPD que esas cesiones no requieren del previo consentimiento del afectado permite al reglamento imponer un límite al derecho fundamental a la protección de datos personales, que como se ha dicho ya, defrauda la previsión del art. 53.1 de la Constitución (STC 101/1991, de 13 de mayo, FJ 3).

El artículo 6.1 del RGPD considera que un tratamiento es lícito cuando cumpla al menos una serie de supuestos, entre los que cabe aquí destacar los siguientes:

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”.

La norma proyectada hace referencia, precisamente, a estos supuestos como base jurídica de legitimación en la disposición adicional primera del reglamento sometido a informe, denominada “Tratamientos de datos de carácter personal”.

Asimismo, el apartado 3 del citado artículo 6 RGPD, ahonda en los requisitos legales de la norma que dé cobertura al tratamiento y propone elementos que pondrán ser tenidos en cuenta en dicha regulación, al indicar que:

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

El Considerando 45 del RGPD señala que *“Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.”*

Por su parte la LOPDGDD establece en su artículo 8, bajo la denominación “Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos”, lo siguiente:

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

A estos requisitos, referidos en general a cualesquiera tratamientos de datos personales (sean o no estos datos pertenecientes a categorías especiales) debemos añadir los exigidos para poder someter a tratamiento datos personales incluidos en dichas categorías especiales.

Es decir, respecto de estas categorías especiales de datos personales, el art. 9.1 RGPD, y el art. 9.1 LOPDGDD prohíben su tratamiento. Se prevén sin embargo determinados requisitos que permiten levantar dicha prohibición de tratamiento a la que hace referencia el apartado 1 del citado artículo 9 del RGPD, para lo que debemos aplicar alguna de las excepciones que se recogen en el apartado 2 del citado precepto. Debiendo destacarse aquí los apartados h) e i):

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.

Como puede observarse, en ambos apartados exigen el establecimiento de garantías y medidas específicas y adecuadas por el Derecho de la Unión o de los Estados miembros, es decir, vuelve a poner de manifiesto la necesidad de que dichos supuestos estén basados en la ley, a lo que hay que añadir la doctrina de nuestro Tribunal Constitucional contenida en la Sentencia 76/2019, de 22 de mayo respecto de la norma en la que deben recogerse dichas garantías (F.J.8):

(...) *La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (...). Según reiterada doctrina constitucional, **la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso**, conforme tanto a exigencias denominadas –unas veces– de predeterminación normativa y –otras– de calidad de la ley como al respeto al contenido esencial del derecho, **que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales**. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares. (...)*

De manera más extensa, y como ya ha venido recordando esta AEPD reiteradamente en sus informes:

*[...] debe tenerse igualmente en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, **la misma deberá tener rango de ley**, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo que “podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones*

especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679” y deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente, en las sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, conforme a **la cual los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley**, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. **Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado.** Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata, en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”. Tampoco sirve por ello que

para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGDD.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6).”

*La misma doctrina sostiene el **Tribunal de Justicia de la Unión Europea** (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que*

deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

*Pues bien, la **STJUE de 6 de octubre de 2020**, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:*

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C- 311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

*Igualmente, el apartado 65 de la **Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17)**, Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:*

Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el

alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos.

*Y en dicha **STJUE de 16 de julio de 2020**, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):*

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado

La ya citada STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, *Tele2*, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

*En consecuencia, **los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.***

II

Dicho lo anterior, lo primero que debe hacerse es abordar el tratamiento que se deriva de la norma reglamentaria proyectada, y de la que trae causa (Real Decreto 568/2024), y en especial la finalidad del mismo, para confrontarla con las habilitaciones legales que se encuentran en el marco jurídico de referencia en este ámbito.

La finalidad que persigue el SIVAIN, de acuerdo con la Disposición Final Tercera del Real Decreto 568/2024, de 18 de junio, por el que se crea la Red Estatal de Vigilancia en Salud Pública, es “recoger la información de las

vacunaciones e inmunizaciones de todas las personas que residen en España”.

Y de acuerdo con el artículo 2 de la norma proyectada, la finalidad es:

es disponer de los datos de las vacunas y otros fármacos específicos, utilizados para la inmunización pasiva preexposición y posexposición frente a las enfermedades inmunoprevenibles administrados en España así como los no administrados, pero sí registrados en España, para el seguimiento y evaluación de los programas de vacunación e inmunización. El SIVAIN tiene como objetivo contribuir a la vigilancia, prevención y control de las enfermedades inmunoprevenibles, así como facilitar una aproximación al estado inmunitario de la población con la finalidad de tutelar la salud de la población

y a continuación señala como “fines específicos del sistema” entre otros:

a) Trazabilidad. Disponer de la información mínima requerida de las vacunas y otros fármacos específicos. De manera retrospectiva se podrá consultar la información de las vacunaciones e inmunizaciones en función de determinadas variables de cada individuo. De manera prospectiva se incluirán las vacunas y fármacos específicos que se vayan administrando a lo largo del tiempo. Se incorporarán los históricos de vacunaciones en la medida en que las administraciones indicadas en el Artículo 4 dispongan de esta información individualizada o la puedan facilitar conforme a los requisitos técnicos y formato aprobados en la Comisión de Salud Digital del Sistema Nacional de Salud dependiente del Consejo Interterritorial del Sistema Nacional de Salud.

b) Accesibilidad a la información de vacunación e inmunización. Facilitar que los antecedentes de vacunación e inmunización de cualquier persona que ha recibido o se le ha registrado una vacuna o producto de inmunización en España, sea accesible a los diferentes responsables

asistenciales y de salud pública independientemente de la comunidad autónoma donde se haya administrado o registrado.

c) Contribuir a la realización de estudios de efectividad y otros necesarios para evaluar los programas de vacunación.

d) Contribuir al cumplimiento de los requerimientos de información de organismos internacionales.

e) Permitir el acceso de los interesados a sus datos y posibilitar la emisión de certificados de vacunación a nivel nacional e internacional.

f) Farmacovigilancia. Contribuir al análisis de seguridad y calidad de las vacunas y otros fármacos específicos y a la evaluación de su relación beneficio-riesgo.

Debe recordarse aquí que, en materia de protección de datos, el artículo 6.3 RGPD requiere que la finalidad del tratamiento, cuando estemos ante los supuestos del artículo 6.1 c) y e) RGPD, debe estar determinada en la norma, y que esta debe ser una norma con rango de ley, siendo insuficiente la regulación reglamentaria. Por ello **la finalidad que se indica en el proyecto sometido a informe debe ser coherente con la que, en su caso, se pueda determinar en las leyes habilitadoras al respecto.**

Otros aspectos esenciales a tener en cuenta para analizar la adecuación del tratamiento de datos previsto en la norma proyectada a las previsiones legales, es la referencia que hace sobre el tipo de información a tratar y quién puede acceder la información.

Respecto de la primera, en el Anexo I de la norma proyectada denominado “Variables mínimas incluidas el SIVAIN y obligatoriedad” se incluye la información mínima que se incorporará al sistema, entre la que se encuentra la siguiente:

Vacuna administrada o registrada documentada; ID de registros; ID personal; Fecha de Nacimiento; Sexo; Lugar de residencia; Lugar de administración; Fecha de administración; Vía de administración; Dosificación; Lote; Tipo de producto; Tipo de Antígeno; Marca Comercial; Fabricante; Motivo de Vacunación y Motivo de NO VACUNACIÓN.

Y respecto de la segunda, por un lado, debe citarse lo indicado en el artículo 8 del proyecto sobre la Difusión de la Información, que establece diferentes niveles de acceso para la consulta de datos, y que son los siguientes:

- a) Consulta estadística, a través del portal estadístico del Ministerio de Sanidad.*
- b) Consulta específica para las administraciones responsables de la gestión sanitaria.*
- c) Consulta específica para las administraciones responsables de evaluación de medicamentos y de la farmacovigilancia.*
- d) Consulta específica para profesionales sanitarios.*
- e) Acceso de datos anonimizados o pseudonimizados en el Espacio Nacional de Datos de Salud para uso secundario de los datos con fines de investigación o evaluación en salud pública. Este acceso se realizará mediante solicitud formal, a la Oficina del Dato Sanitario del Ministerio de Sanidad, quien actuará de acuerdo con lo establecido en el modelo de Gobierno del Dato en el Sistema Nacional de Salud y el apartado segundo de la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Y por otro, debe citarse lo dispuesto en el artículo 6.3 del proyecto, a cuyo tenor:

El SIVAIN debe tener la capacidad de intercambiar datos con, al menos, los siguientes sistemas de información y entidades, siempre que sus características técnicas y normativas lo permitan:

- a) Sistemas de información de la Red de Vigilancia en Salud Pública.*
- b) Sistemas de información clínicos, la historia clínica digital (HCD), incluyendo la historia clínica electrónica, registros hospitalarios y otros registros clínicos, principalmente del ámbito público.*
- c) Bases de datos de usuarios como la tarjeta sanitaria individual (TSI) y otras bases de datos poblacionales, como la Mutualidad General de Funcionarios Civiles del Estado (MUFACE), el Instituto Social de las Fuerzas Armadas (ISFAS) y la Mutualidad General Judicial (MUGEJU). De estos registros o sistemas de información se obtendrán los denominadores y los identificadores únicos para cada individuo.*
- d) De Farmacovigilancia (Farmacovigilancia española. Datos de reacciones adversas –FEDRA-), para la evaluación de acontecimientos adversos tras la vacunación y/o sospechas de reacciones adversas a medicamentos.*
- e) De Sanidad Exterior.*
- f) Del Ministerio de Defensa.*
- g) Otros que puedan ser aplicables a los fines del Sistema de Información de Vacunaciones e Inmunizaciones no contemplados en este momento, desarrollados en virtud de lo establecido en la Ley 33/2011, de 4 de octubre, o de la normativa de la Unión Europea. La norma de creación establecerá su inclusión en el sistema o su carácter de fuentes de datos del sistema.*

Finalmente, también debe citarse lo indicado en el apartado 5 del mismo artículo, por su indudable afectación a la protección de datos:

5. El Ministerio de Sanidad a través de la Oficina del Dato Sanitario de la Subdirección General de Información Sanitaria, establecerá el protocolo de acceso a los datos, de acuerdo con la normativa de protección de

datos. Para ello, la Dirección General de Salud Pública y Equidad en Salud establecerá la definición funcional y la Dirección General de Salud Digital y Sistemas de información para el Sistema Nacional de Salud, la definición técnica.

III

Habiéndose identificado los principales elementos de la regulación que tienen una importante incidencia en el derecho a la protección de datos, procede acudir al marco jurídico de referencia para comprobar si el tratamiento de datos que se deriva de la aplicación de la norma proyectada podría encontrar, no sólo un supuesto que dé licitud al tratamiento, que cumpla con el requisito de la determinación en la norma de la finalidad del tratamiento (artículo 6.1 y 3 RGPD) y las garantías exigidas por el Tribunal Constitucional, sino también una causa que levantara la prohibición de tratamiento a la que están sometidas las categorías especiales de datos (artículo 9 RGPD).

Asimismo, deberá analizarse el cumplimiento del resto de principios recogidos en el artículo 5 del RGPD, y la adecuación del SIVAIN a la protección de datos desde el diseño y por defecto de acuerdo con el artículo 25 del RGPD.

Debe partirse de las previsiones contenidas en la Ley 14/1986, de 25 de abril, General de Sanidad, cuyo artículo 8 apartado 1 señala que *“Se considera como actividad fundamental del sistema sanitario la realización de los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica”* estableciendo en su artículo 23, primero del Capítulo V del Título I dedicado a la intervención pública en relación con la

salud individual colectiva, que *“Para la consecución de los objetivos que se desarrollan en el presente capítulo, las Administraciones Sanitarias, de acuerdo con sus competencias, crearán los Registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria”*.

Por su parte, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, además de establecer acciones de coordinación y cooperación de las administraciones públicas sanitarias, define en el artículo 53 los objetivos del «Sistema de Información Sanitaria del Sistema Nacional de Salud», entre los que se encuentran en relación con las “Autoridades Sanitarias”, *favorecer el desarrollo de políticas y la toma de decisiones, dándoles información actualizada y comparativa de la situación y evolución del Sistema Nacional de Salud*; en relación con los “Profesionales”, el objetivo será *mejorar sus conocimientos y aptitudes clínicas. Incluirá directorios, resultados de estudios, evaluaciones de medicamentos, productos sanitarios y tecnologías, análisis de buenas prácticas, guías clínicas, recomendaciones y recogida de sugerencias*; y en relación con los Ciudadanos *facilitar la toma de decisiones sobre su estilo de vida, prácticas de autocuidado y utilización de los servicios sanitarios*

La Ley 33/2011, de 4 de octubre, General de Salud Pública, dedica el Capítulo I del Título II a la vigilancia de la salud pública, estableciendo su concepto y ámbitos en el artículo 12 y las autoridades competentes y la creación, por vía reglamentaria, de la Red de Vigilancia en Salud Pública en el artículo 13:

Artículo 12. De la vigilancia en salud pública.

1. La vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objeto de fundamentar las actuaciones de salud pública. (...)

Artículo 13. Articulación de la vigilancia en salud pública.

1. Corresponde a la Administración General del Estado, a las comunidades autónomas, a las ciudades de Ceuta y Melilla y a la Administración local, en el ámbito de sus competencias, la organización y gestión de la vigilancia en salud pública.

2. Corresponde al Consejo Interterritorial del Sistema Nacional de Salud, a través de la Comisión de Salud Pública, asegurar la cohesión y calidad en la gestión de los sistemas de vigilancia en salud pública.

(...)

Asimismo, determina en su artículo 40 apartado 1 en qué consiste el “Sistema de Información en Salud Pública” al indicar que:

Los sistemas de información en materia de salud pública o cuya información sea relevante en la toma de decisiones en esta materia, con independencia de su titularidad, integrarán el Sistema de Información en Salud pública

Y en su apartado 3, determina la información mínima que habrá de contener:

a) Las estadísticas, registros y encuestas que midan los condicionantes de la salud: educación, situación social, situación laboral, entorno físico y medioambiental, incluyendo los cambios en el clima, seguridad, demografía, economía, servicios, recursos sanitarios, presencia de contaminantes en las personas y cualquier otra variable que el conocimiento científico y las necesidades de la Administración sanitaria hagan necesaria.

b) Las estadísticas, registros y encuestas que midan la salud, la calidad de vida y el bienestar de la población.

c) La información sobre políticas y sobre actuaciones de salud pública en todos los ámbitos de acción.

Pues bien, de los preceptos indicados, y teniendo en cuenta la doctrina del Tribunal Constitucional antes citada (STCs 292/2000 de 30 de noviembre, 76/2019 de 22 de mayo y STC 14/2003, de 28 de enero), no puede afirmarse que puedan dar cobertura en los términos del artículo 6.1 c) o e) del RGPD, y de acuerdo con lo dispuesto en el apartado 3 de dicho artículo, al tratamiento de datos personales que derivaría de la implementación del SIVAIN, tal como se deduce de la norma proyectada (atendiendo a la finalidad del sistema, al tipo de información objeto de tratamiento, y a otros aspectos como el acceso a la información, la conservación, las posibles comunicaciones, las garantías y medidas de seguridad, etc., tal como se expondrá durante el presente informe).

También debe traerse a colación las indicaciones que existen en los cuerpos legales analizados hasta ahora, en relación con el derecho a la protección de datos, que constituyen una garantía y contrapeso frente a cualquier injerencia que pueda suponer el desarrollo de cualquier acción pública en esta materia, y en especial, los sistemas de información.

En el apartado 6, del citado artículo 53 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, se establece que:

“La cesión de los datos, incluidos aquellos de carácter personal necesarios para el sistema de información sanitaria, estará sujeta a la legislación en materia de protección de datos de carácter personal y a las condiciones acordadas en el Consejo Interterritorial del Sistema Nacional de Salud”.

El artículo 7.2 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, dispone lo siguiente:

2. La información personal que se emplee en las actuaciones de salud pública se registrará por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 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

Los apartados 2 y 3 del artículo 41 determinan que:

2. Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.

3. A los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública se someterá a lo dispuesto en el apartado 3 del 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.

Y en el artículo 43 sobre la seguridad e la información se hace constar que:

1. En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos.

2. Los trabajadores de centros y servicios públicos y privados y quienes por razón de su actividad tengan acceso a los datos del sistema de información están obligadas a mantener secreto.

En cuanto a la normativa internacional que incide en esta materia y que se cita en la propia Exposición de Motivos del proyecto, como el Reglamento Sanitario Internacional de 2005, el cual contiene previsiones específicas en materia de protección de datos personales en su artículo 45:

Artículo 45 Tratamiento de los datos personales

1. La información sanitaria que los Estados Parte obtengan o reciban en cumplimiento del presente Reglamento de otro Estado Parte o de la OMS y que se refiera a personas identificadas o identificables será considerada confidencial y tratada de forma anónima según estipule la legislación nacional.

2. Sin perjuicio de las disposiciones del párrafo 1, los Estados Parte podrán dar a conocer y tratar datos personales cuando sea esencial para evaluar y manejar un riesgo para la salud pública, pero los Estados Partes, de conformidad con la legislación nacional, y la OMS se asegurarán de que los datos personales sean:

a) tratados de manera justa y con arreglo a la ley, y evitando todo procesamiento adicional incompatible con esa finalidad;

b) adecuados, pertinentes y no excesivos en relación con esa finalidad;
42 45

c) exactos y, cuando sea preciso, actualizados; deberán adoptarse todas las medidas razonables necesarias para garantizar que los datos inexactos o incompletos sean eliminados o rectificados; y

d) no se conserven más tiempo del necesario.

3. A petición, la OMS proporcionará en lo posible a una persona sus propios datos personales a los que se refiere este artículo de manera inteligible, sin retrasos ni gastos excesivos y, cuando sea necesario, permitirá su corrección.

Asimismo, también se cita en la Exposición de motivos del proyecto el Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo de 23 de noviembre de 2022 sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.º 1082/2013/UE que también incluye previsiones específicas en relación con el tratamiento de datos personales, que queda sujeto a la normativa sobre protección de datos personales, destacando que el mismo debe limitarse a lo estrictamente necesario.

Artículo 27 Protección de datos personales

1. El presente Reglamento se entenderá sin perjuicio de las obligaciones de los Estados miembros en lo relativo al tratamiento de datos personales que efectúen de conformidad con el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE y las obligaciones de las instituciones, órganos y organismos de la Unión en lo relativo al tratamiento de datos personales que efectúen de conformidad con el Reglamento (UE) 2018/1725, en el desempeño de sus funciones.

2. La Comisión y, cuando proceda, otras instituciones, órganos y organismos de la Unión no tratarán datos personales, excepto en aquellos casos en que ello sea estrictamente necesario para el cumplimiento de su misión. Los datos de carácter personal se anonimizarán cuando proceda, de tal modo que el interesado no sea identificable.

Como puede observarse se hace una remisión al sometimiento a la normativa de protección de datos cuya consecuencia inmediata es observar el marco jurídico actual en la materia, constituido fundamentalmente por el RGPD y por

la LOPDGDD, sin perjuicio de otras normas *ratione materiae* que puedan aplicarse al amparo del principio de especialidad normativa.

Tal como se ha indicado antes, de la lectura de los preceptos que se acaban de citar por un lado, y de la finalidad del SIVAIN, y el tipo de datos que sometería a tratamiento, así como el acceso al mismo, por otro, el tratamiento de datos que se plantea en el proyecto sometido a informe no tiene base jurídica de rango suficiente para llevarse a cabo (artículo 6.1 RGPD), ni tampoco podemos entender que se dé alguna circunstancia que levante la prohibición del tratamiento (artículo 9.2 RGPD) que remite a la legislación de la Unión o de los Estados Miembros, todo ello de acuerdo con la doctrina del Tribunal Constitucional referida a que debe ser una norma con rango legal la que establezca la injerencia en el derecho fundamental (STC 292/2000 de 30 de noviembre), y la que establezca los supuestos concretos y las garantías para llevar a cabo dicho tratamiento (STC 76/2019 de 22 de mayo), todo ello sin perjuicio de cumplir el principio de proporcionalidad (por todas la STC 14/2003, de 28 de enero).

En efecto, en las leyes citadas no se encuentra la determinación de la finalidad del tratamiento que persigue el SIVAIN, ni regula los supuestos específicos en los que se permite la injerencia en el derecho a la protección de datos.

Si se pretende legitimar el tratamiento en los apartados c) y e) del artículo 6.1 RGPD, tal como se indica en el apartado 3, la finalidad y los supuestos deben estar determinados en la norma, y una cosa es que están determinados en las leyes citadas, (algo que no sucede) y otra es que por vía reglamentaria, se pretenda establecer dicha finalidad, lo que supone una deslegalización de la materia regulada pues se sustituye la intervención del legislador tal como exige, no solo los preceptos indicados, sino la jurisprudencia que se ha ido citando.

Asimismo, cuando se citan los posibles supuestos que podrían levantar la prohibición de tratamiento (artículo 9.2 h) e i) RGPD), no debe olvidarse que en ambos se hace una remisión al Derecho de la Unión o de los Estados

miembros, derecho que como hemos visto resulta insuficiente por no prever un tratamiento como el que se pretende llevar a cabo con la norma proyectada, y por tanto tampoco se prevén las *medidas adecuadas y específicas para proteger los derechos y libertades del interesado*, pues si bien se hace una remisión al secreto profesional en el artículo 43.2 de la Ley 33/2011, de 4 de octubre, y por extensión al artículo 16.6 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, este deber de secreto profesional se muestra insuficiente en atención a la injerencia que supone el tratamiento de datos del SIVAIN y las obligaciones que se derivan del cumplimiento de otros principios de protección de datos, como el de minimización, de integridad y confidencialidad y la protección de datos desde el diseño y por defecto.

Asimismo, tal como se pondrá de manifiesto a continuación, existen importantes elementos que la norma proyectada no ha tenido en cuenta y que tampoco contempla el marco jurídico de referencia citado, que impide que exista una legitimación (artículo 6.1 y 3 y artículo 9.2 ambos del RGPD) para llevar a cabo el SIVAIN.

Por último y antes de entrar a abordar los aspectos indicados, debe recordarse de nuevo, la remisión que se hace en los preceptos citados al cumplimiento de la normativa de protección de datos (artículo 53.6 Ley 16/2003, de 28 de mayo; artículos 7.2 y 41.3 Ley 33/2011, de 4 de octubre; artículo 45 Reglamento Sanitario Internacional; artículo 27 del proyecto de Reglamento (UE) 2022/2371) en el sentido de que dicha remisión no debe percibirse como una habilitación indeterminada e indefinida para llevar a cabo cualquier tratamiento de datos, sino bien lo contrario, su mención constituye precisamente la obligación de cumplir con dicha normativa en toda su extensión.

Como ejemplo comparativo, podemos poner de manifiesto que la Disposición Adicional primera de la norma proyectada, como ya se ha expuesto, contiene

una regulación que se pretende completa de los tratamientos de datos personales que pudieran derivarse de la norma. Ahora bien, dicha regulación completa, en situaciones similares (ya existan o no tratamientos de datos personales de categorías especiales) se ha llevado a cabo, tras reiterados informes de esta AEPD poniendo de manifiesto lo ya expuesto hasta este momento, mediante normas de rango legal que cumplen con el principio de reserva de ley tan reiterado.

Así, cabe mencionar las siguientes normas con rango de ley formal:

- Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte, ver Disposición Adicional (DA) cuarta;
- Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. DA cuarta
- Ley 20/2022, de 19 de octubre, de Memoria Democrática, DA décima;
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, Título VI, arts. 30 y 32.
- Ley 3/2023, de 28 de febrero, de Empleo, art. 16.
- Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, art. 10, apartados 2, 4, 5, 6, 7, y art. 12.

Obsérvese, además, por último, que la información de vacunación, como dato de salud, estaría incluida en la historia clínica, regulada 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, y por la vía de la norma que ahora se informa se estaría deslegalizando el acceso a dicha información de vacunación sin las garantías específicamente previstas para estos casos, tanto en la citada ley 41/2002, como en la propia

Ley 33/2011, de 4 de octubre, General de Salud Pública. Así, en la primera de estas normas con rango de ley, el art. 16 permite el uso para fines epidemiológicos de la historia clínica, pero para ello se requiere que se preserven los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos, y salvo en los casos de prevención de un riesgo o peligro grave para la salud de la población, como prevé el art. 16.3. Por otra parte, la ley 33/2011, lo que parece prever no es que la Administración tenga los datos de vacunación de todos los españoles, sino que si ello es imprescindible para la toma de decisiones en salud pública (art. 41.3) la autoridad sanitaria podrá *requerir* a todas las personas públicas o privadas, datos de carácter personal, sin necesidad de contar con el consentimiento de los interesados (art. 41.2), y dichas personas públicas o privadas que tengan dichos datos deberán proporcionarlos a la autoridad sanitaria (art. 41.3), reiterando de nuevo la aplicación del art. 16.3 de la ley 41/2002 para los tratamientos de datos personales por razones epidemiológicas.

IV

Tal como nos recuerda la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de Octubre de 2024 (Asunto C-446/2021) en sus apartados 46 y 47 *todo tratamiento de datos personales debe, por una parte, ser conforme con los principios relativos al tratamiento de tales datos enunciados en el artículo 5 del mismo Reglamento y cumplir las condiciones de licitud enumeradas en su artículo 6 y, por otra parte, respetar los derechos del interesado que figuran en los artículos 12 a 22 del RGPD [sentencia de 11 de julio de 2024, Meta Platforms Ireland (Acción de representación), C-757/22, apartado 49 y jurisprudencia citada]. (...) 47. Como ya ha puntualizado el Tribunal de Justicia,*

los principios relativos al tratamiento de datos personales enunciados en el artículo 5 del RGPD son aplicables de forma acumulativa (sentencia de 20 de octubre de 2022, Digi, C-77/21, apartado 47) .

En efecto, para que el tratamiento de datos personales sea conforme al RGPD, deben cumplirse los principios de protección de datos, recogidos en el artículo 5 del RGPD a cuyo tenor.

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; 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»).

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

Asimismo, el artículo 25 del RGPD, bajo la denominación “Protección de Datos desde el diseño y por defecto” establece que:

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.

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.

V

En el presente caso, y sin perjuicio de que, como hemos visto, el tratamiento de datos que supone el SIVAIN no cumpliría con el principio de licitud por falta de base jurídica suficiente (apartado 1. a) del artículo 5 y artículo 6.1 ambos del RGPD), procede analizar otros aspectos de la norma proyectada en relación con el resto de los principios.

En relación con el principio de limitación de la finalidad, y teniendo en cuenta que en las leyes citadas no se encuentra determinada la misma (artículo 6.3 RGPD) y con el principio de minimización, no se encuentra en la norma (ni en la MAIN) explicación que justifique que se deba recoger la identificación de la persona vacunada, ni tampoco el motivo de recoger la NO vacunación, como recoge expresamente el citado Anexo, con el peligro añadido que dicha información supone, y que recuerda casos que desgraciadamente se han dado en la historia que, habiéndose regulado con buena voluntad inicial y para fines concretos y en principio aceptables la recopilación de determinados datos personales, de carácter especialmente protegido, dieron lugar a consecuencias funestas para los derechos fundamentales (a la vida, a la libertad, a la no discriminación por razón de etnia etc.) de los interesados cuando los datos personales recopilados se utilizaron para fines diferentes de los previstos.

Respecto de la identidad de la persona vacunada, no encuentra justificación su utilización para cumplir los fines del sistema en los términos que está redactada la norma. Para facilitar los antecedentes de vacunación y permitir el acceso de los interesados a sus datos, ya existe la historia clínica que recoge los episodios asistenciales y que está previsto en la Ley de Autonomía del Paciente, que regula los supuestos de acceso a la información, sin perjuicio de las leyes autonómicas correspondientes en tanto que es legislación básica.

Para las otras finalidades, tampoco se justificaría la obtención de la identidad del paciente; ni en la exposición de motivos, ni en la MAIN, ni tampoco en los cuerpos legales citados se puede deducir siquiera la necesidad de tratamiento de esa información. Llegados a este punto es preciso traer a colación las Directrices 4/2019 relativas al artículo 25 del RGPD, del Comité Europeo de Protección de Datos, adoptadas el 20 de octubre de 2020, indican en su apartado 75 que:

La minimización también puede referirse al grado de identificación. Si la finalidad del tratamiento no requiere que el conjunto final de datos se refiera a una persona física identificada o identificable (como en las estadísticas), pero el tratamiento inicial sí (por ejemplo, antes de la agregación de datos), el responsable del tratamiento suprimirá o anonimizará los datos personales tan pronto como la identificación deje de ser necesaria. O bien, si se requiere una identificación continua para otras actividades de tratamiento, los datos personales deberán ser seudonimizados a fin de mitigar los riesgos para los derechos de los interesados.

Tampoco se explica cuál es la razón para la existencia y cumplimentación obligatoria que consta en el Anexo I, en el campo “Motivo de la No Vacunación” cuando, en principio, el SIVAIN contendría información de las vacunas administradas, no de las no administradas. Además no se explica la necesidad de dicha información, por lo que igualmente se desconoce la finalidad de esta

actividad de tratamiento. Tal y como expondremos más adelante en este informe, no se ha aportado un análisis de los riesgos que dicha norma puede suponer en los derechos y libertades de los interesados, ni se ha realizado una evaluación de impacto en protección de datos (EIPD) que determine las medidas organizativas, técnicas, de seguridad etc., para eliminar o minimizar el impacto de la norma.

Nos dice el Considerando 39 del RGPD que los *datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados (...)* y añade que (...) *Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios*

También deben entenderse comprometidos por la regulación propuesta los principios de minimización, de integridad y confidencialidad y la protección de datos desde el diseño y por defecto.

En las citadas Directrices 4/2019 del CEPD, se establece en sus apartados 42, 44 y 45 lo siguiente:

42. El responsable debe elegir y responsabilizarse de aplicar parámetros y opciones de tratamiento por defecto de manera que, por defecto, solo se lleve a cabo el tratamiento que sea estrictamente necesario para cumplir el fin lícito establecido. En este caso, los responsables deberán basarse en su evaluación de la necesidad del tratamiento por lo que respecta a los fundamentos jurídicos del artículo 6, apartado 1. Esto significa que, por defecto, el responsable del tratamiento no debe recoger más datos de los que sean necesarios, ni realizar un tratamiento de los datos recogidos más amplio de lo necesario para sus fines, ni conservar los datos durante más tiempo del necesario. El requisito básico es que la protección de datos esté integrada en el tratamiento por defecto.

(...)

44. Si el responsable utiliza software de terceros o software comercial estándar, deberá realizar una evaluación de riesgos del producto y asegurarse de que las funciones que no tengan base jurídica o que no sean compatibles con los fines previstos del tratamiento estén desactivadas.

45. Las mismas consideraciones son aplicables a las medidas organizativas de apoyo a las operaciones de tratamiento. Deben estar concebidas para tratar, desde el principio, únicamente la cantidad de datos personales mínima necesaria para las operaciones específicas. Esto debe tenerse especialmente en cuenta a la hora de asignar el acceso a los datos a personas con diferentes funciones y diferentes necesidades de acceso. (...)

El artículo 8.1 de la norma proyectada establece que

1. Se facilitarán diferentes niveles de acceso para la consulta de los datos:
 - a) Consulta estadística, a través del portal estadístico del Ministerio de Sanidad.
 - b) Consulta específica para las administraciones responsables de la gestión sanitaria.
 - c) Consulta específica para las administraciones responsables de evaluación de medicamentos y de la farmacovigilancia.
 - d) Consulta específica para profesionales sanitarios.
 - e) Acceso de datos anonimizados o pseudonimizados en el Espacio Nacional de Datos de Salud para uso secundario de los datos con fines de investigación o evaluación en salud pública.

Este acceso se realizará mediante solicitud formal, a la Oficina del Dato Sanitario del Ministerio de Sanidad, quien actuará de acuerdo con lo establecido en el modelo de Gobierno del Dato en el Sistema Nacional de Salud y el apartado segundo de la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

No se justifica en la norma la razón por la que se hace dicha estructura y la finalidad que se persigue con la misma. Deber recordarse aquí que, en cuanto a la finalidad en protección de datos, no es posible confundir necesidad con conveniencia. Se desconoce en qué medida podría servir a cumplir la finalidad del sistema.

No puede crearse por una norma de este rango, y aun si no fuera así (es decir, si existiera norma legal), sin una justificación de la finalidad y los demás requisitos expuestos en la doctrina del Tribunal Constitucional citada, una “base de datos universal” con la identidad de las personas vacunadas, y con la vacuna administrada en el que el acceso a la misma no se permita en función de la competencia, función, puesto, etc. Así, por ejemplo, para los apartados a), b) y c) no estaría justificado el acceso a la identidad de las personas vacunadas, pues en función de la finalidad perseguida podría cumplirse la misma sin conocer esa información.

Las Directrices 4/2019 del CEPD, indican en este sentido en sus apartados 55, 56 y 59:

55. El responsable del tratamiento debe limitar quién tiene acceso y qué tipo de acceso a los datos personales en función de una evaluación de necesidades y asegurarse además de que los datos personales sean efectivamente accesibles para quienes los necesiten cuando los necesiten, por ejemplo en situaciones críticas. Deben observarse controles de acceso para todo el flujo de datos durante el tratamiento.

56. El artículo 25, apartado 2, establece además que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. Por defecto, el responsable del tratamiento debe limitar la accesibilidad y ofrecer al interesado la posibilidad de intervenir antes de publicar o poner de otro modo datos personales acerca del interesado a disposición de un número indeterminado de personas físicas.

59. Aun en el caso de que los datos personales se pongan a disposición del público con el permiso y entendimiento del interesado, ello no significa que cualquier otro responsable del tratamiento que tenga acceso a los datos personales pueda tratarlos libremente por su cuenta y para sus propios fines: estos siempre deben tener su propia base jurídica.

Para garantizar el cumplimiento del principio de confidencialidad, debería estructurarse el SIVAIN de tal modo que únicamente puedan acceder los distintos sujetos para cumplir una concreta finalidad.

Para ello sería necesario establecer un acceso mediante autenticación y contraseña y un registro de acceso. De modo que se impida un acceso universal tanto desde el punto de vista de quién accede como desde el punto de vista de a lo que se accede. (Gestión del Control de Acceso con la oportuna (i) Limitación de Acceso en cuanto a los agentes que pueden acceder, (ii) Limitación de Acceso en cuanto al contenido al que se puede acceder, y (iii) Segregación de Acceso en cuanto a la cantidad de información sobre una persona. Apartado 85 de las Directrices 4/2019).

En relación con este aspecto, es preciso el artículo 6.5 de la norma proyectada, que dispone que:

5. El Ministerio de Sanidad a través de la Oficina del Dato Sanitario de la Subdirección General de Información Sanitaria, establecerá el

protocolo de acceso a los datos, de acuerdo con la normativa de protección de datos. Para ello, la Dirección General de Salud Pública y Equidad en Salud establecerá la definición funcional y la Dirección General de Salud Digital y Sistemas de información para el Sistema Nacional de Salud, la definición técnica.

Las garantías de acceso y confidencialidad deberían estar previstas en la ley, (artículos 6.3 y 9.2 h) e l) RGPD) no puede establecerse por vía reglamentaria una remisión a las decisiones que se adopten por órganos directivos de la administración pública.

No es que la ley deba abordar con ese detalle el acceso (pues cuestiones técnicas como esas son las que están llamadas a regularse por vía reglamentaria), sino que sea la propia ley la que imponga la obligación de exigir un modo de acceso que garantice la confidencialidad de los datos, y el cumplimiento de los principios de limitación de finalidad, de minimización y la protección de datos por defecto.

Otro aspecto importante que tampoco aborda la norma proyectada es la observancia del principio de exactitud y de integridad de los datos personales. El SIVAIN debería disponer de medidas que impidieran la modificación, la extracción y en su caso la eliminación de la información. Esta necesidad va más allá de la identificación sobre el acceso, sino que debería establecerse los supuestos en los que la información contenida en el SIVAIN pudiera ser modificada, extraída del sistema y en su caso eliminada.

Las Directrices 4/2019 resultan especialmente clarificadoras en relación con el principio de exactitud y la relevancia de su cumplimiento, así en su apartado 78 indica que:

(...) Los datos personales inexactos podrían suponer un riesgo para los derechos y libertades de los interesados, por ejemplo, cuando den lugar a un diagnóstico erróneo o a un tratamiento injustificado de un protocolo

de salud, o puede que una imagen incorrecta de una persona ocasione que se tomen decisiones por motivos incorrectos, bien sea manualmente, bien mediante un proceso de toma de decisiones automatizado o bien mediante inteligencia artificial

Y en su apartado 79 propone elementos que considera esenciales desde el diseño y por defecto con respecto a la exactitud:

- *Fuente de los datos: Las fuentes de datos personales deben ser fiables en cuanto a la exactitud de los datos.*
- *Grado de exactitud: Cada elemento de datos personales deberá ser tan exacto como sea necesario para los fines especificados.*
- *Exactitud medible: Se reducirá el número de falsos positivos o negativos, por ejemplo, sesgos en las decisiones automatizadas y la inteligencia artificial.*
- *Verificación: En función de la naturaleza de los datos, en relación con la frecuencia con la que puedan cambiar, el responsable deberá contactar con el interesado para verificar si los datos personales son correctos antes del tratamiento y en sus diferentes fases (por ejemplo, cuando existan requisitos de edad).*
- *Supresión y rectificación: El responsable del tratamiento debe suprimir o rectificar los datos inexactos sin dilación. El responsable deberá facilitar esto, en particular, cuando los interesados sean o hayan sido menores y posteriormente quieran eliminar dichos datos personales³⁹.*
- *Evitación de la propagación de errores: Los responsables deben mitigar el efecto de un error acumulado en la cadena de tratamiento.*
- *Acceso: Se debe facilitar a los interesados información acerca de sus datos personales y acceso efectivo a los mismos, de conformidad con*

los artículos 12 a 15 del RGPD, a fin de controlar su exactitud y rectificarlos si es necesario.

- *Exactitud continuada: Los datos personales deben ser exactos en todas las fases del tratamiento, debiendo llevarse a cabo pruebas de exactitud en puntos críticos.*
- *Actualizados: Los datos personales se actualizarán si es necesario para el fin previsto.*

Todas estas cuestiones, y las que estime el responsable del tratamiento de acuerdo con el principio de responsabilidad proactiva, son las que deberían haberse tenido en cuenta el prelegislador en la regulación el SIVAIN, y que nada se indica en la norma proyectada.

Todo ello sin perjuicio de reiterar que el cumplimiento de los requisitos que se acaban de exponer no puede suplir la necesaria intervención del legislador tal como se ha puesto de manifiesto durante el presente informe.

VI

Siguiendo con el principio de integridad y confidencialidad, y la adopción de medidas de seguridad adecuadas, es preciso traer a colación la necesidad, como ya hemos mencionado anteriormente, de realización del correspondiente análisis de riesgos y de la Evaluación de Impacto en Protección de Datos (EIPD).

Ni en la norma proyectada ni en la MAIN aportada a la consulta se hace referencia a estos elementos.

El artículo 28.2 de la LOPDGDD, establece lo siguiente:

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones 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, moral o social significativo para los afectados.

(...)

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

(...)

En el presente caso la norma proyectada regula el SIVAN, que es un sistema de información que contiene categorías especiales de datos, (datos de salud), que la información tratada está sujeta al secreto profesional, que supone un tratamiento a gran escala de este tipo de datos, y que un uso inadecuado o indebido puede causar situaciones de discriminación, no solo en la “población general”, sino también en colectivos especialmente vulnerables (piénsese en menores de edad y el impacto que puede tener en según qué entornos conocer que se está vacunado o que no se está vacunado de según qué- enfermedad).

Por todo ello, se debería, por parte de los responsables del tratamiento, analizarse el riesgo del tratamiento que supone la creación del SIVAIN, teniendo en cuenta, en especial, estos aspectos que se acaban de indicar, para así determinar las medidas de seguridad adecuadas que permitan cumplir el RGPD y la LOPDGDD.

Análisis de riesgos que como se ha indicado anteriormente, se desconoce si se ha llevado a cabo, ya que no se ha incorporado a la norma ni se hace mención en la MAIN.

En cuanto a la Evaluación de Impacto, el artículo 35 apartados 1, 3 y 10 del RGPD lo siguiente:

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

(...)

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: (...)

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

(...)

*10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, **tal Derecho regule la operación específica de tratamiento** o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.*

En el presente caso, teniendo en cuenta que se pretende el tratamiento de datos de salud a gran escala, y en consecuencia, atendiendo al alto riesgo de dichos tratamientos, hubiera sido muy conveniente haberse realizado por el prelegislador la Evaluación de impacto en la protección de datos (EIPD), y adjuntarse esta como anexo a la MAIN, conforme a lo previsto en el artículo 35.10 del RGPD, que permita identificar adecuadamente los riesgos derivados de dichos tratamientos e incorporar en la norma las garantías oportunas.

No podemos considerar como tal el mero hecho de que en la MAIN exista un apartado denominado Impacto en materia de protección de datos, que se limita a transcribir la disposición adicional primera del proyecto, en el que se abordan los aspectos relativos a la protección de datos -sin incluir ningún aspecto de los

analizados durante el presente informe -, lo que no constituye por tanto ni un análisis de riesgos ni una evaluación de impacto.

Para la elaboración de la evaluación que se acompañe a la norma, deberían tenerse en cuenta las indicaciones recogidas en las “Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”, recientemente publicadas por esta Agencia (<https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>).

VII

Sin perjuicio de las carencias que se han ido citando en el presente informe sobre la norma reglamentaria proyectada, procede realizar las siguientes consideraciones al contenido de la Disposición Adicional Primera, denominada *Tratamiento de datos de carácter personal*, por si en la correspondiente modificación legislativa se incluyera una disposición específica en materia de protección de datos, tal como ya se ha hecho en las leyes que se han citado a título de ejemplo en el apartado III del presente informe, al que se hace la oportuna remisión.

En primer lugar a efectos sistemáticos, se propone que en el apartado 2 se incluya la información relativa a los responsables del tratamiento en lugar de aparecer en el apartado 4 y que inmediatamente después se aborde la regulación del encargado del tratamiento, y no como consta en la actualidad que figura en un apartado antes. Es decir, primero responsables del tratamiento, y en su caso, después encargados del tratamiento.

Dicho esto, en cuanto al contenido del apartado que identifica a los responsables del tratamiento, este está redactado en los siguientes términos:

4.Los responsables de los tratamientos del sistema serán el Ministerio de Sanidad, el Instituto Nacional de Gestión Sanitaria, las comunidades autónomas y ciudades de Ceuta y Melilla, el Ministerio de Defensa y el

órgano responsable de la coordinación de los programas de vacunación en salud pública, cada una en el ámbito de sus respectivas competencias en el ámbito sanitario, los cuales deberán garantizar la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos y evaluación de impacto, teniendo en cuenta que se trata de un tratamiento a gran escala de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos, y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad .

El apartado identifica al responsable del tratamiento y también trata otras obligaciones derivadas de tal condición que se abordan en otros apartados de la disposición adicional. Es decir, mezcla aspectos que debe estar abordados de manera individual.

Se propone la siguiente redacción de este apartado:

4.Los responsables de los tratamientos del sistema serán el Ministerio de Sanidad, el Instituto Nacional de Gestión Sanitaria, las comunidades autónomas y ciudades de Ceuta y Melilla, el Ministerio de Defensa y el órgano responsable de la coordinación de los programas de vacunación en salud pública, cada una en el ámbito de sus respectivas competencias en el ámbito sanitario.

Se suprime las referencias a la evaluación de impacto y al ENS, ya que se incluyen posteriormente en el conjunto de apartados referidos a la seguridad del tratamiento, y al cumplimiento del principio de integridad y confidencialidad.

En segundo lugar, tanto en el apartado 2, como en el apartado 8 de la disposición se hace referencia a las bases jurídicas del tratamiento, o dicho de otro modo, a la adecuación al principio de licitud, por lo que para darle

coherencia a la sistemática se propone que se modifiquen ambas de modo que se integren en la medida de lo posible o en su defecto, consten de manera sucesiva.

Dicho lo anterior en el apartado 2 de la disposición, se indica que:

2. Las bases jurídicas para el tratamiento de datos se encuentran recogidas en el art.6.1.c) y e) del Reglamento General de Protección de Datos. Los datos personales de salud se usarán para los fines del sistema, y que se respetará el principio de minimización de datos. Conforme a lo previsto en el artículo 9.2.h) y 9.2.i) será lícito el tratamiento de datos personales relacionados con la salud cuando ello sea estrictamente necesario para la tutela de la salud de la población.

Y en el apartado 8 consta lo siguiente:

8. Las administraciones sanitarias responsables de los programas de vacunación, no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras administraciones públicas sanitarias, cuando ello sea necesario por razones de interés público en el ámbito de la salud pública o en el ejercicio de poderes públicos y en cumplimiento de obligaciones legales, conforme al artículo 9.2 y al artículo 6. 1. c) y e) del Reglamento General de Protección de Datos y al artículo 41 de la Ley 33/2011, de 4 de octubre. En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública que realizan las administraciones sanitarias con estas funciones se someterá a lo dispuesto en el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, de acuerdo con la disposición final tercera de la Ley 33/2011, de 4 de octubre.

Se propone la inclusión en el apartado 2, de una referencia general de los principios del tratamiento, y añadir a la cita del principio de minimización de

datos, el de integridad y confidencialidad, así como integrar parte del apartado 8 (que quedaría suprimido) de dicha disposición en la medida que aborda la no exigibilidad del consentimiento, de tal modo que el texto quede como sigue:

2. Las bases jurídicas para el tratamiento de datos se encuentran recogidas en el artículo 6.1.c) y e) del Reglamento General de Protección de Datos. El tratamiento de los datos personales se realizará conforme a los principios del tratamiento, en especial de acuerdo con el de minimización y con el de integridad y confidencialidad. Conforme a lo previsto en el artículo 9.2.h) y 9.2.i) será lícito el tratamiento de datos personales relacionados con la salud cuando ello sea estrictamente necesario para la tutela de la salud de la población. En consecuencia, las administraciones de los programas de vacunación no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras administraciones públicas sanitarias de conformidad con lo dispuesto en el artículo 41 de la Ley 33/2011, de 4 de octubre.

Se ha excluido la referencia los acceso a las historias clínicas para integrarlo en otro apartado que aborde la seguridad del tratamiento, y la adecuación al principio de integridad y confidencialidad.

A continuación se propone que se aborde el tipo de datos a someter a tratamiento. Comenzando por la referencia que se realiza en el apartado 5 que cita el Anexo I de recogida de datos. Este sería el primer apartado de los que se refieren a los datos objeto de tratamiento. Se reitera aquí en relación con el campo ID personal, éste deberá ser accesible únicamente en función de la finalidad que este llamado a cumplir el sujeto o sujetos que accedan al SIVAIN, **impidiendo así un acceso universal a los datos de identificación.**

A continuación, se propone abordar las cuestiones relativas a la seguridad del sistema, tanto en su vertiente de protección de datos (RGPD) como en su vertiente de seguridad de la información (ENS).

En dos apartados referidos a seguridad y confidencialidad, se propone que se integren los apartados 9, 10 y 11 y se incluya en ellos una referencia a la necesidad de que el acceso, al que se refiere el artículo 6.4 y artículo 8 del proyecto, se realice mediante identificador y contraseña y con un registro de acceso. De tal modo que se crean nuevos apartados 8 y 9, y se renumeran los 9, 10 y 11, que pasan a ser 10, 11, y 12.

8. Los responsables del tratamiento a los que se refiere el apartado 4, deberán realizar con carácter previo al inicio del tratamiento la correspondiente Evaluación de Impacto, y establecer las medidas de seguridad adecuadas, teniendo en cuenta en especial, tanto las categorías especiales de datos objeto de tratamiento como el volumen de datos contenidos en el SIVAIN, para garantizar el cumplimiento del RGPD y su adecuación al Esquema Nacional de Seguridad.

9. Para el acceso al SIVAIN, y sin perjuicio de otras medidas acordadas por el responsable del tratamiento previa realización del correspondiente análisis de riesgos, deberán implantarse medidas de seguridad, como el acceso mediante identificación y el establecimiento de un registro de accesos, para garantizar que el tratamiento se realiza de acuerdo al principio de minimización, y el principio de integridad y confidencialidad. Estas medidas se tendrán en cuenta en la elaboración del protocolo de acceso que establecerá reglamentariamente.

10. Todas las personas que tengan acceso a los datos generados como consecuencia de la puesta en marcha del SIVAIN están sometidos al deber de secreto, de conformidad con lo dispuesto en

el artículo 43.2 de la Ley 33/2011, de 4 de octubre, General de Salud Pública y el artículo 16.6 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. El acceso a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública que realizan las administraciones sanitarias responsables de los programas de vacunación e inmunización 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.

11. Los datos recogidos por SIVAIN podrán cederse a terceras partes, como instituciones académicas o centro de investigación, para la realización de estudios de investigación o evaluación utilizando siempre datos anonimizados o pseudonimizados, garantizando la protección de la confidencialidad y la privacidad conforme a la normativa aplicable en materia de protección de datos. La cesión de datos a terceras partes deberá responder a las finalidades que establece esta ley y se realizará de acuerdo con lo dispuesto en el Reglamento General de Protección de Datos y en lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.

12. Los datos recogidos en SIVAIN estarán disponibles de forma abierta para su acceso por los interesados. La información se facilitará excluyendo datos personales. Este acceso podrá efectuarse dentro de los límites fijados por la normativa en materia de derecho de acceso a la información pública, la de protección de datos de carácter personal, así como –en su caso– las derivadas de las garantías para unidades informantes sobre confidencialidad y secreto estadístico. Los responsables de los tratamientos de

SIVAIN, valorarán aquella información que no podrá ser objeto de difusión abierta para los interesados, a los efectos de cumplir con la citada normativa.

VIII

En conclusión, se informa desfavorablemente la norma proyectada ya que el tratamiento de datos que supondría el SIVAIN no encuentra legitimación en el marco jurídico actual de referencia y en consecuencia no pueden aplicarse los supuestos previstos en los apartados c) y e) del artículo 6.1 del RGPD como base jurídica por falta de habilitación legal. Sería necesario una norma de rango legal, de acuerdo con la jurisprudencia constitucional tan reiterada, (por todas, STC 76/2019).

La norma reglamentaria no puede suplir las deficiencias del actual marco jurídico, por lo que debería procederse a la oportuna modificación legislativa para dar cumplimiento a las exigencias del artículo 6.3 del RGPD y la doctrina del Tribunal Constitucional derivada de las Sentencias 292/2000 de 30 de noviembre, 76/2019 de 22 de mayo y STC 14/2003, de 28 de enero), en cuanto a la determinación por ley de los supuestos en los que se permita la injerencia en el derecho a la protección de datos y las garantías adoptadas, todo ello de acuerdo con el principio de proporcionalidad.

Asimismo, la regulación de la norma proyectada sería contraria a los principios de limitación de la finalidad, de minimización, de integridad y confidencialidad, y de la protección de datos desde el diseño y por defecto. Las indicaciones que se realizan en el presente informe al respecto de estos principios deben ser tenidas en cuenta en una hipotética modificación legislativa para que el SIVAIN se adecuara al marco jurídico actual en materia de protección de datos personales, en coherencia con la remisión a la normativa de protección de

datos, que, en reiteradas ocasiones, realizan los cuerpos legales citados en el presente informe.

Por último, debe tenerse en cuenta que dicha modificación legislativa se vería afectada también, por el Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios (que a la fecha del presente informe no ha sido aun promulgado formalmente o publicado en el DOUE), ya que el artículo 34.1a) incluye, entre los fines para los que pueden tratarse datos sanitarios electrónicos para uso secundario, “las actividades de interés público en el ámbito de la salud pública y la salud laboral, como la protección contra las amenazas transfronterizas graves para la salud, la vigilancia de la salud pública o la garantía de unos niveles elevados de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios”.

A este respecto, la propuesta recoge una serie de garantías específicas dirigidas a garantizar la protección de datos de carácter personal, que deberían tenerse en cuenta, como son las relativas a la prohibición del uso secundario de datos sanitarios electrónicos (artículo 35), las funciones de los organismos de acceso a los datos sanitarios (artículo 37) la minimización de datos y limitación de la finalidad (artículo 44), las solicitudes de acceso a los datos (artículo 45) o el entorno de tratamiento seguro (artículo 50).

Asimismo, en relación con el desarrollo de espacios comunes de datos al amparo del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos o DGA), esta Agencia ha publicado recientemente el documento “Aproximación a los espacios de datos desde la perspectiva del RGPD” (<https://www.aepd.es/es/documento/aproximacion-espacios-datos-rgpd.pdf>), con recomendaciones que pueden ser de utilidad en el presente caso para el adecuado cumplimiento del RGPD.