012/2026

El proyecto de Real Decreto por el que se regula el Sistema de Información de Vacunaciones e Inmunizaciones **(SIVAIN)** tiene por objeto establecer el marco jurídico, organizativo y técnico de un instrumento estatal integrado en el Sistema de Información de Salud Pública, creado en desarrollo de 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. Este sistema se configura como una herramienta esencial para la coordinación, evaluación y explotación homogénea de la información relativa a las vacunaciones e inmunizaciones en todo el territorio nacional, con el fin de contribuir a la vigilancia, prevención y control de enfermedades inmunoprevenibles.

En nuestro **Informe 0047/2024,** de 24 de octubre de 2024, la Agencia analizó una versión anterior del proyecto normativo y emitió un **informe desfavorable**, al considerar que el tratamiento de datos personales, especialmente los relativos a la salud, calificados como categorías especiales de datos, según el artículo 9 del Reglamento General de Protección de Datos, carecía de una base jurídica suficiente con rango de ley formal, tal como exige el artículo 6.3 del RGPD y la jurisprudencia del Tribunal Constitucional (TC) y del Tribunal de Justicia de la Unión Europea (TJUE). En concreto, se señalaba que el proyecto no cumplía con los requisitos derivados de la doctrina constitucional establecida en las Sentencias 292/2000, de 30 de noviembre; 76/2019, de 22 de mayo; y 14/2003, de 28 de enero, que exigen que los límites al derecho fundamental a la protección de datos sean establecidos por una norma con rango de ley, previa ponderación de los intereses en conflicto y con sujeción al principio de proporcionalidad.

Asimismo, en dicho informe se advirtió que el proyecto normativo resultaba contrario a los principios de limitación de la finalidad, minimización, integridad y confidencialidad, así como a las exigencias de protección de datos desde el diseño y por defecto —artículo 25 del RGPD—. Se concluyó, por tanto, que el proyecto debía ser adecuado al marco jurídico aplicable en materia de protección de datos, incorporando las garantías y condiciones necesarias para cumplir con los estándares constitucionales y comunitarios.

No obstante lo anterior, debe señalarse que, en la actualidad, el marco legal vigente en materia de protección de datos —especialmente los artículos 41 y 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, y el artículo 16 de la Ley 41/2002, de 14 de noviembre— ya establecen un núcleo de garantías legales aplicables al tratamiento de datos de salud. Estas normas regulan aspectos tales como la delimitación legal de la finalidad, los

criterios de necesidad y proporcionalidad, los sujetos legitimados para acceder a datos, las medidas de seguridad generales y el deber de secreto.

I

El 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales —LOPDGDD—, conforman el marco jurídico de referencia en España que afecta a la protección de datos de carácter personal. En estas normas se regulan los principios y fundamentos a los que deben ajustarse la recogida y el tratamiento de los datos personales por cualquier persona pública o privada que lleve a cabo tratamiento de datos de carácter personal en el ejercicio de su actividad.

Entre otras definiciones, el artículo 4 del RGPD se refiere a «datos personales» como toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Y «tratamiento» como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Por su parte, el apartado 1 del artículo 2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que: *“Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente Ley Orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.”*

Pues bien, según se extrae del texto normativo que se informa, de acuerdo con lo previsto en su articulado, se procederá al tratamiento de datos de carácter personal. Así, especialmente, se prevén, entre otros, los siguientes tratamientos de datos personales, incluyendo datos relativos a la salud:

- Recogida, registro y validación de datos identificativos y clínicos relativos a la administración de vacunas y otros medicamentos específicos en todo el territorio nacional (artículos 1, 2, 4 y 8; disposición transitoria única y Anexo I).

- Incorporación, estructuración y conservación de dichos datos en el Sistema de Información de Vacunaciones e Inmunizaciones, con integración e interoperabilidad con otros sistemas de información sanitaria (artículo 6; artículo 8; disposición adicional primera).

- Procesos automatizados de seudonimización de los datos personales con fines de análisis, evaluación y explotación estadística o de salud pública (artículo 8; disposición adicional primera —apartado relativo al algoritmo de seudonimización—).

- Consulta y acceso a datos identificativos y clínicos por profesionales sanitarios para fines asistenciales y de prevención de riesgos graves para la salud pública (artículo 9; artículo 10.1; disposición adicional primera —apartados relativos a acceso, secreto profesional y condiciones de acceso—).

- Acceso a datos seudonimizados o anonimizados para fines de evaluación de programas, investigación sanitaria, farmacovigilancia y cumplimiento de obligaciones de información nacionales e internacionales (artículo 10; disposición adicional primera —apartados relativos a cesiones para investigación, tratamiento ulterior y garantías del artículo 89 RGPD—).

- Cesión o comunicación de datos anonimizados o seudonimizados a terceros legitimados, incluidos organismos de investigación, así como posibles intercambios internacionales en los supuestos previstos normativamente (artículo 10.2; disposición adicional primera —apartados sobre cesiones, reutilización, intercambio internacional y datos abiertos agregados—).

En resumen, habida cuenta del objeto y del contenido del proyecto normativo que se informa, se llevarán a cabo tratamientos de datos de carácter personal, cuyo análisis de necesidad resulta imprescindible en atención a las exigencias derivadas de la normativa de protección de datos.

En este contexto, destaca la existencia de una **regulación específica** sobre protección de datos de carácter personal, incorporada al contenido de la *Disposición adicional primera* del proyecto reglamentario, en la que, bajo el epígrafe *"Tratamiento de datos de carácter personal"* se dispone:

"Disposición adicional primera. Tratamiento de datos de carácter personal.

1. Los tratamientos de datos personales regulados en este Real Decreto se llevarán a cabo conforme a lo dispuesto en el 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 (en adelante, Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Los responsables de los tratamientos del sistema serán el Ministerio de Sanidad, las Comunidades Autónomas y ciudades de Ceuta y Melilla y el Ministerio de Defensa, cada una en el ámbito de sus respectivas competencias en el ámbito sanitario.

3. En el supuesto de que intervenga una entidad ajena a los responsables del tratamiento como encargada del tratamiento, deberá suscribirse con los respectivos responsables del tratamiento el correspondiente instrumento en los términos previstos en el artículo 28.3 del Reglamento General de Protección de Datos.

4. Las bases jurídicas para el tratamiento de datos personales son los apartados c) y e) del artículo 6.1. del Reglamento General de Protección de Datos y, de acuerdo con el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las normas con rango de ley que constituyen la base jurídica que fundamenta el tratamiento de datos personales son el artículo 8.1 de la Ley 14/1986, de 25 de abril, General de Sanidad, el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; los artículos 1, 11, 69 y 71.2.c de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y los artículos 12, 13, 19, 22, 23, 40, 41, 42 y 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública. 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.

Respecto a los datos personales de salud, las administraciones de los programas de vacunación no precisarán obtener el consentimiento de las personas afectadas para el tratamiento en atención a las circunstancias previstas en las letras h) e i) del artículo 9.2 del Reglamento General de Protección de Datos. De acuerdo con el artículo 9.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las normas con rango de ley que amparan el tratamiento de estos datos personales de salud son el artículo 8.1 de la Ley 14/1986, de 25 de abril, General de Sanidad, el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica,

el artículo 1 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y los artículos 12, 13 y 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública. 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.

5. La información a recoger y tratar se establece en el Anexo I, en base al documento de Requerimientos Funcionales, aprobado por acuerdo de la Comisión de Salud Pública del Consejo Interterritorial del Sistema Nacional de Salud.

6. El Ministerio de Sanidad utilizará un algoritmo de seudonimización para garantizar la adecuada interoperabilidad con las bases de datos establecidas en el artículo 6.5 y garantizar la posibilidad de ejecutar analíticas de datos avanzadas basadas en identificadores seudonimizados, explotando el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud aprobados por el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud. Los datos personales de identificación recibidos y utilizados para la validación son el nombre y apellidos, el código SNS (CIPSNS) o CITE (código de identificación de la Comunidad Autónoma que emite la Tarjeta Sanitaria Individual del SNS), el Código de Identificación Personal (CIP) de la Comunidad Autónoma (CIPAUT, CIPAUT alternativo), el Documento Nacional de Identidad (DNI), Número de Identificación de Extranjeros (NIE), Número de Identificación Fiscal (NIF) y pasaporte. A los efectos de la identificación unívoca se utilizará una combinación de identificadores con niveles de priorización (CIPSNS, CITE, CIPAUT, CIPAUT alternativo, DNI/NIE, pasaporte, y otros posibles identificadores disponibles como el de Salud Pública de la Comunidad Autónoma, el código de Sanidad Exterior, combinación de otros identificadores –nombre, apellidos, sexo y fecha de nacimiento-), utilizándose el CIPSNS, siempre que sea posible, como identificador principal de persona.

7. Los accesos a los que se refiere el artículo 10.1 en sus apartados a), b) y c) en ningún caso incluirán información sobre datos personales ni información que permita la reidentificación de una persona, salvo los casos contemplados en el apartado 2.d de la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre.

8. Los responsables del tratamiento a los que se refiere el apartado 2, 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 tratamiento a gran escala de datos contenidos en el SIVAIN, para garantizar el cumplimiento del Reglamento General de Protección de Datos y su adecuación al Esquema

Nacional de Seguridad.

9. Para el acceso al SIVAIN, y sin perjuicio de otras medidas que pueda acordar el responsable del tratamiento previa realización del correspondiente análisis de riesgos, deberán implantarse medidas de seguridad adecuadas, entre ellas la autenticación y el control de acceso a través de las aplicaciones habilitadas por cada comunidad autónoma, así como el establecimiento de un registro de accesos. Estas medidas garantizarán que el tratamiento se realiza conforme al principio de integridad y confidencialidad. SIVAIN únicamente conservará la información relativa a los accesos con fines de auditoría y trazabilidad.

10. Todas las personas que tengan acceso a los datos generados como consecuencia de la puesta en funcionamiento de SIVAIN están sometidas 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 solicite el acceso a los datos. En estos casos, el acceso sólo se realizará en las condiciones establecidas en el art 16.3, cuarto párrafo de la Ley 41/2002, de 14 de noviembre.

11. Los datos recogidos por SIVAIN podrán cederse a terceras partes, como instituciones académicas o centros de investigación, previa solicitud a la unidad competente en Sistemas de Información Sanitaria del Ministerio de Sanidad y en coordinación con ésta, conforme se establece en el artículo 10.2 para la realización de estudios de investigación o evaluación utilizando siempre datos anonimizados o seudonimizados, garantizando la protección de la confidencialidad y la privacidad conforme a la normativa aplicable en materia de protección de datos. La cesión deberá responder estrictamente a las finalidades previstas en este Real Decreto y se ajustará a lo dispuesto en el artículo 5 del Reglamento (UE) 2016/679, de modo que el tratamiento ulterior con fines de archivo en interés público, investigación científica o histórica, o fines estadísticos, no se considerará incompatible con la finalidad inicial, de conformidad con las garantías establecidas en el artículo 89 del RGPD y con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.

12. El intercambio de datos con otros países en amenazas transfronterizas graves para la salud se regirá por el Reglamento General de Protección de Datos y por 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 de acuerdo con lo establecido en el Reglamento sanitario internacional (2005) de la Organización Mundial de la Salud.

13. Los datos de SIVAIN se pondrán a disposición de la ciudadanía de forma abierta y reutilizable. Dicha información se facilitará siempre en formato de datos agregados o anonimizados, de modo que no sea posible la identificación de los interesados.

14. El acceso mencionado en el apartado anterior se ejercerá dentro de los límites de la normativa de transparencia y protección de datos. Los responsables del tratamiento realizarán una valoración previa para determinar qué conjuntos de datos, por su nivel de detalle o riesgo de reidentificación, no podrán ser objeto de difusión abierta, garantizando en todo caso el secreto estadístico."

Sin embargo, la transcrita regulación de la Disposición adicional primera no resulta conforme con la normativa de protección de datos, ya que no se abordan en una norma con rango de ley formal —de manera sistemática— *todos los extremos esenciales* exigidos por el marco jurídico vigente en la materia.

No obstante, según se expuso anteriormente, es importante señalar que el marco legal vigente —especialmente los artículos 41 y 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, y el artículo 16 de la Ley 41/2002, de 14 de noviembre— ya establece un núcleo de garantías legales aplicables al tratamiento de datos de salud. Estas normas regulan aspectos como:

• La delimitación legal de la finalidad del tratamiento y la sujeción a los principios de necesidad, pertinencia y proporcionalidad, de modo que solo se traten los datos adecuados y no excesivos para los fines previstos (art. 41.1 de la Ley 33/2011, de 4 de octubre).

• La determinación de los sujetos legitimados para el acceso a los datos, que comprende a los profesionales sanitarios implicados en la asistencia, así como a otros sujetos habilitados en el ejercicio de sus funciones, todos ellos sometidos al deber de secreto (art. 16.6 de la Ley 41/2002, de 14 de noviembre).

• La exigencia de medidas de seguridad y de garantías de confidencialidad en el tratamiento de la información, junto con el correlativo deber de secreto (arts. 43.2 de la Ley 33/2011, de 4 de octubre, y 16.6 de la Ley 41/2002, de 14 de noviembre).

• La previsión de mecanismos de acceso a la historia clínica que, en usos no asistenciales, tienden a la disociación de los datos identificativos respecto de los clínicos, limitando el acceso a aquellos datos que resulten adecuados a la finalidad perseguida (art. 16.3 de la Ley 41/2002, de 14 de noviembre).

Este bloque normativo, en combinación con el RGPD, constituye un marco legal de referencia que el proyecto SIVAIN debe respetar y desarrollar. **Sin embargo, como se analizará a continuación, su aplicación al sistema concreto requiere una regulación legal más específica.**

Así, aunque el texto proyectado intenta establecer un marco regulatorio para el tratamiento de datos de salud, la ausencia de una base legal con rango de ley *que abarque todos los aspectos necesarios* para la regulación de las exigencias y las garantías en materia de protección de datos, impide que la norma informada cumpla con los requisitos constitucionales y comunitarios, tal y como ha sido reiteradamente exigido por el Tribunal Constitucional y el Tribunal de Justicia de la Unión Europea.

En este sentido, el **Informe 0047/2024** ya advirtió que el tratamiento de datos personales —especialmente los relativos a la salud, calificados como categorías especiales de datos según el artículo 9 del RGPD— carecía de una base jurídica suficiente con rango de ley formal. Esta carencia persiste en la versión actual del proyecto, que sigue basándose en un Real Decreto, sin el desarrollo legal necesario para cumplir con los estándares constitucionales y comunitarios. Así, el Tribunal Constitucional, en su Sentencia 76/2019, de 22 de mayo, ha sido claro al señalar que:

> *"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."*

Asimismo, según se ha adelantado, el artículo 9.2 del RGPD establece que el tratamiento de categorías especiales de datos —como los relativos a la salud— solo puede llevarse a cabo si está expresamente autorizado por el Derecho de la Unión o de los Estados miembros, siempre que se establezcan garantías adecuadas y específicas para proteger los derechos y libertades de los interesados. La simple regulación mediante un Real Decreto, sin el respaldo de una norma con rango de ley, no satisface estos requisitos, ya que no garantiza la seguridad jurídica ni la protección efectiva de los derechos fundamentales de los ciudadanos.

En conclusión, aunque en la versión actual del proyecto se han introducido modificaciones de redacción y estructura, no se ha subsanado la carencia de una norma con rango de ley que regule de manera exhaustiva y garantista el tratamiento de datos de salud. La Disposición adicional primera, pese a su amplitud, no puede suplir la necesidad de una regulación legal que cumpla con los principios de

reserva de ley y proporcionalidad, tal como exige la jurisprudencia constitucional y comunitaria. En su virtud, la regulación contenida en esta Disposición adicional primera, aunque detallada, no es suficiente, ya que debería comprenderse en una norma con cobertura legal suficiente para garantizar su conformidad con el RGPD y la Constitución Española.

II

Por lo demás, el proyecto que se informa —SIVAIN— se enmarca en el bloque normativo básico en materia sanitaria y de salud pública, conformado por la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, la Ley 33/2011, de 4 de octubre, General de Salud Pública, y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Su objetivo es articular un sistema común que supere la fragmentación derivada de la regulación existente en las Comunidades Autónomas, la Administración General del Estado y el sector privado en materia de registro e información sobre vacunación e inmunizaciones.

En cuanto a su estructura y contenido, el proyecto regula el objeto, la finalidad, el ámbito de aplicación y los tipos de acceso a la información en materia de registro y gestión de vacunaciones e inmunizaciones, incorporando la definición de vacunas y otros medicamentos específicos sujetos a seguimiento. Asimismo, delimita las responsabilidades de las Administraciones públicas competentes, impone obligaciones al sector sanitario privado y establece el marco técnico de funcionamiento, interoperabilidad e integración de los sistemas de información.

La parte expositiva del proyecto de Real Decreto se articula en tres apartados en los que se expone el contexto normativo y sanitario que fundamenta la creación de este instrumento, su integración en el Sistema de Información en Salud Pública y las razones de interés general que lo justifican, incluyendo consideraciones expresas sobre protección de datos de carácter personal y sobre el respeto a los principios de buena regulación.

La parte dispositiva del texto proyectado se estructura en dos capítulos con un total de diez artículos. El primero, dedicado a las disposiciones generales, regula el objeto y la finalidad del sistema, el régimen de acceso a los datos, el ámbito de aplicación, la definición de los productos sujetos a registro y la distribución de responsabilidades entre Administraciones Públicas y operadores privados. El segundo capítulo aborda el funcionamiento y la gestión de la información, estableciendo las reglas de integración e interoperabilidad, el tratamiento técnico de los datos y el régimen de acceso a la información tanto para la prestación sanitaria como para otros usos

distintos del asistencial.

Finalmente, la norma incorpora cuatro disposiciones adicionales. La disposición adicional primera regula —**con las carencias de rango normativo a las que se ha hecho cumplida mención**—, el tratamiento de datos de carácter personal. La disposición adicional segunda establece la integración del Registro Nacional de Vacunaciones frente al COVID-19 (REGVACU) en el SIVAIN. La disposición adicional tercera prevé la evaluación periódica del sistema, y la disposición adicional cuarta fija el plazo de adaptación y de plena operatividad.

El proyecto incluye igualmente una disposición transitoria única sobre la remisión inicial y la incorporación de datos históricos, así como cuatro disposiciones finales relativas a modificación normativa, título competencial, habilitación de desarrollo y entrada en vigor. El texto se cierra con dos anexos que precisan, respectivamente, el contenido de la información a recoger y remitir al Ministerio de Sanidad, y la relación de vacunas y otros medicamentos específicos sometidos a registro y seguimiento.

Aunque el proyecto de Real Decreto ha introducido avances significativos en aspectos técnicos y organizativos —como la incorporación de mecanismos de seudonimización, y una delimitación más clara de los responsables del tratamiento—, persisten deficiencias estructurales que impiden considerar que se cumpla plenamente con los requisitos del RGPD y la jurisprudencia aplicable.

En concreto, las modificaciones realizadas son insuficientes para subsanar la carencia fundamental identificada en el Informe 0047/2024: la ausencia de una norma con rango de ley formal que regule de manera exhaustiva y garantista el tratamiento de datos de salud, tal como exige el artículo 6.3 del RGPD y la doctrina del TC (STC 76/2019) y del TJUE. Si bien los avances técnicos son valorables, su eficacia jurídica depende de que estén respaldados por una base legal adecuada, requisito que el proyecto actual no cumple.

III

Para determinar la condición de responsable del tratamiento de los datos de carácter personal en el marco del proyecto de Real Decreto que regula el Sistema de Información de Vacunaciones e Inmunizaciones (SIVAIN), debe atenderse a lo dispuesto en el artículo 4.7 del Reglamento General de Protección de Datos, según el cual esta condición corresponde a *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".*

Desde una perspectiva material, el proyecto normativo implica de

manera inequívoca el tratamiento de datos personales, incluyendo categorías especiales de datos conforme al artículo 9 del RGPD. Entre estos datos se encuentran información identificativa —como nombre y apellidos, el código de identificación personal del Sistema Nacional de Salud (CIPSNS), el código de identificación de la Comunidad Autónoma que emite la Tarjeta Sanitaria (CITE), el DNI, NIE, NIF o pasaporte— y datos clínicos relativos a la administración de vacunas y otros medicamentos específicos destinados a la inmunización. Estos últimos, al tratarse de datos relativos a la salud, constituyen categorías especiales de datos, cuyo tratamiento requiere la concurrencia de alguna de las circunstancias previstas en el artículo 9.2 del RGPD para levantar la prohibición general aplicable a este tipo de datos especialmente sensibles.

Sin embargo, según se viene señalando, la regulación actual carece de una norma con rango de ley formal que aborde de manera sistemática y exhaustiva los tratamientos de datos y las garantías aplicables en relación con la materia objeto de regulación, tal como exige el artículo 6.3 del RGPD y la jurisprudencia del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea. Esta carencia impide que el tratamiento de datos de salud en el SIVAIN cuente con una base jurídica suficiente que cumpla con los principios de reserva de ley y proporcionalidad, así como con las exigencias de protección de datos desde el diseño y por defecto establecidas en el artículo 25 del RGPD.

El proyecto prevé tratamientos de datos personales múltiples y estructurales, que incluyen operaciones como la recogida, registro, validación, seudonimización, almacenamiento, consulta, cruce con otras bases de datos, cesión para investigación, elaboración de estadísticas y difusión en forma agregada. Además, se contempla el tratamiento a gran escala y la interconexión con sistemas como la historia clínica digital, los sistemas de farmacovigilancia o los registros autonómicos de vacunación, así como su eventual intercambio internacional en el marco de amenazas transfronterizas graves para la salud.

En cuanto a la determinación de los responsables del tratamiento, el proyecto realiza una delimitación expresa y sistemática en la disposición adicional primera —relativa al "Tratamiento de datos de carácter personal"—, en conexión con los artículos 6 (responsabilidades de las Administraciones Públicas) y 8 (integración, interoperabilidad y tratamiento de la información). Según esta regulación, y **sin perjuicio de la necesidad de incorporar estos contenidos a una norma con rango de ley**, ostentarían la condición de responsables del tratamiento el Ministerio de Sanidad, las Comunidades Autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Defensa, cada uno en el ámbito de sus respectivas competencias en materia sanitaria. Esta atribución satisface las exigencias del artículo 4.7 del RGPD, al identificar con claridad las autoridades que determinan los fines —gestión de los programas

de vacunación, vigilancia epidemiológica, evaluación y planificación sanitaria — y los medios esenciales del tratamiento.

El proyecto configura un escenario de posible corresponsabilidad funcional, en el que cada administración mantiene la responsabilidad respecto de los datos que recopila, incorpora y remite al sistema común, determinando, en su respectivo ámbito competencial, las finalidades y condiciones del tratamiento. Al mismo tiempo, se prevé que el Ministerio de Sanidad, a través de la unidad competente en sistemas de información sanitaria, lleve a cabo operaciones técnicas de seudonimización orientadas a garantizar la interoperabilidad y la explotación analítica de los datos. En la medida en que estas operaciones puedan realizarse por cuenta de las restantes administraciones responsables, el Ministerio actuaría, en ese concreto ámbito funcional, en condición de *encargado del tratamiento*, lo que exigiría la formalización de los correspondientes instrumentos jurídicos conforme al artículo 28.3 del RGPD, tal como expresamente prevé la Disposición adicional primera.

Esta dualidad de posiciones —responsable en el ámbito propio de sus competencias sanitarias y, en su caso, encargado del tratamiento respecto de operaciones técnicas realizadas por cuenta de otros responsables— constituye un elemento especialmente relevante del modelo diseñado. El proyecto delimita con claridad estas funciones, remitiendo a los instrumentos de cooperación y coordinación del Consejo Interterritorial del Sistema Nacional de Salud para la adecuada articulación técnica y organizativa del sistema.

No obstante, la mera identificación de los responsables del tratamiento no es suficiente para garantizar la conformidad del SIVAIN con el marco jurídico aplicable. De tal modo, resulta imprescindible que los responsables y encargados de los tratamientos, las bases jurídicas, las finalidades, las categorías de datos, los destinatarios, los plazos de conservación y las garantías específicas se regulen en una norma con rango de ley, tal como exige el Tribunal Constitucional en su Sentencia 76/2019, de 22 de mayo, y el artículo 9.2 del RGPD. La ausencia de esta regulación legal compromete la seguridad jurídica y limita la eficacia de las garantías previstas para la protección de los derechos fundamentales de los interesados, por lo que se reitera la necesidad de que estas previsiones se incorporen a una norma con rango de ley formal que garantice el cumplimiento de los estándares constitucionales y comunitarios en materia de protección de datos.

IV

La normativa de protección de datos contempla diferentes supuestos que pueden dar lugar al tratamiento de datos de carácter personal. En

concreto, de acuerdo con el **artículo 6** –"Licitud del tratamiento"-, del **RGPD**, entre otros, dicho tratamiento es lícito y legítimo cuando:

> *"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
>
> *a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
>
> *b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
>
> ***c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*** (La negrita es nuestra)
>
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
>
> ***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 negrita es nuestra)
>
> *f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*
>
> *Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."*

Específicamente, *en materia sanitaria y de datos de salud,* el artículo 9 del RGPD, bajo el epígrafe *"Tratamiento de categorías especiales de datos personales"*, establece una regulación específica que incorpora una prohibición inicial de tratamiento y la remoción de esta de acuerdo con determinados requisitos y condiciones:

> *"Artículo 9 Tratamiento de categorías especiales de datos personales*
>
> *1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,* ***datos relativos a la salud*** *o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. (la negrita es nuestra)*

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

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;* (la negrita es nuestra)

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, (…)* (la negrita es nuestra)

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

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

De nuevo en este punto, conviene traer a colación que, en el Informe 0047/2024, esta Agencia concluyó que el tratamiento de datos personales, especialmente los relativos a la salud, calificados como categorías especiales de datos según el artículo 9 del RGPD, carecía de una base jurídica suficiente con rango de ley formal. Esta carencia persiste en la versión actual del proyecto, que sigue basándose en un Real Decreto, sin el desarrollo legal necesario para cumplir con los estándares constitucionales y comunitarios (por todas la STC 76/2019, de 22 de mayo).

Asimismo, el artículo 9.2 del RGPD establece que el tratamiento de categorías especiales de datos —como los relativos a la salud— solo puede llevarse a cabo si está expresamente autorizado por el Derecho de la Unión o

de los Estados miembros, siempre que se establezcan garantías adecuadas y específicas para proteger los derechos y libertades de los interesados.

En la versión actual del proyecto, aunque se han introducido modificaciones de redacción y estructura, no se ha subsanado la carencia de una norma con rango de ley que regule de manera exhaustiva y garantista el tratamiento de datos de salud. En relación con el objeto y la finalidad del SIVAIN, la versión de 2024 hacía referencia explícita a la tutela de la salud de la población como objetivo principal del sistema. Sin embargo, en la versión actual, se redefine la finalidad como la disponibilidad de datos sobre vacunas y fármacos específicos, eliminando la referencia directa a la tutela de la salud.

Aunque se mantienen fines específicos como la trazabilidad, la accesibilidad a la información y la farmacovigilancia, no se justifica de manera suficiente la necesidad de tratar datos identificativos de los pacientes para cumplir con dichos fines, lo que plantea dudas sobre el cumplimiento del principio de minimización de datos establecido en el artículo 5.1.c) del RGPD, máxime teniendo en consideración el carácter meramente reglamentario de la norma que se informa.

Por otro lado, el ámbito de aplicación del *nuevo* proyecto se ha ampliado para incluir explícitamente a personas físicas o jurídicas del sector privado, lo que conlleva una mayor recolección de datos. No obstante, no se establecen garantías adicionales que aseguren que estos tratamientos cumplan con los principios de minimización de datos y protección desde el diseño y por defecto, conforme al artículo 25 del RGPD. Esta omisión resulta especialmente relevante, dado que la inclusión del sector privado en el ámbito de aplicación del SIVAIN incrementa el riesgo de tratamientos no controlados y potencialmente lesivos para los derechos de los interesados.

En cuanto a las bases de legitimación que se analizan en este Punto, la versión de 2024 citaba múltiples leyes —como la Ley 14/1986, la Ley 41/2002, la Ley 16/2003 y la Ley 33/2011— como fundamento jurídico para el tratamiento de datos. En la versión actual, sin embargo, se simplifica la referencia a las bases jurídicas, limitándose a citar el artículo 6.1.c) y e) del RGPD y el artículo 9.2.h) e i) del RGPD. Aunque esta referencia es técnicamente correcta, **no se subsana la falta de una norma con rango de ley que regule específicamente el tratamiento de datos de salud en el SIVAIN**. La mera remisión a los preceptos del RGPD, sin un desarrollo normativo interno que concrete las garantías y condiciones aplicables, resulta insuficiente para cumplir con el principio de reserva de ley formal y con el principio de proporcionalidad.

Aunque el proyecto cita correctamente las bases jurídicas del RGPD, **falta una norma con rango de ley que desarrolle las garantías específicas** para el tratamiento de datos de salud en el SIVAIN. Las leyes

actuales, como la Ley 33/2011, de 4 de octubre, y la Ley 41/2002, de 14 de noviembre, establecen garantías generales, pero no regulan aspectos concretos del SIVAIN, como el uso de algoritmos de seudonimización o la reutilización de datos.

En consecuencia, las modificaciones introducidas en la versión actual del proyecto no parecen suficientes para subsanar las deficiencias señaladas en el Informe 0047/2024, especialmente en lo que respecta a la necesidad de una norma con rango de ley formal que regule el tratamiento de datos de salud en el SIVAIN. Esta Agencia reitera, por tanto, la necesidad de que se proceda a la modificación de la Ley 33/2011, de 4 de octubre, General de Salud Pública, o a la aprobación de una norma con rango de ley que incorpore las garantías y condiciones necesarias para cumplir con los estándares constitucionales y comunitarios en materia de protección de datos.

En consecuencia, se reitera la necesidad de que las previsiones relativas al tratamiento de datos de salud —actualmente contenidas en el proyecto de Real Decreto— se regulen mediante una norma con rango de ley formal. Solo así concurrirían las circunstancias exigidas por el artículo 9.2, letras h) e i) del RGPD, que permiten levantar la prohibición inicial aplicable al tratamiento de categorías especiales de datos, como son los relativos a la salud. En este caso, la base legal legitimadora de los tratamientos llevados a cabo por el SIVAIN debería fundamentarse en los artículos 6.1.c), d) y e) del RGPD, siempre que dichas previsiones estén respaldadas por una norma con rango de ley que desarrolle de manera exhaustiva las garantías, condiciones y límites aplicables.

A mayor abundamiento, la finalidad del SIVAIN —orientada a la prevención y control de enfermedades inmunoprevenibles en el marco de las actuaciones de salud pública— no encuentra cobertura suficiente en una norma reglamentaria, como es el caso del proyecto de Real Decreto. No resulta aplicable, a estos efectos, la habilitación legal genérica contenida en el artículo 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, en su actual redacción, pues no cumple con los requisitos de precisión y determinación exigidos por el Tribunal Constitucional y el RGPD para el tratamiento de datos de salud. **Por ello, se insiste en la necesidad de que estas previsiones se incorporen a una ley formal, única vía para garantizar el pleno respeto a los derechos fundamentales de los interesados y el cumplimiento de los principios de reserva de ley y proporcionalidad.**

V

Tal y como se señalaba en el Punto I de nuestro **Informe 0047/2024,** de 24 de octubre de 2024, y ahora se reitera:

"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 contraríe 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 licito 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."*

En consecuencia, no resulta suficiente que, para el establecimiento de las garantías adecuadas y específicas que exige el tratamiento de datos de salud, la norma se limite a remitirse de manera genérica al RGPD o a la LOPDGDD. El Tribunal Constitucional, en su jurisprudencia, ha subrayado de manera reiterada que la previsión de tales garantías debe formar parte de la propia regulación legal que habilita el tratamiento, ya sea mediante su incorporación directa en la norma o a través de una remisión expresa a otras disposiciones con rango suficiente, de modo que quede plenamente preservada la reserva de ley exigida por el artículo 53.1 de la Constitución Española. Estas exigencias constitucionales se encuentran en plena consonancia con lo previsto en el artículo 8 de la LOPDGDD, que establece que el tratamiento de datos personales basado en el cumplimiento de una obligación legal o en el ejercicio de poderes públicos requiere que dicha base jurídica se encuentre establecida en una norma con rango de ley.

Esto es, la habilitación para el tratamiento de datos personales por las Administraciones públicas, y particularmente cuando se trate de datos relativos a la salud —considerados como categorías especiales de datos según el artículo 9 del RGPD—, debe apoyarse necesariamente en normas legales que definan el interés público perseguido, delimiten el alcance del tratamiento y establezcan las garantías necesarias para la protección de los derechos de los interesados.

La Disposición adicional primera del proyecto normativo, en su apartado 4, segundo párrafo, contiene una referencia expresa a las normas legales que amparan el tratamiento de los datos de salud en el ámbito de los programas de vacunación. **Sin embargo, esta previsión no puede reputarse suficiente en orden a los objetivos pretendidos de regulación legal del sistema SIVAIN, pues se limita a una mera remisión genérica sin desarrollar las garantías específicas que exige el marco jurídico aplicable.**

Así, entre otros aspectos que requieren regulación legal específica, se evidencia que el proyecto adolece de una regulación legal mínima para aspectos clave del SIVAIN, que por su novedad y complejidad exigen un desarrollo normativo con rango de ley, tales como:

- La delimitación legal de las categorías de datos tratados: el Anexo I del proyecto enumera los datos a recoger, pero falta una norma legal que defina con precisión qué categorías son estrictamente necesarias para cada finalidad (ej.: ¿son imprescindibles el DNI o el pasaporte para la seudonimización?).

- El uso de algoritmos de seudonimización e identificadores personales: el proyecto regula técnicamente el algoritmo (art. 6.5 y Disposición adicional primera), pero carece de base legal que garantice su proporcionalidad y limite los riesgos de reidentificación. (por ejemplo: ¿Qué ley autoriza el uso del CIPSNS como identificador principal?).

- La reutilización, cesión y usos ulteriores de datos: las leyes actuales (arts. 41 y 43 Ley 33/2011, de 4 de octubre) son insuficientes para regular operaciones como:

    - La cesión a terceros (investigadores, organismos internacionales) incluso con datos seudonimizados.

    - La reutilización con fines estadísticos o de I+D, que requiere garantías adicionales según el art. 89 RGPD.

    - Los intercambios internacionales en casos de amenazas transfronterizas (Reglamento UE 2022/2371, de 23 de noviembre de 2022).

La ausencia de regulación legal sobre estos aspectos impide considerar suficiente la remisión genérica al RGPD o a las leyes sectoriales, tal como exigen el Tribunal Constitucional (STC 76/2019) y el TJUE (STJUE 6/10/2020, C-623/17).

En este contexto, resulta relevante destacar que**, en el marco del actual procedimiento legislativo, se encuentra en tramitación la Proposición de Ley sobre el programa de cribado neonatal del Sistema Nacional de Salud (122/000233), presentada el 6 de noviembre de 2025.**

En el debate parlamentario de esta proposición de ley, se han presentado enmiendas que van en la línea de incorporar una regulación con rango de ley formal para el tratamiento de datos de salud, en cumplimiento de las exigencias derivadas de la doctrina del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea. Esta circunstancia confirma el criterio seguido en nuestro Informe 0047/2024, al poner de manifiesto la necesidad de que las garantías y condiciones para el tratamiento de datos sensibles sean establecidas por una norma con rango de ley, y no por vía reglamentaria, tal como exige el artículo 6.3 del RGPD y la jurisprudencia constitucional.

La existencia de estas enmiendas en materia de salud y protección de datos refuerza la conclusión de que el proyecto de Real Decreto que se informa, al carecer de una base legal suficiente con rango de ley formal, no cumple con los requisitos constitucionales y comunitarios aplicables al tratamiento de datos de salud. En consecuencia, se reitera la necesidad de que se proceda a la modificación de la Ley 33/2011, de 4 de octubre, General de Salud Pública, o a la aprobación de una norma con rango de ley que incorpore las garantías y condiciones necesarias para asegurar el cumplimiento de los estándares en materia de protección de datos personales.

VI

El proyecto de Real Decreto que regula el Sistema de Información de Vacunaciones e Inmunizaciones incluye en su Memoria del Análisis de Impacto Normativo (MAIN) un análisis específico del impacto en materia de protección de datos personales, incorporando una Evaluación de Impacto en Protección de Datos (EIPD). Este análisis pone de manifiesto que, atendiendo a la naturaleza, alcance y finalidades de los tratamientos previstos en el sistema, se ha considerado expresamente la incidencia de la norma sobre la protección de datos personales. En la MAIN se concluye que, mediante la adopción de las salvaguardas adecuadas, los tratamientos derivados de la aplicación del Real Decreto podrían desarrollarse de conformidad con las exigencias del ordenamiento jurídico vigente.

En este sentido, la MAIN dedica un epígrafe específico dentro de su apartado VI, relativo al análisis de impactos, a la evaluación de impacto en materia de protección de datos de carácter personal. En él se describen las

finalidades del tratamiento de los datos de salud en el marco del SIVAIN, destacando que su objetivo es permitir el análisis de información necesaria para la evaluación de los programas de vacunación, su monitorización y eventual ajuste, así como la realización de estudios con fines de investigación o evaluación en salud pública.

Asimismo, se señala que el sistema facilitará el cumplimiento de requerimientos de información de organismos nacionales e internacionales, la realización de evaluaciones en materia de farmacovigilancia relativas a la seguridad y calidad de las vacunas, el análisis con fines estadísticos o de georreferenciación, y la consulta por la ciudadanía de sus propios datos de vacunación, incluyendo la emisión de certificados de vacunación a nivel nacional o internacional. También se prevé el acceso de los profesionales sanitarios a la información contenida en el SIVAIN en el marco de la prestación de asistencia sanitaria, así como la posibilidad de actuar de forma eficaz por razones epidemiológicas o de protección de la salud pública ante riesgos o peligros graves.

La MAIN destaca, además, que, para garantizar el cumplimiento de la normativa de protección de datos, el sistema se basa, con carácter general, en el tratamiento de datos personales de salud seudonimizados. A tal fin, se prevé que la unidad receptora de la información aplique un algoritmo común de seudonimización a los datos identificativos de las personas, garantizando así la interoperabilidad con otras bases de datos del Ministerio de Sanidad y, en su caso, de otras administraciones sanitarias. Esto permitiría la realización de análisis avanzados de datos, estableciéndose una separación técnico-funcional entre la unidad receptora de los datos y la unidad gestora del sistema, en línea con el principio de protección de datos desde el diseño y por defecto (artículo 25 del RGPD).

Asimismo, la MAIN subraya que la Disposición adicional primera del proyecto de Real Decreto regula de manera detallada los aspectos relativos a la protección de datos personales, incluyendo la previsión de que los responsables del tratamiento realicen, con carácter previo al inicio de las operaciones de tratamiento, una evaluación de impacto relativa a la protección de datos, en cumplimiento del artículo 35 del RGPD. Esta previsión resulta especialmente relevante, dado que en el supuesto examinado concurren varios de los supuestos que determinan la obligatoriedad de dicha evaluación, como son el tratamiento a gran escala de datos relativos a la salud, la interconexión sistemática de bases de datos y la evaluación sistemática de información relacionada con la salud de la población.

No obstante, a pesar de que la inclusión de la EIPD en la MAIN y en el articulado del proyecto representa un avance significativo, **no resulta suficiente que esta evaluación se incorpore únicamente a un texto reglamentario, como es el caso del Real Decreto que se informa. La**

evaluación de impacto en protección de datos, dada su relevancia y las garantías que debe asegurar, debería incorporarse a una norma con rango de ley formal, y no limitarse a una regulación de carácter reglamentario.

En este sentido, aunque el proyecto ha tenido en cuenta las consideraciones emitidas en informes anteriores de esta Agencia —como los Informes 15/2022, de 15 de febrero de 2022, y 14/2023, de 8 de febrero de 2023—, en los que se recomendaba la realización e incorporación a la MAIN del análisis de riesgos (artículo 24 del RGPD) y la evaluación de impacto relativa a la protección de datos (artículo 35 del RGPD), la mera inclusión de estas evaluaciones en un Real Decreto no satisface plenamente las exigencias constitucionales y comunitarias. La reserva de ley exigida por el artículo 53.1 de la Constitución Española y el artículo 9.2 del RGPD requiere que las garantías y condiciones para el tratamiento de categorías especiales de datos, como los relativos a la salud, se establezcan en una norma con rango de ley, que defina de manera precisa los supuestos, condiciones y salvaguardas aplicables.

En consecuencia, a pesar de los avances introducidos en la MAIN y en el articulado del proyecto, se informa desfavorablemente la suficiencia de la regulación de la EIPD en un texto reglamentario, reiterándose la necesidad de que esta evaluación, junto con las garantías y condiciones para el tratamiento de datos de salud, se incorporen a una norma con rango de ley formal. Solo de este modo se garantizará el pleno cumplimiento de los principios de reserva de ley, proporcionalidad y protección de datos desde el diseño y por defecto, en línea con las exigencias del Tribunal Constitucional, el Tribunal de Justicia de la Unión Europea y el RGPD.

VII

A la vista del análisis realizado, **se informa desfavorablemente** el proyecto normativo sometido a informe, y en particular su Disposición adicional primera (relativa al "Tratamiento de datos de carácter personal"), pues su regulación no cumple con los requisitos constitucionales y comunitarios aplicables al tratamiento de datos de salud. Aunque el texto analizado incorpora una serie de previsiones en materia de protección de datos —como la determinación de los responsables del tratamiento, el régimen de encargos, las bases jurídicas de licitud, la regulación del tratamiento de categorías especiales de datos, la seudonimización de la información, las condiciones de acceso a los datos, las medidas de seguridad, la evaluación de impacto y la disciplina de las cesiones y reutilización de información—, todas estas garantías resultan insuficientes al no estar respaldadas por una norma con cobertura legal suficiente.

En efecto, si bien el proyecto explicita el sometimiento de los tratamientos al RGPD y a la LOPDGDD, ninguna de sus previsiones en materia de protección de datos puede considerarse válida ni suficiente al no estar contenidas en una norma con rango de ley. El artículo 6.3 del RGPD y la jurisprudencia del Tribunal Constitucional (en particular, la Sentencia 76/2019, de 22 de mayo) exigen que los tratamientos de datos de salud, por su especial sensibilidad, deban estar regulados mediante una ley formal que defina de manera exhaustiva las garantías, condiciones y límites aplicables.

Aunque el proyecto configura un sistema aparentemente sólido desde una perspectiva técnica, con una base jurídica aparente en los artículos 6.1.c) y e) y 9.2.h) e i) del RGPD, y con un esquema de responsabilidades, seudonimización, controles de acceso y evaluación de impacto, la ausencia de una norma con rango de ley formal invalida su conformidad con el ordenamiento jurídico. La legitimación del tratamiento no puede fundamentarse exclusivamente en una remisión genérica al RGPD y a la LOPDGDD, sino que requiere un desarrollo legal específico que concrete las condiciones, finalidades, plazos de conservación, destinatarios y garantías aplicables al tratamiento de datos de salud en el SIVAIN.

Asimismo, aunque el proyecto pretende cumplir con las disposiciones sobre seguridad y confidencialidad previstas en el artículo 32 del RGPD y en el artículo 28 de la LOPDGDD, la mera previsión de medidas de seguridad en una norma reglamentaria no satisface el principio de reserva de ley exigido por la Constitución Española y el Tribunal Constitucional. Las medidas técnicas y organizativas, los controles de acceso, los mecanismos de trazabilidad y el deber de secreto deben estar regulados en una norma con rango de ley que garantice su obligatoriedad, eficacia y vinculatoriedad para todas las administraciones y operadores involucrados.

En conclusión, este informe reconoce **el esfuerzo realizado** por el redactor de la norma para articular un sistema integrado de gestión de datos de vacunación. Así, el proyecto SIVAIN incorpora una regulación detallada de garantías ya previstas en la Ley 33/2011, de 4 de octubre, y en la Ley 41/2002, de 14 de noviembre, como el principio de minimización o el secreto profesional. Este desarrollo normativo **supone un avance significativo** en la construcción de un criterio uniforme en materia de salud pública. A su vez, se valora positivamente la incorporación de garantías técnicas y organizativas, como la seudonimización, la EIPD y la delimitación de responsables del tratamiento.

Sin embargo, a pesar de los avances, **el proyecto no cumple con los requisitos constitucionales y comunitarios** aplicables al tratamiento de datos de salud. En concreto:

- La Disposición adicional primera, aunque detallada, no puede suplir la ausencia de una norma con rango de ley que regule las garantías para el tratamiento de categorías especiales de datos.

- Las bases jurídicas invocadas requieren la existencia de un desarrollo legal específico que concrete los límites, plazos y condiciones del tratamiento.

- La EIPD debe incorporarse a una ley formal para garantizar su eficacia.

Por todo lo expuesto, esta Agencia considera que el proyecto de Real Decreto no cumple con los requisitos constitucionales y comunitarios aplicables al tratamiento de datos de salud, reiterándose la necesidad de que las previsiones en materia de protección de datos se incorporen a una norma con rango de ley formal que garantice el pleno respeto de los derechos fundamentales de los interesados.

Solo mediante una modificación de la Ley 33/2011, de 4 de octubre, General de Salud Pública —o la aprobación de una norma *ad hoc* con rango de ley— podrían cumplirse los estándares exigidos por el ordenamiento jurídico. Hasta entonces, el proyecto no ofrece las garantías suficientes para el tratamiento de datos de salud en el SIVAIN, por lo que se mantiene el criterio desfavorable ya expresado en nuestro Informe 0047/2024.