

INFORME

CÁMARA DE COMERCIO DE ESPAÑA

Registro del Pasaporte Digital de Producto

Mayo de 2026

1 | INTRODUCCIÓN

La Comisión Europea ha iniciado el proceso de adopción del Reglamento de Ejecución por el que se establecen las disposiciones para el funcionamiento del registro del Pasaporte Digital de Producto, en desarrollo del Reglamento (UE) 2024/1781 relativo al diseño ecológico de productos sostenibles.

En este escenario, el desarrollo del Pasaporte Digital de Producto constituye una de las herramientas clave para avanzar hacia un modelo productivo más transparente, trazable y circular, así como para mejorar el acceso a la información a lo largo de la cadena de valor. Al mismo tiempo, su correcta implementación plantea desafíos relevantes desde el punto de vista técnico, operativo y organizativo, especialmente en un entorno caracterizado por la diversidad de sectores y por la heterogeneidad del tejido empresarial europeo.

La Cámara de Comercio de España valora positivamente esta iniciativa, en la medida en que un sistema adecuado puede contribuir a mejorar la seguridad jurídica y facilitar la adopción del Pasaporte Digital de Producto por parte de las empresas.

En este sentido, se trasladan a continuación una serie de consideraciones y observaciones orientadas a favorecer una implementación proporcionada, técnicamente viable y alineada con la realidad operativa del tejido empresarial.

2 | VALORACIÓN GLOBAL

La Cámara de Comercio de España acoge favorablemente el proyecto de Reglamento de Ejecución y reconoce que la creación de un registro común a escala europea constituye una pieza necesaria para hacer operativo el pasaporte digital de producto y supone un avance relevante en la modernización del marco regulatorio aplicable a los productos en el mercado interior. La existencia de una infraestructura común, gobernada por la Comisión y compatible con la diversidad de actores y sectores, resulta clave para garantizar la coherencia y eficacia del sistema.

No obstante, la viabilidad y el éxito del sistema dependerán de que su diseño final dé respuesta adecuada a varios retos transversales:

- La proporcionalidad de las cargas, especialmente para las pequeñas y medianas empresas, que en muchos casos no disponen de los recursos necesarios para afrontar procesos complejos de verificación o integración.
- La neutralidad tecnológica, evitando que se penalicen inversiones ya realizadas en soluciones interoperables.
- La claridad y transparencia en la asignación de responsabilidades a lo largo de la cadena de valor, particularmente en entornos con múltiples actores.
- La protección de la información empresarial sensible, incluidos secretos comerciales y conocimiento industrial.
- La flexibilidad operativa en el proceso de registro, que permita una implantación progresiva adaptada a la diversidad de sectores.

Esta iniciativa debería ser coherente con la agenda europea de simplificación regulatoria y con el objetivo de reducir las cargas administrativas de las empresas, especialmente de las pymes. El registro del Pasaporte Digital de Producto no debería convertirse en una capa adicional de obligaciones duplicadas, sino en una infraestructura facilitadora que simplifique trámites, refuerce la vigilancia de mercado y mejore la circularidad sin menoscabar la competitividad empresarial. La prioridad debe ser asegurar interoperabilidad, fiabilidad, seguridad jurídica y cargas proporcionadas.

Sobre esta base, la Cámara de España formula a continuación una serie de observaciones transversales y específicas en relación con los aspectos del proyecto que se consideran más relevantes.

3 | OBSERVACIONES TRANSVERSALES

3.1. Proporcionalidad y enfoque basado en riesgo

Las pymes constituyen una parte relevante del tejido empresarial y de las cadenas de suministro europeas, por lo que su participación será determinante para el éxito del Pasaporte Digital de Producto. En este contexto, resulta importante que el Reglamento incorpore mecanismos que faciliten su incorporación, evitando que las exigencias técnicas, organizativas o económicas se conviertan en un obstáculo de entrada.

En este sentido, la proporcionalidad constituye un elemento esencial para la correcta implantación del sistema, especialmente en un entorno caracterizado por la diversidad de operadores, sectores y niveles de madurez digital. Por ello, resulta importante que los requisitos previstos en el Reglamento se apliquen de forma ajustada a la función de cada operador, a la criticidad de las operaciones realizadas y a la capacidad efectiva de cumplimiento de las empresas.

Un enfoque excesivamente uniforme podría generar cargas desproporcionadas, particularmente para pequeñas y medianas empresas o para aquellos actores cuya intervención en el sistema sea más limitada.

Por todo ello, podría valorarse una aplicación proporcionada de determinadas exigencias técnicas y operativas, de manera que el sistema preserve sus objetivos regulatorios sin introducir barreras onerosas o innecesarias.

En particular, la implantación debería apoyarse en un enfoque escalonado: una primera fase centrada en identificadores, datos esenciales, interoperabilidad aduanera, acceso público a información no sensible y funcionamiento básico del registro; y fases posteriores para las funcionalidades más complejas de gestión de identidades, accesos diferenciados, datos restringidos y actualización dinámica de información.

En esta línea, podría también explorarse el desarrollo de vías simplificadas de acceso y cumplimiento, así como complementar el marco regulatorio con medidas de acompañamiento, formación y apoyo práctico.

Asimismo, se considera relevante prever periodos transitorios suficientes que permitan una adaptación gradual por parte de las empresas.

3.2. Neutralidad tecnológica e interoperabilidad

Las empresas subrayan la importancia de preservar un enfoque tecnológicamente neutral, que permita la coexistencia de distintas soluciones e infraestructuras siempre que cumplan los requisitos del sistema en términos de seguridad, trazabilidad y verificabilidad. En este sentido, resulta importante evitar que la configuración del registro

genere dependencias de arquitecturas únicas o desincentive el uso de soluciones interoperables ya implantadas.

Asimismo, es importante garantizar una interoperabilidad real con los sistemas empresariales existentes, incluidos los de gestión de producto y cadena de suministro. Una integración excesivamente compleja o costosa podría ralentizar la adopción y generar duplicidades innecesarias, especialmente en organizaciones con menor madurez digital.

Para facilitar esta interoperabilidad, las especificaciones técnicas, las interfaces de programación de aplicaciones (API), los esquemas de datos y los vocabularios controlados deberían publicarse con antelación suficiente, versionado estable y entornos de prueba. También convendría prever mecanismos de compatibilidad con estándares ampliamente implantados en la industria y con soluciones que ya garanticen trazabilidad, disponibilidad e intercambio seguro de información.

3.3. Protección de la información empresarial sensible

La necesidad de compatibilizar los objetivos de transparencia y trazabilidad con la protección de la información empresarial sensible resulta especialmente relevante. En numerosos sectores, la información incorporada al Pasaporte Digital de Producto puede incluir configuraciones de producto, relaciones de suministro, composiciones o procesos productivos cuya exposición indebida podría afectar a la competitividad de las empresas.

En este contexto, cabría reforzar los mecanismos de control de acceso basados en roles, legitimidad de uso y proporcionalidad, de modo que el acceso a la información responda a una necesidad justificada y se adapte a la posición del actor que la consulta.

El principio de acceso en función de la necesidad de conocer debería incorporarse de forma operativa, diferenciando con claridad la información accesible al consumidor, a operadores de la cadena, a autoridades de vigilancia de mercado y a autoridades aduaneras. Además, debería quedar expresamente protegido el uso de datos que puedan revelar secretos comerciales, propiedad industrial, estrategias de aprovisionamiento o configuraciones técnicas críticas, salvo en los casos estrictamente necesarios y con garantías reforzadas.

3.4. Copia de respaldo: proporcionalidad y alternativas

Los operadores económicos que ya crean, gestionan y alojan sus Pasaportes Digitales de Productos generalmente están obligados a garantizar el cumplimiento de los requisitos existentes en materia de accesibilidad, persistencia, gobernanza e interoperabilidad de la información que gestionan. En muchos casos, las empresas ya operan infraestructuras internas seguras capaces de preservar registros digitales

conforme a las normas de ciberseguridad y protección de datos de la UE. En este contexto, la obligación sistemática de mantener una copia de respaldo adicional a través de proveedores independientes externos puede generar una duplicación de infraestructuras y obligaciones existentes, al tiempo que introduce una mayor complejidad operativa y costes financieros adicionales relacionados con el almacenamiento, la ciberseguridad, el mantenimiento y la integración de sistemas, sin aportar necesariamente beneficios adicionales proporcionales en la práctica.

A la luz del objetivo más amplio de reducir cargas administrativas innecesarias y simplificar las obligaciones y costes de cumplimiento, especialmente para las pymes, debería reconsiderarse por tanto la exigencia general de proporcionar de forma sistemática una copia de respaldo alojada por un tercero. Los operadores económicos responsables de crear y mantener los Pasaportes Digitales de Producto deberían disponer de suficiente flexibilidad para garantizar la continuidad, fiabilidad y persistencia de la información a través de sus infraestructuras principales cuando estas ya cumplan los requisitos pertinentes. Como alternativa, podría contemplarse la adopción de enfoques más proporcionados centrados en garantizar la preservación de los datos del Pasaporte Digital de Producto en sí, sin exigir sistemáticamente infraestructuras de alojamiento separadas de alta disponibilidad ni sistemas de copia de respaldo duplicados gestionados por terceros.

La exigencia de continuidad no debería confundirse con una obligación única de externalización. La solución regulatoria más equilibrada sería permitir al operador acreditar, mediante criterios verificables, que su infraestructura propia o la de un proveedor de confianza ofrece niveles equivalentes de disponibilidad, integridad, reversibilidad y continuidad, incluyendo planes de salida, portabilidad de datos y transferencia ordenada en caso de cese de actividad.

4 | OBSERVACIONES ESPECÍFICAS

4.1. Estructura del registro y neutralidad tecnológica (artículo 3)

Se valora positivamente la arquitectura federada del registro como base para un sistema escalable y adaptable. No obstante, resulta importante reforzar el principio de neutralidad tecnológica, evitando que la infraestructura común limite en la práctica el uso de soluciones interoperables ya existentes.

Asimismo, es importante que las interfaces de conexión del sistema se diseñen con criterios de integración progresiva, facilitando su conexión con sistemas empresariales y reduciendo los costes de adaptación. Se recomienda introducir un enfoque de registro mínimo viable, que permita la activación del pasaporte con un conjunto esencial de datos, habilitando una posterior cumplimentación progresiva. Este enfoque favorecería una implantación más realista, especialmente en cadenas de suministro complejas.

Por otra parte, se considera necesario desarrollar con mayor precisión la figura de los proveedores de servicios de pasaporte digital de producto en lo relativo a criterios de certificación, requisitos operativos y mecanismos de supervisión.

En relación con los proveedores de servicios, sería conveniente que el Reglamento o sus guías de aplicación concretaran requisitos mínimos de solvencia técnica, ciberseguridad, portabilidad, reversibilidad, acuerdos de nivel de servicio y tratamiento de incidentes. Esta clarificación reduciría riesgos de dependencia tecnológica y favorecería un mercado competitivo de soluciones.

4.2. Requisitos de verificación y proporcionalidad (artículos 4 y 5)

La Cámara de España comparte el objetivo de garantizar la autenticidad y fiabilidad de los actores que interactúan con el sistema. No obstante, determinados mecanismos avanzados de identificación electrónica pueden resultar complejos o costosos para operadores con menor madurez digital, especialmente pymes y microempresas.

En este sentido, podría valorarse la introducción de soluciones equivalentes en términos de seguridad jurídica, pero más accesibles desde el punto de vista operativo, así como mecanismos de autenticación progresiva que ajusten el nivel de exigencia al perfil del operador y a la criticidad de las operaciones.

Asimismo, podría explorarse la adopción de fórmulas simplificadas durante las primeras fases de implantación, con el fin de evitar que el cumplimiento del pasaporte digital de producto resulte inasumible en etapas iniciales para determinados operadores.

Asimismo, el sistema debería apoyarse, cuando sea posible, en mecanismos de identificación digital ya existentes para empresas, evitando dobles verificaciones y

reconociendo vías equivalentes en otros sistemas europeos. En la práctica, la verificación debe ser rigurosa, pero también sencilla, documentada y accesible para microempresas, pymes, importadores y representantes autorizados.

4.3. Gestión de usuarios y delegación técnica (artículo 6)

Se considera relevante reforzar el marco de gestión de usuarios, teniendo en cuenta que muchas empresas no dispondrán de capacidad interna suficiente para gestionar directamente el sistema.

En este sentido, podría reconocerse de forma más explícita la posibilidad de delegación técnica en terceros, estableciendo garantías en términos de trazabilidad de las acciones, identificación de los actores implicados y mecanismos de supervisión.

Este enfoque permitiría facilitar la incorporación al sistema sin generar dependencias informales o inseguridad operativa.

La delegación técnica no debe diluir la responsabilidad del operador económico, pero sí puede ser imprescindible para que pymes y empresas sin capacidades digitales internas puedan cumplir. Por ello, el registro debería permitir perfiles de usuario diferenciados, autorizaciones limitadas, trazabilidad de actuaciones y revocación sencilla de poderes.

4.4. Registro del pasaporte y flexibilidad operativa (artículo 8)

Una exigencia de completitud semántica plena desde el inicio podría dificultar la puesta en marcha del sistema, especialmente en cadenas de suministro complejas. En este contexto, podría contemplarse un registro inicial basado en requisitos esenciales, permitiendo completar progresivamente la información.

Asimismo, resulta relevante mantener flexibilidad en el nivel de granularidad, de manera que pueda adaptarse a las características de cada sector. En algunos casos, el nivel de modelo puede ser suficiente, mientras que en otros, como determinados materiales reciclados, la trazabilidad por lote puede resultar más adecuada.

Por otra parte, en relación con la verificación automatizada prevista en el artículo 8, resulta importante delimitar su alcance, de modo que se limite a los elementos previstos en el proyecto, evitando su evolución hacia mecanismos más amplios de control o supervisión.

4.5. Prueba de registro, persistencia, soluciones escalables (artículo 9)

Los mecanismos de prueba de registro deberían poder adaptarse a entornos de alto volumen y permitir soluciones escalables desde el punto de vista operativo, especialmente en sectores con elevados volúmenes de producción o transacciones.

Asimismo, resulta importante garantizar la persistencia del identificador del producto y la continuidad del acceso al pasaporte digital de producto a lo largo de su ciclo de vida, evitando riesgos derivados de cambios en proveedores tecnológicos o sistemas de gestión.

4.6. Gestión de los datos de registro y conservación de la información (artículo 10)

En relación con los periodos de conservación, un plazo horizontal uniforme puede no reflejar adecuadamente la diversidad de situaciones entre sectores y categorías de producto. Se recuerda, además, que el pasaporte digital de producto no implica únicamente la conservación pasiva de documentación, sino también el mantenimiento activo de infraestructuras digitales, bases de datos, APIs, mecanismos de interoperabilidad y sistemas de ciberseguridad durante periodos prolongados, con los costes operativos y de mantenimiento asociados.

En este contexto, podría valorarse un enfoque más flexible, que tenga en cuenta la naturaleza del producto, su ciclo de vida y la relevancia operativa de la información almacenada. Una modulación sectorial de estos periodos podría contribuir a una aplicación más proporcionada y adaptada a la realidad de los distintos operadores.

En este mismo contexto, convendría evitar requisitos que impliquen duplicidades de infraestructuras o la dependencia obligatoria de terceros cuando los operadores ya dispongan de sistemas que cumplan las condiciones exigidas en términos de accesibilidad, persistencia y fiabilidad de la información.

4.7. Modelos de datos, repositorio semántico y gobernanza del dato (artículos 11 y 12)

Se valora positivamente el desarrollo de un repositorio semántico común como herramienta para reforzar la interoperabilidad del sistema. No obstante, resulta importante evitar modelos de datos excesivamente rígidos, que puedan dificultar su aplicación en sectores con realidades diversas.

En este sentido, podría adoptarse un enfoque basado en un núcleo común de datos armonizados, complementado con desarrollos sectoriales que permitan adaptar el sistema a las particularidades de cada industria. Asimismo, la estandarización de

formatos de información contribuiría a evitar requerimientos heterogéneos por parte de distintos actores a lo largo de la cadena de valor.

Asimismo, en aquellos casos en que la naturaleza del material lo requiera, el modelo de datos debería permitir reflejar rangos razonables o composiciones variables, siempre que ello responda a la realidad del producto y pueda documentarse de forma adecuada.

Resulta también relevante reforzar la gobernanza del dato, aclarando la generación, validación y actualización de la información, así como la asignación de responsabilidades cuando el producto cambia de estado u operador. En este contexto, se valora positivamente la posibilidad de contemplar mecanismos que permitan reflejar la evolución del producto a lo largo de su ciclo de vida.

4.8. Soporte técnico, acompañamiento y capacitación (artículo 13)

El soporte técnico debería extenderse más allá de una función reactiva, teniendo en cuenta que la implantación del pasaporte digital de producto implica también una adaptación organizativa en las empresas.

En este sentido, podría contemplarse la incorporación de herramientas de evaluación del nivel de preparación, programas de formación y entornos de prueba que faciliten la implementación, especialmente en el caso de las pymes.

El apoyo práctico debería incluir manuales sectoriales, preguntas frecuentes, plantillas de datos, sesiones formativas, un entorno de pruebas estable y asistencia en las lenguas oficiales de la Unión. En España, podría resultar útil canalizar parte de este acompañamiento a través de instituciones intermedias de naturaleza empresarial y redes territoriales con capilaridad suficiente para llegar a pymes, como las cámaras de comercio.

4.9. Sistemas de logs, mantenimiento y disponibilidad (artículos 14 y 15)

Se valora positivamente la incorporación de sistemas de logs para reforzar la trazabilidad del registro. No obstante, estos deberían permitir también su uso en auditorías o procesos de verificación, reforzando sus garantías de integridad y trazabilidad.

Asimismo, resulta importante que los periodos de mantenimiento y las posibles interrupciones del servicio se comuniquen con antelación y queden debidamente documentados, a fin de minimizar su impacto en los operadores.

Asimismo, sería recomendable definir indicadores mínimos de disponibilidad, plazos máximos de restablecimiento, procedimientos de comunicación de incidencias y ventanas de mantenimiento coordinadas con periodos de baja actividad. Esta

previsibilidad es esencial cuando el registro se convierta en una condición operativa para introducir productos en el mercado.

4.10. Responsabilidades y cadena de valor (artículos 19 y 20)

Resulta importante clarificar la asignación de responsabilidades a lo largo de la cadena de valor, de forma que las obligaciones se correspondan con la función real de cada operador.

En particular, los operadores intermedios deberían limitar su contribución a los datos relativos a sus propios materiales, sin asumir automáticamente la responsabilidad del pasaporte del producto final, salvo que se establezca expresamente. Todo ello sin perjuicio de que la responsabilidad del registro del pasaporte del producto final corresponda al operador que lo introduce en el mercado.

Del mismo modo, sería conveniente clarificar el tratamiento de los códigos de mercancía en el sistema, precisando si su referencia debe vincularse al material intermedio, al producto final o a ambos, y si puede recurrirse al código del sistema armonizado (HS Code) cuando resulte aplicable.

Asimismo, convendría avanzar en la delimitación de los procesos de generación, validación y actualización de los datos, así como en la asignación de responsabilidades cuando el producto cambie de estado o de operador a lo largo de su ciclo de vida.

También debería preverse una regla clara para los supuestos de transformación, reparación, reacondicionamiento o remanufactura que den lugar a un producto con identidad comercial distinta. En estos casos, conviene delimitar cuándo procede actualizar el pasaporte existente y cuándo debe generarse uno nuevo, evitando inseguridad jurídica para operadores intermedios.