

Bruselas, 20 de noviembre de 2025
(OR. en)

15698/25

**Expediente interinstitucional:
2025/0360 (COD)**

**SIMPL 186
ANTICI 185
DATAPROTECT 307
CYBER 337
TELECOM 417
PROCIV 155
CODEC 1872**

PROPUESTA

De: Por la secretaria general de la Comisión Europea, D.^a Martine DEPREZ, directora

Fecha de recepción: 20 de noviembre de 2025

A: D.^a Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea

N.º doc. Ción.: COM(2025) 837 final

Asunto: Propuesta de
REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO
por el que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Ómnibus Digital)

Adjunto se remite a las delegaciones el documento COM(2025) 837 final.

Adj.: COM(2025) 837 final



Bruselas, 19.11.2025
COM(2025) 837 final

2025/0360 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Ómnibus Digital)

{SWD(2025) 836 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

En su Comunicación sobre la aplicación y la simplificación («Una Europa más sencilla y rápida»)¹, la Comisión presentó su enfoque para adaptar el marco regulador de la Unión a un mundo más volátil: una nueva dinámica para simplificar, aclarar y mejorar el acervo de la UE, como medida clave para apoyar la competitividad de la UE.

Esta visión refleja el plan a mayor escala establecido por la presidenta de la Comisión, Ursula von der Leyen, en sus orientaciones políticas para el mandato 2024-2029². Como también se puso de manifiesto en los informes Draghi³ y Letta⁴, la acumulación de normas ha tenido a veces un efecto negativo en la competitividad. Son necesarias mejoras rápidas y visibles para las personas y las empresas, mediante una aplicación de nuestras normas más eficiente en términos de costes y favorable a la innovación, al tiempo que se mantienen unas normas estrictas y los objetivos acordados.

Las Conclusiones del Consejo Europeo de 20 de marzo de 2025 instaban además a la Comisión a «que siga revisando y poniendo a prueba la resistencia del acervo de la Unión a fin de determinar formas de simplificar y consolidar más la legislación vigente»⁵. También destacó la necesidad de llevar a cabo un seguimiento con nuevos conjuntos de iniciativas de simplificación. En sus Conclusiones de 26 de junio de 2025, el Consejo Europeo subrayó la importancia de un enfoque de «simplicidad desde la concepción» en lo que respecta a la legislación, «sin comprometer la previsibilidad, los objetivos estratégicos y las normas estrictas»⁶. Las Conclusiones del Consejo Europeo de 23 de octubre de 2025 reafirmaron «la necesidad urgente de progresar en una agenda ambiciosa y horizontal de simplificación y mejora de la legislación en todos los niveles (de la UE, nacional y regional) y en todos los ámbitos, para garantizar la competitividad de Europa». Asimismo, solicitaron a la Comisión que «lleve adelante rápidamente nuevos y ambiciosos paquetes legislativos de simplificación, entre otras cosas, sobre [...] el ámbito digital [...]»⁷.

En su Resolución sobre la aplicación y racionalización de las normas del mercado interior de la Unión para reforzar el mercado único, votada el 11 de septiembre en el Pleno⁸, el

¹ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones titulada «Una Europa más sencilla y rápida: Comunicación sobre la aplicación y la simplificación» [COM(2025) 47 final], 11 de febrero de 2025.

² Von der Leyen, U. (2024). *La decisión de Europa: Orientaciones políticas para la próxima Comisión Europea 2024-2029*. Disponible en: e6cd4328-673c-4e7a-8683-f63ffb2cf648_es.

³ Draghi, M. (2024). *The future of European competitiveness* [«El futuro de la competitividad europea», documento en inglés]. Disponible en: El Informe Draghi sobre la competitividad de la UE.

⁴ Letta, E. (2024). *Much more than a market* [«Mucho más que un mercado», documento en inglés]. Disponible en: Enrico Letta, Much more than a market [«Mucho más que un mercado», documento en inglés] (abril de 2024).

⁵ Consejo Europeo, Conclusiones, EUCO 1/25, Bruselas, 20 de marzo de 2025, apartado 13.

⁶ Consejo Europeo, Conclusiones, EUCO 12/25, Bruselas, 26 de junio de 2025, apartado 30.

⁷ Consejo Europeo, Conclusiones, EUCO 18/25, Bruselas, 23 de octubre de 2025, apartados 33 y 35.

⁸ Parlamento Europeo, Resolución sobre la aplicación y racionalización de las normas del mercado interior de la Unión para reforzar el mercado único, 11 de septiembre de 2025 (2025/2009/INI).

Parlamento Europeo hizo hincapié en la necesidad de simplificación a fin de facilitar el cumplimiento por parte de las empresas sin comprometer los objetivos estratégicos fundamentales de la Unión.

En las actividades de consulta y participación de la Comisión en torno al programa de simplificación, las partes interesadas que representan distintos intereses han solicitado modificaciones específicas de determinadas normas digitales, tanto para racionalizar los costes de cumplimiento como para aclarar las interacciones entre las normas de sus respectivos sectores.

Con un valor añadido de 791 000 millones EUR en toda la UE en 2022⁹, el sector de las tecnologías de la información y de las comunicaciones (TIC) desempeña un papel crucial a la hora de impulsar la competitividad de la UE en todos los sectores de la economía, tanto a través del crecimiento de las empresas digitales como de la provisión de soluciones digitales clave en todos los ámbitos. Las normas digitales han sido decisivas en la configuración de un entorno empresarial justo en la UE. Han establecido un verdadero mercado único de servicios digitales. La UE ha sido pionera en la regulación digital y ha establecido la norma de referencia para el máximo nivel de protección de los derechos fundamentales, la seguridad de los consumidores y la protección de los valores europeos.

La Comisión se ha comprometido a llevar a cabo una «prueba de resistencia» exhaustiva del código normativo digital a lo largo de todo el mandato legislativo. El propósito es muy claro: garantizar que las normas sigan siendo adecuadas para apoyar la innovación y el crecimiento, que cumplan sus objetivos y que son un motor para la competitividad. A lo largo de este proceso, la Comisión tratará de ofrecer soluciones sólidas y eficaces para simplificar, aclarar y consolidar la eficacia de las normas y su aplicación a través de todos los instrumentos disponibles, ya sean ajustes normativos, una mayor cooperación entre las autoridades, la promoción de soluciones digitales que simplifiquen el cumplimiento de la normativa «desde la concepción» u otras medidas de acompañamiento.

La propuesta Ómnibus Digital es un primer paso para optimizar la aplicación del código normativo digital. Incluye una serie de modificaciones técnicas de un amplio corpus de legislación digital, seleccionadas para proporcionar un alivio inmediato a empresas, administraciones públicas y ciudadanos por igual, a fin de estimular la competitividad. El objetivo inmediato es garantizar que el cumplimiento de las normas tenga un menor coste, cumpla los mismos objetivos y aporte por sí mismo una ventaja competitiva a las empresas responsables. Las modificaciones se priorizaron sobre la base de las consultas con las partes interesadas y los primeros diálogos sobre la aplicación llevados a cabo por la vicepresidenta ejecutiva Henna Virkkunen y el comisario Michael McGrath.

Por estos motivos, las modificaciones se centran en brindar nuevas oportunidades en el uso de los datos, como recurso fundamental en la economía de la UE, en particular con vistas a apoyar el desarrollo y el uso de soluciones de inteligencia artificial (IA) fiables en el mercado de la UE. Las modificaciones específicas de las normas en materia de protección de datos y

⁹ Eurostat (2025) *Statistics explained: ICT sector – value added, employment and R&D* [«Estadísticas explicadas – Sector de las TIC: valor añadido, empleo e I+D», página web en inglés]. Disponible en: [ICT sector - value added, employment and R&D - Statistics Explained - Eurostat](#).

privacidad apoyan este objetivo y proporcionan medidas inmediatas de simplificación para las empresas y las personas, a fin de reforzar su capacidad para ejercer sus derechos.

Además, las modificaciones del Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial¹⁰), presentadas en una propuesta legislativa separada que forma parte del paquete Ómnibus Digital, tienen por objeto facilitar la aplicación fluida y eficaz de las normas para un desarrollo y un uso seguros y fiables de la IA.

El paquete Ómnibus Digital también propone una solución muy clara para optimizar la notificación de incidentes de ciberseguridad, al englobar todas las obligaciones relacionadas en un mecanismo único de notificación.

Por último, la propuesta deroga normas obsoletas en el ámbito de la regulación de las plataformas, que han sido sustituidas por reglamentos más recientes.

Las modificaciones tienen por objeto simplificar las normas, reducir el número de leyes y armonizar las disposiciones. Asimismo, reducen los costes administrativos mediante la simplificación de las disposiciones y los procedimientos. Eximen a las pequeñas empresas de mediana capitalización de determinadas obligaciones contempladas en la legislación en materia de datos y en el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial¹¹), además de a las pequeñas empresas y microempresas ya cubiertas por un régimen especial. También fomentan las oportunidades para un entorno empresarial dinámico y crean más seguridad jurídica y oportunidades, en particular para el intercambio y la reutilización de datos, el tratamiento de datos personales o el entrenamiento de sistemas y modelos de IA.

Al mismo tiempo, las modificaciones propuestas siguen siendo de carácter técnico y tienen por objeto ajustar el marco regulador, pero no modificar sus objetivos subyacentes. Las medidas se calibran para preservar el mismo nivel de protección de los derechos fundamentales.

Junto con el paquete Ómnibus Digital, la Comisión también presenta su propuesta de **Reglamento sobre las carteras europeas para empresas**, como iniciativa fundamental para simplificar el cumplimiento de la normativa y reducir las cargas administrativas para las empresas. Las carteras para empresas se diseñarán como herramientas digitales seguras para las empresas, y actuarán como una plataforma única para simplificar sus interacciones en toda la UE. Mediante la aplicación de un identificador único y persistente, las empresas estarán facultadas para verificar identidades de forma digital, firmar documentos, sellar fechas y horas e intercambiar información digital verificada sin problemas a través de las fronteras mediante el uso de una solución única. Con la adopción de carteras europeas para empresas, las empresas, especialmente las pymes, podrán abordar sus obligaciones de cumplimiento con mayor facilidad y liberar recursos esenciales que pueden reorientarse hacia el crecimiento y la innovación.

¹⁰ Según la propuesta legislativa separada.

¹¹ Según la propuesta separada.

Como segundo paso en el compromiso de llevar a cabo «pruebas de resistencia» del código normativo digital, **la Comisión también está llevando a cabo un control de adecuación digital**. Si bien las propuestas del paquete Ómnibus Digital son inmediatas y específicas, el análisis que llevará a cabo la Comisión en el control de adecuación digital se centrará en el impacto acumulativo de las normas digitales, con el fin de comprobar cómo apoyan la competitividad de la UE y dónde será necesario proponer nuevos ajustes en la segunda mitad del mandato legislativo.

El control de adecuación digital se pone en marcha al mismo tiempo que la propuesta Ómnibus Digital, con una amplia consulta pública. La intención de la Comisión es colaborar con todas las partes interesadas y realizar amplias consultas. El objetivo es realizar un seguimiento con una visión de conjunto y un amplio inventario de cómo el código normativo digital se aplica en sectores estratégicos de la industria de la UE, y abordar de qué manera el efecto acumulativo de las normas repercute en su competitividad. Sobre esta base, el análisis profundizará en una segunda fase en las sinergias y los ámbitos que podrían armonizarse aún más, desde las definiciones y los conceptos jurídicos hasta la eficacia y la interacción de los sistemas de gobernanza y otras medidas de apoyo.

Las «pruebas de resistencia» del acervo digital también continuarán a través de diálogos sobre la aplicación, así como con **evaluaciones de todos los principales instrumentos jurídicos**. En la planificación actual, entre otras iniciativas, la Comisión espera publicar en 2026 una revisión de Reglamento de Mercados Digitales, del Programa Estratégico de la Década Digital, el Reglamento de Chips, la Directiva de Servicios de Comunicación Audiovisual y una evaluación de la Directiva sobre derechos de autor. Para 2027, los actos legislativos que se espera evaluar incluyen, entre otros, el Reglamento de Cibersolidaridad, el Reglamento sobre la internet abierta, la Directiva SRI 2 y el Reglamento de Servicios Digitales. En 2028, por ejemplo, la Comisión debe evaluar el Reglamento Europeo sobre la Libertad de los Medios de Comunicación y el Reglamento de Datos, seguidos de una evaluación del Reglamento de Inteligencia Artificial en 2029 y una evaluación de la cláusula de extinción del Reglamento por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

Las partes interesadas han subrayado reiteradamente que, en muchos casos, el esfuerzo de simplificación tiene menos que ver con modificar las normas y más con aportar claridad sobre su aplicación. **La Comisión da prioridad a una serie de directrices** destinadas a apoyar la aplicación uniforme de las normas, sin perjuicio de las interpretaciones del Tribunal de Justicia de la Unión Europea (TJUE).

Por lo que respecta al marco regulador en materia de datos, la Comisión anunció su carácter prioritario en la Estrategia de Datos de la Unión, centrándose en particular en directrices sobre una compensación razonable para aclarar lo que puede cobrarse por el intercambio de datos y aportar seguridad jurídica tanto a los tenedores de datos como a los destinatarios de datos, así como en directrices destinadas a aclarar las definiciones.

Para apoyar la aplicación del Reglamento de Inteligencia Artificial, la Comisión sigue dando prioridad a la publicación de directrices sobre varios aspectos, como se detalla en la exposición de motivos de la propuesta Ómnibus Digital por la que se modifica el citado Reglamento.

Propuestas incluidas en el paquete Ómnibus Digital

El «acervo legislativo en materia de datos» se ha ampliado en los últimos años hasta abarcar una serie de reglamentos, lo que ha generado complejidad jurídica, en particular algunos solapamientos, definiciones no perfectamente armonizadas y preguntas sobre la interacción de los instrumentos. En concreto, se adoptó el Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), que se concibió para crear un mercado único de servicios en la nube. Ha sido parcialmente sustituido por el capítulo VI del Reglamento (UE) 2023/2854 (Reglamento de Datos), que establece obligaciones relativas al cambio entre servicios de tratamiento de datos.

Otro ejemplo es el capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos), que completa las normas sobre la reutilización de la información del sector público de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) en el caso de los datos que no pueden reutilizarse sin restricciones. Además, otros capítulos del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) crearon normas sobre los servicios de intermediación de datos, la cesión altruista de datos y los requisitos para las solicitudes de acceso de gobiernos extranjeros a datos no personales, y crearon el Comité Europeo de Innovación en materia de Datos. Por otra parte, el Reglamento (UE) 2023/2854 (Reglamento de Datos) creó la obligación sustantiva para los fabricantes de dispositivos conectados y los proveedores de servicios relacionados de compartir datos con sus usuarios, así como la obligación de que las empresas compartan datos con organismos del sector público y normas sobre contratos justos de intercambio de datos.

Para abordar esta cuestión, el paquete Ómnibus Digital propone derogar normas obsoletas, especialmente las normas actuales del Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), con la excepción de la prohibición de los requisitos de localización de datos en la Unión, y consolidar y racionalizar las normas del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos), como las normas sobre la cesión altruista de datos y los servicios de intermediación de datos, a fin de aumentar el atractivo de dichos mecanismos de intercambio de datos. Al mismo tiempo, las normas sobre reutilización de datos protegidos del Reglamento relativo a la gobernanza europea de datos se fusionan con las normas de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) para crear un marco único para la reutilización de los datos en poder de los organismos del sector público que se refleja en el Reglamento (UE) 2023/2854 (Reglamento de Datos). Esta solución presenta numerosas ventajas para las administraciones públicas que poseen datos del sector público, así como para los reutilizadores, ya que pueden optimizar los procesos y reducir la carga administrativa asociada a la interpretación y aplicación de diversas leyes nacionales.

La propuesta introduce además la posibilidad de que los organismos del sector público establezcan condiciones diferentes y cobren tasas más elevadas por la reutilización por parte de empresas muy grandes y, en particular, empresas designadas como «guardianes de acceso», tal como se definen en el artículo 3 del Reglamento (UE) 2022/1925 (Reglamento de Mercados Digitales), dado que ostentan un poder y una influencia significativos en el mercado interior. Para evitar que estas empresas aprovechen su considerable poder de mercado en detrimento de la competencia leal y la innovación, los organismos del sector público podrán establecer condiciones especiales para la reutilización de datos y documentos por parte de tales empresas.

La propuesta incluye las normas consolidadas y racionalizadas del Reglamento (UE) 2024/1689 (Reglamento sobre la libre circulación de datos no personales), el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) y la Directiva (UE)

2019/1024 (Directiva sobre datos abiertos) en el Reglamento (UE) 2023/2854 (Reglamento de Datos), creando un único instrumento consolidado para la economía de los datos de Europa. Quedan derogados el Reglamento (UE) 2024/1689 (Reglamento sobre la libre circulación de datos no personales), la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) y el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). Las normas de los cuatro instrumentos están mejor armonizadas y racionalizadas para aumentar la claridad y la coherencia, mejorar su eficacia y apoyar a las empresas en el fomento de la innovación. Esta iniciativa se ajusta a la Estrategia de Datos de la Unión, cuyo objetivo fundamental es impulsar la simplificación del marco legislativo.

Además, para seguir ayudando a las empresas más pequeñas, las normas que facilitan el cumplimiento de la legislación de la UE en materia de datos para las pymes se amplían a efectos de incluir a las pequeñas empresas de mediana capitalización. El Reglamento (UE) 2023/2854 (Reglamento de Datos), que entró en vigor el 12 de septiembre de 2025, supone un paso significativo hacia una economía de los datos justa y competitiva en la UE. Los cambios que plantea la presente propuesta no tienen por objeto introducir modificaciones en lo ya conseguido por el Reglamento (UE) 2023/2854 (Reglamento de Datos).

Sin embargo, para alcanzar plenamente su objetivo de equilibrar la innovación y la disponibilidad de datos con la protección de los derechos e intereses de los tenedores de datos, es necesario calibrar cuatro elementos clave. En concreto, es fundamental garantizar que el Reglamento (UE) 2023/2854 (Reglamento de Datos) no solo reduzca las cargas, sino que también aumente la claridad jurídica e impulse la competitividad. En primer lugar, existe una necesidad urgente de reforzar las garantías contra el riesgo de filtraciones de secretos comerciales a terceros países en el contexto de las disposiciones obligatorias sobre el intercambio de datos de la internet de las cosas. En segundo lugar, el amplio ámbito de aplicación del marco entre empresas y administraciones públicas podría dar lugar a ambigüedad jurídica. En tercer lugar, las disposiciones sobre los requisitos esenciales para los contratos inteligentes que ejecutan acuerdos de intercambio de datos podrían generar inseguridad jurídica. Por último, las disposiciones del Reglamento (UE) 2023/2854 (Reglamento de Datos) sobre el cambio entre servicios de tratamiento de datos mantienen su pertinencia como contribución esencial a un mercado en la nube más abierto y competitivo. Sin embargo, estas disposiciones no tenían suficientemente en cuenta la situación específica de los servicios que, para poder utilizarse, requieren una personalización significativa para adaptarse a las necesidades de un cliente o que son prestados por pymes y pequeñas empresas de mediana capitalización. Las modificaciones que contiene la presente propuesta mantendrán la ambición de eliminar la dependencia de un proveedor, en particular los costes por cambio y los costes de salida de datos, al tiempo que reducen la carga administrativa para los proveedores de los servicios mencionados. Así pues, la propuesta presenta modificaciones que mejoran la claridad jurídica y se ajustan en gran medida a los objetivos generales del Reglamento (UE) 2023/2854 (Reglamento de Datos).

Además, para seguir ayudando a las empresas más pequeñas, las normas que facilitan el cumplimiento del acervo de la UE en materia de datos para las pymes se amplían a efectos de incluir a las pequeñas empresas de mediana capitalización.

Por lo que se refiere a los datos personales, el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos o RGPD) entró en vigor el 25 de mayo de 2018 y creó normas, reglas y garantías a escala de la Unión para el tratamiento de los datos personales de las personas físicas, los derechos de los interesados y

un marco jurídico general para dicho tratamiento de datos personales. Si bien las partes interesadas consideran, en general, que el Reglamento (UE) 2016/679 es equilibrado y sólido y sigue siendo adecuado para su finalidad, algunas entidades, especialmente las empresas y asociaciones de menor tamaño con un número reducido de operaciones de tratamiento de datos no intensivas y a menudo de bajo riesgo, expresaron su preocupación en lo que respecta a la aplicación de algunas obligaciones del Reglamento general de protección de datos. Algunas de estas preocupaciones pueden abordarse mediante una interpretación y una aplicación más coherentes y armonizadas en todos los Estados miembros, mientras que otras requieren modificaciones específicas de la legislación. En este contexto, las modificaciones que contiene la presente propuesta tienen por objeto abordar dichas preocupaciones, en particular mediante la aclaración de determinadas definiciones clave, por ejemplo, el concepto de datos personales; mediante la facilitación del cumplimiento, por ejemplo, con el apoyo a los responsables del tratamiento con respecto a los criterios y los medios para determinar si los datos resultantes de la seudonimización no constituyen datos personales, en relación con los requisitos de información y las notificaciones de violaciones de la seguridad de los datos a las autoridades de control; así como mediante la aclaración de determinados aspectos del tratamiento de datos para el entrenamiento y el desarrollo de la IA. Las modificaciones propuestas también abordan la falta de claridad sobre las condiciones para la investigación científica al proporcionar una definición de investigación científica, aclarar en mayor medida que el tratamiento ulterior con fines científicos es compatible con la finalidad inicial del tratamiento y precisar que la investigación científica constituye un interés legítimo. También se propone ampliar las excepciones a la obligación de información para el tratamiento. Cuando proceda, la presente propuesta refleja las modificaciones del Reglamento general de protección de datos contenidas en el Reglamento (UE) 2018/1725 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión.

Por otro lado, hace tiempo que es necesaria una solución reglamentaria sobre el hartazgo del consentimiento y la proliferación de anuncios de *cookies*. La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, revisada por última vez en 2009, proporciona un marco para proteger la confidencialidad de las comunicaciones y remite al Reglamento (UE) 2016/679 («Reglamento general de protección de datos») en lo que respecta al tratamiento de datos personales en el contexto de las comunicaciones electrónicas. También protege los equipos terminales de los usuarios que pueden utilizarse para invadir su privacidad y recopilar información relativa a dichos usuarios. Una parte esencial del uso de equipos terminales, como teléfonos y ordenadores personales, es consumir contenidos y utilizar servicios en línea. Muchos de estos servicios en línea dependen de los ingresos procedentes de la publicidad, en particular la publicidad personalizada. Este es también el caso de los servicios de medios de comunicación. Los proveedores de servicios en línea recurren a las denominadas *cookies* o tecnologías similares que utilizan las capacidades de tratamiento y almacenamiento de los equipos terminales, y acceden de esta manera, por ejemplo, a información almacenada en los equipos terminales o emitida por ellos. Esto se hace con diversos fines, como optimizar la prestación del servicio para el equipo terminal concreto y garantizar la seguridad del equipo terminal y del servicio en general, pero también para hacer un seguimiento del comportamiento y la interacción de las personas con diferentes servicios en línea a fin de ofrecer publicidad personalizada.

Cuando el uso de estas tecnologías no sea necesario para el almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o cuando sea estrictamente necesario a fin de proporcionar un servicio de la sociedad de la información expresamente solicitado por el usuario o el abonado, la Directiva 2002/58/CE requiere el consentimiento. Este

consentimiento suele solicitarse a través de anuncios emergentes que se muestran en el sitio web o la aplicación para dispositivos móviles. Estos anuncios contienen información sobre los fines del tratamiento, a menudo vinculados a tipos de *cookies* y destinatarios de datos, y no siempre son fáciles de entender para las personas. Por estos motivos, es posible que no logren su objetivo, es decir, informar a la persona y darle control sobre la protección de su privacidad y el tratamiento de sus datos personales, sino que, en su lugar, los usuarios de internet los perciban como una molestia. Al mismo tiempo, los proveedores de servicios en línea asumen costes considerables para diseñar anuncios que cumplan la normativa.

Haciendo que la complejidad sea cada vez mayor, el artículo 5, apartado 3, de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) se aplica a la colocación de *cookies* o tecnologías similares para obtener información del equipo terminal de un usuario, mientras que el tratamiento posterior de datos personales está sujeto al Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Si bien el consentimiento es necesario para garantizar el control por parte de los interesados, no siempre es la base jurídica más adecuada para el tratamiento posterior, por ejemplo, cuando el tratamiento es necesario para la prestación de un servicio distinto del servicio de la sociedad de la información. Esto ha dado lugar a inseguridad jurídica y a mayores costes de cumplimiento para los responsables del tratamiento que tratan datos personales obtenidos de equipos terminales. Además, el doble régimen de la Directiva sobre la privacidad y las comunicaciones electrónicas y del RGPD ha dado lugar a que diferentes autoridades nacionales sean competentes para supervisar las normas de ambos marcos jurídicos.

Por estas razones, se propone simplificar inmediatamente la interacción de las normas aplicables. El tratamiento de datos personales en equipos terminales o procedentes de ellos debe regirse únicamente por el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) e incorporar asimismo el requisito claro de obtener el consentimiento para acceder al equipo terminal de una persona física cuando se recojan datos personales. Las modificaciones propuestas también prevén determinados fines para los que no debe ser necesario obtener el consentimiento y para los que el tratamiento posterior debe considerarse lícito, en particular cuando supongan un riesgo bajo para los derechos y libertades de los interesados o cuando la colocación de dichas tecnologías sea necesaria para la prestación de un servicio solicitado por el interesado.

Por último, la propuesta allana el camino para las indicaciones automatizadas y legibles por máquina de las preferencias individuales y el respeto de dichas indicaciones por parte de los proveedores de sitios web y aplicaciones para dispositivos móviles y los proveedores de aplicaciones para teléfonos móviles una vez que se disponga de normas al respecto. Esto se basa en la modificación de 2009 de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) (véase el considerando 66 de la Directiva 2009/136/CE), que ya animaba a permitir que los usuarios expresaran su consentimiento utilizando la configuración adecuada de un navegador u otra aplicación cuando sea técnicamente posible y eficaz, y en el artículo 21, apartado 5, del Reglamento (UE) 2016/679 (Reglamento general de protección de datos), así como en la propuesta de 2017 de la Comisión relativa a un Reglamento sobre la privacidad y las comunicaciones electrónicas [COM(2017) 10 final], que proponía la gestión de las opciones de usuario mediante la configuración del navegador web. La propuesta otorga a la Comisión el mandato de solicitar a los organismos de normalización que elaboren un conjunto de normas para codificar las indicaciones automatizadas y legibles por máquina de las preferencias de los interesados, así como la comunicación de dichas preferencias de los navegadores a los sitios web y de las aplicaciones para teléfonos móviles a los servicios web. Una vez que estén disponibles, y tras un período de transición de seis

meses, los responsables del tratamiento que utilicen sitios web y aplicaciones para dispositivos móviles para prestar su servicio estarán obligados a respetar dichas indicaciones codificadas automatizadas y legibles por máquina. Cuando los responsables del tratamiento garanticen que sus sitios web o aplicaciones para teléfonos móviles cumplen dichas normas, deben beneficiarse de una presunción de cumplimiento. Sobre esta base, se espera que los navegadores también desarrollen parámetros pertinentes. Las disposiciones se formulan de manera tecnológicamente neutra, de modo que también otras herramientas, como la IA agente, podrían ayudar a los usuarios a tomar decisiones de consentimiento, siempre que resulten adecuadas para garantizar el cumplimiento de los requisitos del RGPD. Teniendo en cuenta la importancia de los flujos de ingresos en línea para el periodismo independiente como pilar indispensable de una sociedad democrática, los prestadores de servicios de medios de comunicación, tal como se definen en el Reglamento (UE) 2024/1083 (Reglamento Europeo sobre la Libertad de los Medios de Comunicación), no deben estar obligados a respetar dichas señales, permitiéndoles que tengan una interacción directa con los usuarios a la hora de informarlos y permitirles escoger sus preferencias de consentimiento.

Las modificaciones presentadas en el presente Reglamento introducirán un **punto de entrada único a través del cual las entidades podrán cumplir simultáneamente sus obligaciones de notificación de incidentes en virtud de varios actos jurídicos**. Al promover el principio de «presentación única de la información y difusión múltiple», el punto de entrada único reducirá la carga administrativa para las entidades, a la vez que garantizará un flujo efectivo y seguro de información sobre incidentes de seguridad a los destinatarios definidos en la legislación correspondiente.

La propuesta establece la obligación de que la Agencia de la Unión Europea para la Ciberseguridad (ENISA) desarrolle el punto de entrada único, teniendo en cuenta la plataforma única de notificación para las notificaciones de vulnerabilidades aprovechadas activamente y de incidentes graves en virtud del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia). Asimismo, exige requisitos específicos para la herramienta, como canal seguro de la información comunicada por las entidades y enviada a las autoridades competentes. No modifica los requisitos legales subyacentes para la notificación de incidentes, pero optimiza significativamente el flujo de trabajo y los recursos que las entidades requieren.

La propuesta también exige el uso del punto de entrada único para una serie de obligaciones de notificación de incidentes estrechamente interconectadas establecidas en la Directiva (UE) 2022/2555 (Directiva SRI 2), el Reglamento (UE) 2016/679 (RGPD), el Reglamento (UE) 2022/2554 (Reglamento sobre Resiliencia Operativa Digital), el Reglamento (UE) n.º 910/2014 (Reglamento eIDAS) y la Directiva (UE) 2022/2557 (Directiva relativa a la resiliencia de las entidades críticas o REC). Otras obligaciones de notificación sectoriales, como las establecidas en el marco del código de red para abordar los aspectos relativos a la ciberseguridad en los flujos eléctricos transfronterizos y en los instrumentos pertinentes para el sector de la aviación, también se integrarán en el punto de entrada único mediante modificaciones de los correspondientes actos delegados y de ejecución que establecen las obligaciones de notificación en virtud de dichos marcos.

La propuesta también tiene por objeto racionalizar el contenido de la información notificada mediante habilitaciones en varios actos jurídicos que aún carezcan de ellas. La propuesta aclara que, a la hora de desarrollar plantillas comunes de notificación de información para la Directiva (UE) 2022/2555, la Directiva (UE) 2022/2557 o el Reglamento (UE) 2016/679, y con el fin de garantizar la coherencia, promover sinergias y reducir la carga administrativa para las entidades mediante la minimización del número de campos de datos que estas deben

cumplimentar, la Comisión debe tener debidamente en cuenta la experiencia adquirida y las plantillas comunes desarrolladas en virtud del Reglamento (UE) 2022/2554 (Reglamento sobre Resiliencia Operativa Digital).

Además de estos cambios fundamentales, la propuesta aprovecha la oportunidad para derogar el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (Reglamento sobre las relaciones entre plataformas y empresas o «Reglamento P2B»). El Reglamento se aplica desde el 12 de julio de 2020 y fue el primer paso hacia la creación de un marco jurídico integral para la economía de plataformas. Desde su entrada en vigor, se han adoptado otros actos legislativos de la UE para regular los servicios de intermediación en línea y las plataformas en línea. Entre ellos se encuentran el Reglamento (UE) 2022/1925 (Reglamento de Mercados Digitales) y el Reglamento (UE) 2022/2065 (Reglamento de Servicios Digitales), que superan en gran medida las disposiciones del Reglamento P2B. Determinadas disposiciones del Reglamento P2B seguirán en vigor para garantizar la seguridad jurídica de los actos legislativos que contengan referencias cruzadas a estas disposiciones, por ejemplo, la Directiva (UE) 2023/2831 relativa a la mejora de las condiciones laborales en el trabajo en plataformas. En general, la simplificación del marco regulador de las plataformas en línea reducirá los costes de cumplimiento derivados de la existencia de normas que se superponen y se solapan, tal como han solicitado las partes interesadas. Los prestadores de servicios intermediarios en línea se beneficiarán de una mayor claridad de las disposiciones legales. La aplicación de la normativa será más específica.

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La propuesta va acompañada de una segunda propuesta por la que se modifica el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial); juntos, forman el paquete «Ómnibus Digital» y marcan el primer paso inmediato en la simplificación del código normativo digital. Además del paquete Ómnibus Digital, la propuesta de revisión del Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad) incluirá, entre otras cosas, el mandato actualizado de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), así como medidas destinadas a simplificar el cumplimiento de los requisitos en materia de ciberseguridad.

El paquete Ómnibus Digital forma parte de una estrategia más amplia de simplificación normativa anunciada a través del paquete digital, que se presenta con mayor detalle en el apartado introductorio de la presente exposición de motivos.

- **Coherencia con otras políticas de la Unión**

La propuesta forma parte de la agenda de la Comisión para la simplificación del marco regulador de la UE. El amplio alcance de los actos modificados muestra el claro potencial de simplificación al abordar la interacción entre las distintas normas, en particular cuando se refieren a diferentes ámbitos estratégicos. Este es el caso, por ejemplo, de la solución de simplificación digital desarrollada en el marco del punto de entrada único para la notificación de incidentes, que no altera las obligaciones reglamentarias subyacentes, pero reúne en la misma interfaz las normas en materia de ciberseguridad aplicables a las entidades esenciales, las aplicables al sector financiero, las normas de protección de datos y otras.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La propuesta se basa en los artículos 16 y 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que constituyen la base jurídica de los actos modificados. La base jurídica adecuada para las disposiciones por las que se modifican el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el Reglamento (UE) 2018/1725 es el artículo 16 del TFUE. Dado que todos los demás actos modificados se basan en el artículo 114 del TFUE, la misma base jurídica también es adecuada para las correspondientes disposiciones por las que se modifica el presente Reglamento.

• Subsidiariedad (en el caso de competencia no exclusiva)

Dado que las normas modificadas son normas de la Unión, solo pueden modificarse a nivel de la Unión. Los ajustes técnicos presentados en el presente Reglamento conservan la lógica de subsidiariedad que subyace a los actos modificados.

Por lo que se refiere al Reglamento (UE) 2023/2854 (Reglamento de Datos), las modificaciones refuerzan el objetivo del Reglamento de eliminar los obstáculos en el mercado único para la economía de los datos, y lo hacen incorporando al Reglamento normas ya existentes. Las modificaciones específicas introducidas en dichas normas tienen por objeto simplificar, aportar claridad y reducir las cargas administrativas tanto para el sector privado como para las autoridades nacionales. No interfieren con las competencias de los Estados miembros o de las instituciones de la UE.

Este es también el caso de la derogación de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos), teniendo en cuenta que sus normas sustantivas se incorporan al Reglamento (UE) 2023/2854 (Reglamento de Datos) sin modificar sustancialmente las competencias otorgadas a los Estados miembros. En la actualidad, una parte significativa de los datos del sector público ya está sujeta al Reglamento de Ejecución (UE) 2023/138, directamente aplicable, relativo a los conjuntos de datos de alto valor¹². La transformación en un Reglamento facilitará la aplicación uniforme de los cambios propuestos en todos los Estados miembros. Apoyará en especial a las administraciones públicas que poseen datos del sector público, pero también a los reutilizadores de estos datos, mediante la optimización de los procesos y la reducción de la carga administrativa asociada a la interpretación y aplicación de diversas leyes nacionales. También es probable que la aplicación de las normas directamente aplicables sea más coherente. La propuesta no modifica los regímenes nacionales de acceso y tiene por objeto ofrecer suficiente flexibilidad a las soluciones nacionales, una prerrogativa que los Estados miembros han destacado.

Por lo que se refiere al Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y al Reglamento (UE) 2018/1725, las modificaciones propuestas tienen por objeto aportar claridad y previsibilidad en la aplicación de las normas vigentes, así como reducir la carga administrativa, en la medida de lo posible, sin socavar el elevado nivel de protección de

¹² Reglamento de Ejecución (UE) 2013/138,

datos en virtud del RGPD y del Reglamento (UE) 2018/1725. Del mismo modo, no modifican las competencias de los Estados miembros ni de los órganos e instituciones de la UE.

Con la introducción del punto de entrada único para la notificación de incidentes, se propone una solución a escala europea para proporcionar un único canal para múltiples obligaciones jurídicas que se imponen a las empresas para la notificación de incidentes que son, en esencia, el mismo. La solución no altera en modo alguno los derechos y competencias de las autoridades nacionales para recibir tales notificaciones. En su lugar, incentiva la notificación al ofrecer un punto de entrada único con una interfaz fácil de utilizar que permite, aparentemente, presentar un único informe, mientras se cumplen simultáneamente varias obligaciones legales. Dado que muchos de los servicios en cuestión se prestan de forma transfronteriza y los proveedores están presentes en varios Estados miembros, es necesaria una solución a escala europea.

- **Proporcionalidad**

La propuesta incluye las modificaciones técnicas necesarias para alcanzar los objetivos de reducir las cargas administrativas y aportar claridad normativa, al tiempo que se preservan y optimizan los objetivos subyacentes de la legislación modificada. Las modificaciones son proporcionadas, ya que imponen costes transitorios y de adaptación insignificantes, en su caso, a las empresas y las autoridades, pero facilitan un elevado rendimiento en términos de ahorro de costes durante los próximos años.

Varias de las modificaciones que introduce el presente Reglamento persiguen el objetivo de simplificación al proporcionar principalmente seguridad jurídica y aclarar la aplicación de las normas, por ejemplo, en lo que respecta a las aclaraciones para los tenedores de datos sobre la protección de los secretos comerciales en el Reglamento (UE) 2023/2854 (Reglamento de Datos), o las aclaraciones sobre los modelos y sistemas de entrenamiento de IA que incluyen datos personales regulados por el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos), o el concepto de datos personales en este último Reglamento y en el Reglamento (UE) 2018/1725. Algunas de las disposiciones tienen por objeto codificar las interpretaciones del Tribunal de Justicia de la Unión Europea, como las relativas a la seudonimización de los datos personales, que se aclaran con más detalle en el Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Como tales, incluyen modificaciones muy específicas de las normas, al tiempo que espera que tengan una gran incidencia a la hora de ofrecer seguridad jurídica a las empresas y los inversores.

Las modificaciones propuestas en el presente Reglamento también tienen por objeto reducir los costes directos para las empresas y las autoridades, constatando que pueden alcanzarse los mismos objetivos normativos con menos cargas y garantizando la proporcionalidad de las normas. Por ejemplo, el régimen obligatorio para los servicios de intermediación de datos previsto en el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) se transforma, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), en un régimen voluntario orientado a reforzar la confianza.

Con la ampliación a las pequeñas empresas de mediana capitalización de determinadas disposiciones aplicables a las pymes, las medidas de simplificación son específicas e introducen cambios mínimos en el ámbito de aplicación de dichas obligaciones, mientras que proporcionan seguridad jurídica a un abanico más amplio de empresas con un elevado potencial de apoyo a la competitividad de la UE. Las propuestas se limitan a los cambios necesarios para garantizar que las pequeñas empresas de mediana capitalización se beneficien del mismo marco jurídico que las pymes.

El punto de entrada único para la notificación de incidentes y las notificaciones de violaciones de la seguridad de los datos conlleva un elevado ahorro de costes para las empresas, al tiempo que aborda la cuestión generalizada de la infranotificación. No es solo una solución proporcionada, sino que aporta una solución clave de simplificación a través de una herramienta digital y apoya la eficacia de las obligaciones de notificación que prevé el punto de entrada único.

La derogación del Reglamento (UE) 2019/1150 (Reglamento P2B) es necesaria para eliminar la duplicación de normas; el Reglamento tiene tan solo un valor residual y, en vista de un enfoque normativo proporcionado en la regulación de las plataformas en línea, es necesario eliminar la doble obligación.

- **Elección del instrumento**

Dada la naturaleza de las normas modificadas, las modificaciones se proponen mediante un Reglamento. Cuando se modifican directivas, las disposiciones se dirigen a organismos europeos o bien introducen modificaciones específicas, en particular para incluir disposiciones que se desarrollarán en mayor profundidad en los reglamentos.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *ex post* / controles de la adecuación de la legislación existente**

La mayor parte de la legislación considerada en la presente propuesta es relativamente reciente y está sujeta a una evaluación continua de los resultados. Las principales observaciones se resumen en el documento de trabajo de los servicios de la Comisión adjunto.

Una excepción es la revisión preliminar de 2023 del Reglamento (UE) 2019/1150 [Reglamento sobre las relaciones entre plataformas y empresas (P2B)¹³]. El informe constató efectos positivos iniciales, por ejemplo, en lo que respecta a la transparencia contractual para los usuarios profesionales y a la tutela judicial efectiva en la tramitación de reclamaciones. Sin embargo, el informe también puso de manifiesto que los usuarios profesionales, así como los proveedores de servicios de intermediación en línea y de motores de búsqueda en línea, desconocían sus respectivos derechos y obligaciones con arreglo al Reglamento (UE) 2019/1150 (Reglamento P2B). Esto se suma también a un cumplimiento deficiente de dicho Reglamento, lo que dio lugar a una falta de aplicación. Hasta 2023 se recibieron muy pocas denuncias en virtud del Reglamento (UE) 2019/1150 (Reglamento P2B). El informe concluyó

¹³ Documento de trabajo de los servicios de la Comisión, *Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on the first preliminary review on the implementation of Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services* [«Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la primera revisión preliminar de la aplicación del Reglamento (UE) 2019/1150 relativo a la promoción de la equidad y la transparencia para los usuarios empresariales de servicios de intermediación en línea», documento en inglés] [SWD(2023) 300 final].

que «en la actualidad no se ha[bía] alcanzado todo el potencial del Reglamento (UE) 2019/1150 (Reglamento P2B)». Mientras tanto, comenzó la plena aplicación del Reglamento (UE) 2022/2065 (Reglamento de Servicios Digitales) y el Reglamento (UE) 2022/1925 (Reglamento de Mercados Digitales), que han superado en gran medida las disposiciones del Reglamento P2B.

- **Consultas con las partes interesadas**

Se llevaron a cabo varias consultas durante la preparación de la propuesta. Cada una de ellas se concibió como complementaria de las demás y se centró en distintos ámbitos temáticos o diferentes grupos de partes interesadas.

En la primavera de 2025 se publicaron tres consultas públicas y convocatorias de datos sobre los pilares clave de la propuesta. Del 9 de abril al 4 de junio se llevó a cabo una consulta sobre la Estrategia para la Aplicación de la IA¹⁴, 11 de abril al 20 de junio se llevó a cabo otra consulta sobre la revisión del Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad)¹⁵ y, por último, el 23 de mayo al 20 de julio se llevó a cabo otra consulta sobre la Estrategia de Datos de la Unión Europea¹⁶. Cada cuestionario tenía una sección específica (varias, en ocasiones) sobre cuestiones relativas a la aplicación y simplificación, directamente relacionadas con las reflexiones sobre el paquete Ómnibus Digital. En conjunto, se obtuvieron 718 respuestas únicas en el marco de esta primera ronda de consultas.

Del 16 de septiembre al 14 de octubre de 2025 se publicó, además, una convocatoria de datos sobre el paquete Ómnibus Digital¹⁷. Su objetivo era dar a las partes interesadas la oportunidad de formular observaciones sobre una propuesta consolidada para el ámbito de aplicación del paquete Ómnibus Digital. Se recibieron 513 respuestas, que presentaron diversos grupos de partes interesadas, en particular empresas y asociaciones empresariales, la sociedad civil, el mundo académico, autoridades y contribuciones individuales de los ciudadanos.

La vicepresidenta ejecutiva Henna Virkkunen organizó dos diálogos sobre la aplicación relacionados con los temas clave que aborda el paquete Ómnibus Digital: la primera sobre la política de datos¹⁸ (1 de julio de 2025) y la segunda sobre la política de ciberseguridad¹⁹ (15 de septiembre).

Por su parte, el comisario McGrath organizó un diálogo sobre la aplicación del RGPD el 16 de julio de 2025.

¹⁴ Comisión Europea (2025). *Convocatoria de datos sobre la Estrategia para la Aplicación de la IA*. Disponible en: Aplicación de la estrategia de IA: reforzar el continente de IA.

¹⁵ Comisión Europea (2025). *Convocatoria de datos sobre el Reglamento sobre la Ciberseguridad*. Disponible en: Reglamento sobre la Ciberseguridad de la UE.

¹⁶ Comisión Europea (2025). *Convocatoria de datos sobre la Estrategia de Datos de la Unión Europea*. Disponible en: Estrategia de Datos de la Unión Europea.

¹⁷ Comisión Europea (2025). *Convocatoria de datos sobre el paquete digital y ómnibus*. Disponible en: Simplificación: paquete digital y ómnibus.

¹⁸ Comisión Europea (2025). *Implementation dialogue — data policy* [«Diálogo sobre la aplicación: política de datos», página web en inglés]. Disponible en: Implementation dialogue – data policy - Comisión Europea.

¹⁹ Comisión Europea (2025). *Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen* [«Diálogo sobre la aplicación de la política de ciberseguridad con la vicepresidenta ejecutiva Henna Virkkunen», página web en inglés]. Disponible en: Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen - Comisión Europea.

Los servicios de la Comisión también llevaron a cabo varias «comprobaciones de las situaciones reales», esto es, grupos de debate en profundidad con empresas y representantes de la sociedad civil, organizados entre el 15 de septiembre y el 6 de octubre de 2025, para debatir sobre los retos prácticos de aplicación que se experimentan en el día a día y estimar los costes de cumplimiento.

Con el fin de consultar específicamente a las pymes y recabar sus observaciones, entre el 4 de septiembre y el 16 de octubre de 2025 se organizó un grupo especial de pymes a través de la Red Europea para las Empresas²⁰.

Por último, los servicios de la Comisión recibieron numerosos documentos de síntesis y organizaron reuniones bilaterales con diversas partes interesadas. Los servicios de la Comisión también colaboraron con los Estados miembros en mesas redondas o en el contexto de diversos grupos de trabajo del Consejo.

En general, las observaciones de las partes interesadas coincidieron en cuanto a la necesidad de una aplicación simplificada de algunas de las normas digitales. Las partes interesadas acogieron con satisfacción la atención prestada a la coherencia y la consolidación de las normas, así como a la optimización de los costes de cumplimiento.

Se hizo un claro llamamiento en favor de la racionalización del acervo en materia de datos y la consolidación de las normas. Esto se aborda en la propuesta, junto con modificaciones específicas apoyadas por las partes interesadas, en particular en lo que respecta al RGPD y al hartazgo generado por los anuncios de *cookies*. Además, las empresas han señalado la necesidad de realizar nuevas evaluaciones de la interacción entre las normas en materia de datos, que justifican un análisis más profundo a través de las herramientas de mejora de la legislación, en particular el próximo control de adecuación digital.

Las empresas de diferentes sectores también han señalado las cargas injustificadas que se derivan de la doble notificación de incidentes en múltiples marcos jurídicos. Este llamamiento a la acción se aborda mediante la propuesta de un punto de entrada único para la notificación de incidentes.

Por lo que respecta al Reglamento de Inteligencia Artificial, las partes interesadas han señalado la necesidad de contar con seguridad jurídica en la aplicación de las normas y, en particular, han subrayado la necesidad de disponer de normas y orientaciones antes de aplicar las normas. La propuesta legislativa separada en el marco del paquete Ómnibus Digital aborda sus preocupaciones.

Por último, las partes interesadas no se han pronunciado respecto a las repercusiones del Reglamento sobre las relaciones entre plataformas y empresas, lo que confirma los resultados del informe de evaluación intermedia de que las normas no son bien conocidas ni eficaces para alcanzar su objetivo. El presente Reglamento propone la derogación de las normas sobre las relaciones entre plataformas y empresas, en particular a la luz de su solapamiento con otras normas más recientes.

²⁰ La Red Europea para las Empresas es la mayor red de apoyo del mundo para las pymes, y su gestión corre a cargo de la Agencia Ejecutiva para el Consejo Europeo de Innovación y las Pymes (Eisma) de la Comisión Europea.

En el documento de trabajo de los servicios de la Comisión en apoyo del paquete Ómnibus Digital se ofrece una visión general detallada de estas consultas con las partes interesadas y de cómo se reflejaron en la propuesta.

- **Obtención y uso de asesoramiento especializado**

Además de los flujos de consulta descritos anteriormente, la Comisión se basó principalmente en análisis internos a efectos de la presente propuesta. También se contrataron dos estudios para apoyar el análisis de los capítulos dedicados a los datos de la propuesta. El primero de los estudios se centró en la aplicación del Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) y el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). El segundo estudio, más estrechamente vinculado a la Comunicación sobre la Estrategia de Datos de la Unión Europea (adoptada como parte del mismo paquete de simplificación junto con el Ómnibus Digital), se centró en la evolución de la política de datos relacionada con la IA generativa, el cumplimiento de la normativa y las dimensiones internacionales. Ambos estudios están en fase de finalización y se publicarán en una etapa posterior.

Los servicios de la Comisión también han llevado a cabo un estudio sobre la interacción entre el Reglamento (UE) 2022/2065 (Reglamento de Servicios Digitales) y otros actos legislativos, en particular el Reglamento (UE) 2019/1150 (Reglamento P2B). La Comisión publica, como parte del paquete digital, el informe en el que se describe la interacción entre el Reglamento (UE) 2022/2065 (Reglamento de Servicios Digitales) y otras normas conexas, de conformidad con el requisito del artículo 91 de dicho Reglamento.

- **Evaluación de impacto**

Las modificaciones propuestas en el presente Reglamento son específicas y de carácter técnico. Están concebidas para garantizar una aplicación más eficiente de las normas. No son proclives a múltiples opciones estratégicas susceptibles de ser evaluadas y comparadas de manera significativa y, en consonancia con las directrices para la mejora de la legislación, no están respaldadas por un informe completo de evaluación de impacto.

El documento de trabajo de los servicios de la Comisión adjunto profundiza en la lógica de intervención de las modificaciones y las opiniones de las partes interesadas sobre las diferentes medidas, y presenta el análisis coste-beneficio de las propuestas, en particular el ahorro de costes generado y otros tipos de repercusiones. En muchos casos, se basa en las evaluaciones de impacto correspondientes que se realizaron inicialmente para los distintos actos legislativos.

- **Adecuación regulatoria y simplificación**

El Reglamento propuesto implica una reducción muy importante de la carga para las empresas, así como para las administraciones públicas y los ciudadanos. Las estimaciones iniciales prevén un posible ahorro de al menos 1 000 millones EUR al año, desde el momento de su entrada en vigor, con un ahorro adicional de 1 000 millones EUR en costes puntuales, lo que supone un total de al menos 5 000 millones EUR a lo largo de 3 años de aquí a 2029. También se esperan en gran medida beneficios no cuantificables, en particular derivados de un conjunto simplificado de normas que facilitará la implicación en su aplicación y su cumplimiento. Los cálculos excluyen las oportunidades de negocio creadas a través del enfoque regulador propuesto.

Si bien las pymes ya están exentas, en virtud de una serie de disposiciones de los actos jurídicos modificados en el paquete Ómnibus Digital, se proponen nuevas medidas de apoyo en el ámbito del cambio de proveedor en la nube. En el capítulo dedicado a las normas armonizadas de intercambio de datos, algunas exenciones ya previstas para las pymes se amplían a las pequeñas empresas de mediana capitalización.

La propuesta también es plenamente coherente con el control de adecuación digital de la Comisión, destinado a garantizar la armonización adecuada de las propuestas estratégicas con los entornos digitales. Para más información al respecto, véase el capítulo 4 de la ficha legislativa de financiación y digital adjunta.

- **Derechos fundamentales**

Las modificaciones propuestas apoyan las oportunidades de innovación para las empresas en el mercado único y, de este modo, promueven el derecho a la libertad de empresa en la Unión.

Algunas disposiciones también están relacionadas con la protección y la promoción de otros derechos fundamentales, en particular el derecho a la intimidad y la protección de los datos personales, y se calibraron para conservar el máximo nivel de protección y apoyar a las personas en el ejercicio efectivo de sus derechos, de manera que también se optimicen los costes y se generen nuevas oportunidades de innovación. De este modo, la propuesta sigue estrictamente el principio de proporcionalidad consagrado en el artículo 52 de la Carta de los Derechos Fundamentales de la Unión Europea.

En el caso concreto de las modificaciones específicas del Reglamento (UE) 2016/679 (RGPD) y del Reglamento (UE) 2018/1725, las modificaciones propuestas simplificarían los requisitos para el tratamiento de bajo riesgo, armonizarían determinadas normas y aclararían ciertos conceptos clave del RGPD y del Reglamento (UE) 2018/1725, lo que permitiría a los responsables del tratamiento aplicar políticas de protección de datos más eficaces. Esto les permitiría concentrar sus recursos en actividades más intensivas en datos y de alto riesgo, para las que las medidas de protección de los datos personales son más críticas.

En lo que respecta a la privacidad de las comunicaciones, la propuesta preserva el máximo nivel de protección, incluido el acceso basado en el consentimiento a los equipos terminales. La modificación de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) no altera las protecciones sustantivas, sino que adapta las normas para el tratamiento de datos personales en equipos terminales o procedentes de ellos a las del Reglamento (UE) 2016/679 (RGPD). Las normas sobre la integridad de los equipos terminales con arreglo a la Directiva se mantienen cuando se tratan datos no personales.

4. REPERCUSIONES PRESUPUESTARIAS

Las repercusiones presupuestarias de la creación y el mantenimiento del punto de entrada único para la notificación de incidentes por parte de la ENISA se detallan en la revisión del Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad), como parte de los recursos para la ENISA.

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

No procede.

- **Explicación detallada de las disposiciones específicas de la propuesta**

Modificaciones del Reglamento (UE) 2023/2854 (Reglamento de Datos)

De forma sólida y simplificada, las modificaciones del marco jurídico en materia de datos consolidan en el Reglamento (UE) 2023/2854 (Reglamento de Datos) las disposiciones del Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos). El capítulo I también incluye modificaciones específicas para ajustar las normas actuales del Reglamento (UE) 2023/2854 (Reglamento de Datos).

El artículo 1 aborda las modificaciones del Reglamento (UE) 2023/2854 (Reglamento de Datos) sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828.

En el artículo 1:

El apartado 1 actualiza el ámbito de aplicación del Reglamento (UE) 2023/2854 (Reglamento de Datos), en el que se introducirán nuevos capítulos, tal como se explica más adelante.

El apartado 2 modifica las definiciones y añade otras nuevas.

El apartado 3 crea una nueva norma en virtud del artículo 4, apartado 8, del Reglamento (UE) 2023/2854 (Reglamento de Datos) que permite a los tenedores de datos denegar la revelación de secretos comerciales a un usuario cuando exista un alto riesgo de obtención, utilización o revelación ilícitas a terceros países, o a entidades bajo su control, que estén sujetas a jurisdicciones con protecciones más débiles que las disponibles en la Unión.

El apartado 5 introduce la misma norma para el artículo 5, apartado 11, del Reglamento (UE) 2023/2854 (Reglamento de Datos), relativa a los tenedores de datos que revelan secretos comerciales a terceros.

Los apartados 5 a 19 limitan el ámbito de aplicación del capítulo V de «necesidades excepcionales» únicamente a «emergencias públicas». Se suprimen los artículos 14 y 15, y se crea un nuevo artículo 15 *bis*, que pasa a ser el único artículo aplicable a las solicitudes durante emergencias públicas en el marco del régimen B2G del Reglamento (UE) 2023/2854 (Reglamento de Datos). Las solicitudes pueden presentarse cuando sea necesario para responder a una emergencia pública (artículo 15 *bis*, apartado 2), o para mitigar o apoyar la recuperación tras una emergencia pública (artículo 15 *bis*, apartado 3). Se ajustan en consecuencia las referencias cruzadas, y se simplifica y aclara el lenguaje utilizado. El artículo 1, apartado 21, crea un nuevo artículo 22 *bis* que enmarca el régimen de reclamaciones del capítulo V, unificando disposiciones previamente reiteradas.

Los apartados 20 a 22 incluyen determinadas excepciones al capítulo VI del Reglamento (UE) 2023/2854 (Reglamento de Datos) (cambio entre servicios de tratamiento de datos). En el artículo 31, se introduce un régimen específico menos estricto para los servicios de tratamiento de datos a medida, es decir, los servicios de tratamiento de datos que no están disponibles para la venta y que no funcionarían sin una adaptación previa a las necesidades y al ecosistema del usuario, en los casos en que dichos servicios se presten sobre la base de contratos celebrados antes del 12 de septiembre de 2025. Del mismo modo, en el artículo 31 se introduce un nuevo régimen específico menos estricto para los servicios de tratamiento de

datos prestados por pymes y pequeñas empresas de mediana capitalización sobre la base de contratos celebrados antes del 12 de septiembre de 2025; dicho régimen va acompañado de una aclaración de que estos proveedores pueden incluir sanciones por rescisión anticipada en los contratos de duración determinada.

Los apartados 23 a 25 incluyen modificaciones del artículo 32 del Reglamento (UE) 2023/2854 (Reglamento de Datos) resultantes de la integración de los organismos que actualmente están regulados por el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) en el Reglamento (UE) 2023/2854 (Reglamento de Datos).

El apartado 26 suprime las obligaciones de los proveedores de contratos inteligentes de cumplir determinados requisitos esenciales y faculta a la Comisión para adoptar normas armonizadas.

El apartado 27 integra dos regímenes jurídicos que actualmente están incluidos en el Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos), el cual se deroga una vez que entre en vigor el paquete Ómnibus Digital. Este punto reforma las normas actuales incluidas en los capítulos III y IV del Reglamento relativo a la gobernanza europea de datos, que establecen un régimen obligatorio de notificación para los proveedores de servicios de intermediación de datos, así como un régimen voluntario de inscripción en el registro para las organizaciones de gestión de datos con fines altruistas. Ambos regímenes se añadirán a modo de nuevo capítulo VII *bis* en el Reglamento (UE) 2023/2854 (Reglamento de Datos). A la luz de la naturaleza emergente del mercado de servicios de intermediación de datos, las obligaciones del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) se flexibilizarán para que este mercado crezca. Por un lado, el régimen aplicable a los proveedores de servicios de intermediación de datos se convertirá en un régimen voluntario. Por otro lado, la obligación más crítica, esto es, la obligación de mantener los servicios de intermediación de datos jurídicamente separados de cualquier otro servicio que una empresa pueda ofrecer, se sustituirá por la obligación de mantener los servicios funcionalmente separados, e irá acompañada de un conjunto adicional de condiciones. Por último, la lista de obligaciones se reduce drásticamente. Por lo que respecta a la cesión altruista de datos, se derogan las obligaciones de información y transparencia para las organizaciones de gestión de datos con fines altruistas, así como la idea de completar las normas del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) con un «código normativo sobre la cesión altruista de datos» que incluya normas aún más detalladas.

Introduce un nuevo capítulo VII *ter* en virtud del cual se añade al Reglamento (UE) 2023/2854 (Reglamento de Datos) la prohibición de los requisitos de localización de datos no personales en la Unión, anteriormente incluida en el Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), el cual se deroga. Se mantiene la obligación de informar a la Comisión, pero se suprime el punto único nacional de información en línea en el que los Estados miembros deben publicar los requisitos de localización de datos aplicables.

Los apartados 4 y 33 a 58 introducen las disposiciones unificadas sobre la reutilización de datos y documentos en poder de organismos del sector público en virtud del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos):

- El punto 4 introduce definiciones de las disposiciones introducidas en el Reglamento (UE) 2023/2854 (Reglamento de Datos), que armonizan la definición de datos y documentos mediante el establecimiento de una delimitación rigurosa entre los contenidos digitales (datos) y los no digitales (documentos).
- Introduce el nuevo capítulo VII *quater* sobre la reutilización de los datos y documentos en poder de los organismos del sector público.
- Incluye una nueva sección 1, que introduce los principios generales aplicables al nuevo capítulo.
- Introduce el objeto y el ámbito de aplicación del capítulo unificado, combinando las normas comunes del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Establece el principio común de no discriminación aplicable al intercambio de datos públicos abiertos y determinadas categorías de datos protegidos.
- Establece la prohibición de acuerdos exclusivos, comunes al régimen de datos públicos abiertos y determinadas categorías de datos protegidos.
- Establece principios generales relativos al cobro por la reutilización de datos públicos abiertos o de determinadas categorías de datos protegidos. Como norma nueva, los organismos del sector público tendrán que garantizar que las tasas también puedan pagarse en línea a través de servicios de pago transfronterizos de amplia disponibilidad, sin discriminación por la reutilización de datos públicos abiertos. Esto representa una ampliación de esta norma que anteriormente se aplicaba solo para la reutilización de determinadas categorías de datos protegidos en virtud del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos).
- Establece el derecho de los reutilizadores de datos públicos abiertos y de determinadas categorías de datos protegidos a ser informados de las vías de recurso disponibles en relación con las decisiones o prácticas que les afecten.
- Introduce la sección relativa a las normas para la reutilización de datos públicos abiertos, que anteriormente eran normas con arreglo a la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Determina el ámbito de aplicación de la sección, en particular la no aplicación a determinadas categorías de datos protegidos comprendidos en el ámbito de aplicación del capítulo general sobre la reutilización de datos y documentos en poder de organismos del sector público.
- Establece el principio general para la reutilización de los datos públicos abiertos.
- Establece las normas para la tramitación de las solicitudes de reutilización de datos públicos abiertos e incorpora la disposición anterior de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Introduce las normas relativas a los formatos disponibles para la reutilización de datos públicos abiertos, que anteriormente estaban incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Introduce las normas que rigen el cobro de los datos públicos abiertos, que anteriormente estaban incluidas en la Directiva (UE) 2019/1024 (Directiva sobre

datos abiertos). Como nueva norma, los organismos del sector público podrán cobrar tarifas más elevadas por la reutilización por parte de empresas muy grandes. Dichas tasas deben ser proporcionadas y su importe debe basarse en criterios objetivos.

- Introduce las normas relativas a las licencias tipo para la reutilización de datos públicos abiertos, que anteriormente estaban incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos). Como nueva norma, los organismos del sector público podrán disponer condiciones especiales para las empresas muy grandes. Dichas condiciones deben ser proporcionadas y deben basarse en criterios objetivos.
- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre las disposiciones prácticas que anteriormente estaban incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos), a fin de facilitar la búsqueda de datos o documentos disponibles para su reutilización.
- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre datos de investigación anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre conjuntos de datos de alto valor, anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Crea una nueva sección para la reutilización de determinadas categorías de datos protegidos a fin de incluir en el capítulo las antiguas normas en virtud del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). El punto describe el ámbito de aplicación de esta sección 3, que excluye de dicho ámbito los datos y documentos incluidos en el ámbito de aplicación de la sección 2, que regula el régimen de reutilización de los datos públicos abiertos. Como nueva norma, los documentos se incluyen en el ámbito de aplicación de esta sección.
- Establece el principio general relativo a la reutilización de determinadas categorías de datos protegidos. Este es el principio que se establece en el capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos), según el cual la sección no impone a los organismos del sector público la obligación de permitir la reutilización de datos protegidos, sino que establece las condiciones mínimas en las que los organismos del sector público deciden poner dichos datos a disposición para su reutilización.
- Introduce las normas sobre las condiciones para la reutilización de determinadas categorías de datos protegidos, que anteriormente estaban incluidas en el capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos), de una forma simplificada y racionalizada. Incluye una aclaración sobre qué normas son aplicables en los casos en que los datos personales se hayan anonimizado. Los requisitos relativos a las transferencias de datos no personales a terceros países se mantienen, pero se dividen en un nuevo artículo en el punto 54.
- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre el cobro de tasas, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). Como nueva norma, los organismos del sector público podrán prever tasas más elevadas por la reutilización por parte de empresas muy grandes. Dichas tasas deben ser proporcionadas y deben basarse en criterios objetivos. La consideración especial

de incentivar la reutilización por parte de las pymes se amplía a las pequeñas empresas de mediana capitalización.

- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre los organismos competentes, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). Los organismos competentes están diseñados para ayudar a los organismos del sector público a responder a las solicitudes de reutilización de datos y documentos contemplados en la sección 3.
- Introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre el punto único de información, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos). Los puntos únicos de información están diseñados para ayudar a los reutilizadores a encontrar fácilmente información sobre la reutilización de determinadas categorías de datos protegidos.
- Por último, introduce, en el Reglamento (UE) 2023/2854 (Reglamento de Datos), las normas sobre el procedimiento de solicitud de reutilización de determinadas categorías de datos protegidos, que anteriormente estaban regidas por el capítulo II del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos).

El apartado 57 integra las normas básicas sobre el Comité Europeo de Innovación en materia de Datos, un grupo que asesora a la Comisión sobre la aplicación coherente del Reglamento de Datos y sirve como foro de coordinación para la elaboración de políticas en el ámbito de las políticas de economía de los datos. Este apartado integrará las normas básicas en el Reglamento de Datos. Los cambios permitirán a la Comisión modificar los documentos fundacionales pertinentes del Comité [Decisión de la Comisión de 20 de febrero de 2023 - C(2023) 1074 final] y ampliar el número de miembros para incluir a representantes de la elaboración de políticas nacionales, además de a las autoridades competentes.

Los apartados 61 a 65 contienen modificaciones de las disposiciones del Reglamento (UE) 2023/2854 (Reglamento de Datos) sobre el procedimiento de comité y el ejercicio de la delegación, y el apartado 66 introduce las modificaciones necesarias del Reglamento (UE) 2022/868 (Reglamento relativo a la gobernanza europea de datos) para incorporar las normas de dicho Reglamento y de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) en el Reglamento (UE) 2023/2854 (Reglamento de Datos).

El apartado 68 amplía la atención especial prestada a las pymes en el contexto de la evaluación a las pequeñas empresas de mediana capitalización y el apartado 69 introduce la evaluación de las normas recientemente introducidas en el Reglamento (UE) 2023/2854 (Reglamento de Datos).

El **artículo 2** introduce en el Reglamento (UE) 2018/174, en el anexo relativo a la «puesta en marcha, gestión y cierre de una empresa», las referencias pertinentes a los servicios de intermediación de datos y a la cesión altruista de datos.

Modificaciones de los Reglamentos (UE) 2016/679 y (UE) 2018/1725, y de la Directiva 2002/58/CE

El artículo 3 de la propuesta introduciría modificaciones específicas en el Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

En el artículo 3:

El apartado 1 aclararía la definición de datos personales con arreglo al artículo 4 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) al establecer que, para una entidad determinada, la información no debe considerarse datos personales cuando dicha entidad no disponga de medios que puedan utilizarse razonablemente para identificar a la persona física a la que se refiere la información. En consecuencia, dicha entidad no entraría, en principio, en el ámbito de aplicación de dicho Reglamento.

El apartado 2 establecería dos exenciones adicionales al tratamiento de categorías especiales de datos: Establecería una excepción de la prohibición general del tratamiento de datos biométricos cuando este sea necesario para confirmar la identidad del interesado y cuando los datos y medios para dicha verificación estén bajo el control exclusivo del interesado. También establecería una excepción para el tratamiento residual de categorías especiales de datos personales para el desarrollo y la explotación de un sistema o modelo de IA, siempre que se cumplan determinadas condiciones, entre ellas, ciertas medidas organizativas y técnicas adecuadas para evitar la recogida de categorías especiales de datos personales y la eliminación de dichos datos.

El apartado 3 aclararía la situación prevista en el artículo 12 del Reglamento (UE) 2016/679 (RGPD) en los casos en que el derecho de acceso es ejercido de forma abusiva por los interesados con fines distintos de la protección de sus datos personales. Como resultado de ello, el responsable del tratamiento podría negarse a atender la solicitud o cobrar una tasa razonable. Además, aclararía las condiciones para demostrar que una solicitud de acceso era excesiva.

El apartado 4 se centraría en la obligación del responsable del tratamiento de informar a los interesados sobre el tratamiento de sus datos personales en virtud del artículo 13 del Reglamento (UE) 2016/679 (RGPD), eliminando esta obligación en situaciones en las que existan motivos razonables para suponer que el interesado ya dispone de la información, salvo que el responsable del tratamiento comunique los datos a otros destinatarios o categorías de destinatarios, transfiera los datos a un tercer país, lleve a cabo decisiones automatizadas o sea probable que el tratamiento entrañe un alto riesgo para los derechos del interesado.

El apartado 5 aclararía los requisitos para las decisiones individuales automatizadas en virtud del artículo 22 del Reglamento (UE) 2016/679 (RGPD), en el contexto de la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento, en particular que el requisito de «necesidad» se aplica independientemente de si la decisión puede adoptarse por medios distintos de los meramente automatizados.

El apartado 6 armonizaría la obligación del responsable del tratamiento de notificar las violaciones de la seguridad de los datos a la autoridad de control competente en virtud del artículo 33 del Reglamento (UE) 2016/679 (RGPD) con su obligación de notificar dichas violaciones a los interesados, estipulando que la notificación solo es necesaria si es probable que una violación de la seguridad de los datos entrañe un alto riesgo para los derechos del interesado. También ampliaría el plazo de notificación a noventa y seis horas. También se incluye la propuesta de que los responsables del tratamiento utilicen el punto de entrada único cuando notifiquen violaciones de la seguridad de los datos a la autoridad de control. Además, el Comité Europeo de Protección de Datos (CEPD) estaría obligado a elaborar y presentar a la Comisión una propuesta de modelo común para las notificaciones de violaciones de la seguridad de los datos, que la Comisión estaría facultada para adoptar, tras revisarlo, mediante un acto de ejecución, en caso de que fuera necesario.

El apartado 7 armonizaría las listas de actividades de tratamiento que requieren y no requieren una evaluación de impacto relativa a la protección de datos estableciendo que se faciliten a escala de la UE listas únicas de operaciones de tratamiento que requieren y no requieren dicha evaluación, contribuyendo así a la armonización del concepto de «alto riesgo». El CEPD estaría obligado a preparar una serie de propuestas para estas listas. También estaría obligado a elaborar una propuesta de modelo y metodología comunes para la realización de evaluaciones de impacto relativas a la protección de datos, que la Comisión estaría facultada para adoptar, tras revisarlas, mediante un acto de ejecución, en caso de ser necesario.

El apartado 8 establece que la Comisión puede apoyar, junto con el CEPD, a los responsables del tratamiento a la hora de evaluar si los datos resultantes de la seudonimización no constituyen datos personales, a través de la especificación de los medios y criterios pertinentes para dicha evaluación, en particular el estado actual de las técnicas disponibles y los criterios para evaluar el riesgo de reidentificación.

El apartado 12 reforma el régimen jurídico sobre el tratamiento de datos personales en equipos terminales o procedentes de ellos («dispositivos conectados»), que actualmente forma parte de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas). Se añade un nuevo artículo 88 *bis* en el Reglamento (UE) 2016/679 (RGPD), que establece el requisito de consentimiento para el almacenamiento o el acceso a los datos personales en los equipos terminales de las personas físicas, y que incorpora el tratamiento de datos personales en equipos terminales o procedentes de ellos a las normas del Reglamento (UE) 2016/679 (RGPD). Se añade un nuevo artículo 88 *ter* al Reglamento (UE) 2016/679 (RGPD), relativo a las indicaciones automatizadas y de lectura mecanizada de las preferencias individuales y el respeto de dichas indicaciones por parte de los proveedores de sitios web una vez que las normas estén disponibles.

En el artículo 4:

El artículo 4 de la propuesta introduciría modificaciones específicas en el Reglamento (UE) 2018/1725, con el fin de adaptar su redacción a las modificaciones del Reglamento (UE) 2016/679 introducidas en el artículo 3.

En el artículo 5:

El artículo 5 prevé modificaciones de la Directiva 2002/58/CE («Directiva sobre la privacidad y las comunicaciones electrónicas»). Queda derogado el artículo 4 de dicha Directiva. La adición al artículo 5, apartado 3, de dicha Directiva, mediante la inclusión de un nuevo artículo 88 *bis* del Reglamento (UE) 2016/679 (RGPD), tal como se ha descrito anteriormente, permite trasladar al RGPD las normas sobre el almacenamiento y el acceso a los datos personales del equipo terminal de una persona física.

Punto de entrada único para la notificación de incidentes

En el artículo 6:

En los apartados 1 y 2, se establece el punto de entrada único para la notificación de incidentes, mediante la inclusión de requisitos específicos para la ENISA. Además, se establece que la notificación de incidentes exigida en virtud de la Directiva SRI 2 debe realizarse a través del nuevo punto de entrada único.

En el artículo 7: el punto de entrada único también es obligatorio para la notificación de incidentes con arreglo al Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).

En el artículo 8: también se establece el uso obligatorio del punto de entrada único para el Reglamento (UE) 2022/2554 (Reglamento sobre Resiliencia Operativa Digital).

En el artículo 9: se establece el uso obligatorio del punto de entrada único también para la Directiva (UE) 2022/2557 (Directiva REC).

Además, el artículo 3, apartado 6, también establece la obligación de que la notificación de incidentes relacionados con violaciones de la seguridad de los datos contemplada en el Reglamento (UE) 2016/679 (RGPD) se canalice a través del punto de entrada único. En el artículo 5, apartado 1, se derogan los requisitos de notificación en virtud de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), ya que están obsoletos a la vista de las disposiciones del Reglamento (UE) 2016/679 (RGPD).

Derogaciones de actos legislativos y disposiciones finales

En el artículo 10:

El apartado 1 deroga el Reglamento (UE) 2019/1150 (Reglamento P2B), que se considera ahora de importancia residual a la vista de las normas recientes que contemplan en gran medida las mismas cuestiones. No obstante lo anterior, el apartado 2 aborda las referencias cruzadas al Reglamento (UE) 2019/1150 (Reglamento P2B) en otros instrumentos jurídicos: estas seguirán en vigor hasta que se modifiquen en sus actos legislativos originales, a más tardar el 31 de diciembre de 2032, con el fin de evitar cualquier inseguridad jurídica.

El apartado 3 deroga los textos jurídicos incorporados al Reglamento (UE) 2023/2854 (Reglamento de Datos).

El **artículo 11** establece las disposiciones finales del Reglamento que introduce las modificaciones.

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Ómnibus Digital)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo²¹,

Visto el dictamen del Banco Central Europeo²²,

Visto el dictamen del Comité de las Regiones²³,

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

- (1) En su Comunicación sobre una Europa más sencilla y rápida²⁴, la Comisión anunció su compromiso con un ambicioso programa para promover políticas innovadoras y con visión de futuro que refuercen la competitividad de la Unión y alivien radicalmente la carga normativa para las personas, las empresas y las administraciones, manteniendo al mismo tiempo el máximo nivel en la promoción de los valores de la Unión. Por consiguiente, la Comisión dio prioridad a la propuesta de realizar ajustes inmediatos de la legislación, en particular la legislación digital, para abordar el reto de la competitividad de la Unión.

²¹ DO C [...], [...], p. [...].

²² DO C [...], [...], p. [...].

²³ DO C [...], [...], p. [...].

²⁴ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones titulada «Una Europa más sencilla y rápida: Comunicación sobre la aplicación y la simplificación» [COM(2025) 47 final], 11 de febrero de 2025.

- (2) La legislación digital de la Unión establece un nivel elevado de exigencia en la UE y puede ser una poderosa fuente de ventaja competitiva para las empresas que cumplen las normas, ya que constituye una marca líder de calidad, seguridad y fiabilidad de referencia mundial. La normativa digital ha enmarcado las reglas claras del juego en la Unión para las empresas responsables, garantizando la equidad y la transparencia en las relaciones entre empresas, estimulando modelos de negocio innovadores y estableciendo un alto nivel de protección y seguridad de los consumidores, así como para la protección de los derechos fundamentales, en particular la privacidad y la protección de datos.
- (3) La legislación digital de la Unión ha evolucionado gradualmente en los últimos años, en respuesta al rápido aumento de la huella de las tecnologías digitales en la economía y la dinámica social de la Unión, y con vistas a abordar los retos emergentes y promover las oportunidades de negocio en la UE. A pesar del compromiso de la Comisión de llevar a cabo una «prueba de resistencia» sistemática de las normas digitales, junto con otras normas de la Unión, que podría dar lugar a nuevos ajustes normativos, en particular tras el próximo control de adecuación digital, así como otras evaluaciones específicas de las normas digitales, son necesarios cambios reglamentarios inmediatos. Por consiguiente, el presente Reglamento propone un primer conjunto de modificaciones del marco legislativo digital, destinadas a proporcionar aclaraciones normativas inmediatas que estimulen la innovación en el mercado de la Unión y que reduzcan los costes administrativos relacionados con el cumplimiento, en particular para las empresas, así como también a racionalizar los costes administrativos y de supervisión para las autoridades de supervisión y los órganos consultivos. Las modificaciones también pretenden aportar claridad a las personas.
- (4) Dado el papel fundacional de los datos a la hora de impulsar la creación de valor en la economía digital, y de conformidad con los objetivos de la Comunicación relativa a una Estrategia de Datos de la Unión Europea, las modificaciones que presenta este Reglamento para el marco legislativo relativo a los datos tienen por objeto establecer un marco regulador coherente y cohesivo para la disponibilidad y el uso de los datos, racionalizando y consolidando dicho marco regulador en solo dos actos jurídicos, a saber, los Reglamentos (UE) 2016/679²⁵ y (UE) 2023/2854²⁶ del Parlamento Europeo y del Consejo, de los cinco actos aplicables actualmente. Las modificaciones tienen por objeto reducir los costes administrativos innecesarios y fomentar la disponibilidad de datos como requisito previo para apoyar a las empresas digitales competitivas en la Unión, manteniendo al mismo tiempo el máximo nivel de protección de la privacidad, los datos personales y las prácticas comerciales justas, y garantizando los objetivos normativos fundamentales, en particular el cumplimiento de la legislación nacional y de la UE en materia de competencia.

²⁵ 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)

²⁶ REGLAMENTO (UE) 2023/2854 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).

- (5) Reconociendo la evolución iterativa de las normas horizontales y sectoriales, es fundamental abordar también los solapamientos en disposiciones específicas que dan lugar a duplicaciones innecesarias de cargas administrativas. Este es el caso de los requisitos establecidos en varias normas para la notificación tras incidentes de ciberseguridad y relacionados, en los que las soluciones digitales, tal como se propone en el presente Reglamento, pueden aportar un alivio inmediato a las empresas de todos los sectores afectados.
- (6) Del mismo modo, con la regulación iterativa de las plataformas en línea en los últimos años, las normas más recientes han establecido un marco más claro y ambicioso que algunas de las normas anteriores, lo que ha hecho que queden obsoletas. Por lo tanto, es necesario que el marco jurídico evolucione, eliminando cualquier duplicación innecesaria que añada complejidad jurídica.
- (7) El Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo²⁷ ha establecido normas para las funciones de intermediación en tres contextos diferentes: a) funciones que apoyen la reutilización de datos protegidos que obren en poder de organismos del sector público en condiciones controladas; b) servicios de intermediación de datos que faciliten el intercambio de datos entre los interesados, los tenedores de datos y los usuarios de datos; y c) organizaciones de gestión de datos con fines altruistas que apoyen el uso de los datos facilitados por los interesados y los tenedores de datos con fines altruistas o filantrópicos. Las funciones de apoyo a la reutilización de datos protegidos en poder del sector público están estrechamente relacionadas con las normas de la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo²⁸. Su interacción ha generado confusión, en particular entre los organismos del sector público. Por lo tanto, es necesario unificar ambos conjuntos de normas. La evaluación de las normas sobre servicios de intermediación de datos ha puesto de manifiesto que la definición de proveedores de servicios de intermediación de datos presenta deficiencias y que las normas son excesivamente estrictas para que los proveedores de servicios encuentren un modelo financiero sostenible. Por ello, también es preciso optimizar el régimen. Con respecto a la cesión altruista de datos, algunas normas del Reglamento (UE) 2022/868, en particular la obligación de que los Estados miembros dispongan de políticas nacionales en materia de cesión altruista de datos, el establecimiento de un «código normativo» y el desarrollo de un formulario europeo de consentimiento para la cesión altruista de datos, parecen constituir una regulación innecesaria, también a la luz de los trabajos en curso del Comité Europeo de Protección de Datos a que se refiere el artículo 68 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo²⁹, relativo a las directrices sobre el tratamiento de datos personales en el contexto de la investigación científica.

²⁷ Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1), ELI: <http://data.europa.eu/eli/reg/2022/868/oj>.

²⁸ Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (DO L 172 de 26.6.2019, p. 56, ELI: <http://data.europa.eu/eli/dir/2019/1024/oj>).

²⁹ 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

- (8) Si bien se reconoce la importancia de los servicios de intermediación de datos en el contexto de numerosas iniciativas de apoyo al intercambio y la colaboración en materia de datos, deben aclararse las normas del Reglamento (UE) 2022/868 sobre los proveedores de servicios de intermediación de datos. En particular, la definición de tales proveedores debe ser más precisa. Deben eliminarse elementos que solo sirven de ejemplos ilustrativos, en lugar de excepciones. Además, deben abordarse las lagunas resultantes de formulaciones ambiguas, en particular en lo que se refiere al concepto de «grupo cerrado». Los servicios no deben poder registrarse como servicios de intermediación de datos cuando los utilice exclusivamente un grupo cerrado de empresas y cuando cualquier ampliación de dicho grupo de empresas solo pueda ser decidida por el propio grupo y no por el proveedor de servicios. Lo que es más importante, someter este mercado emergente a un régimen obligatorio ha generado costes de cumplimiento innecesarios. En esta fase de desarrollo del mercado, parece suficiente un régimen voluntario que permita a los operadores neutrales distinguirse de otros operadores. Asimismo, a fin de permitir modelos de negocio sostenibles, el régimen debe flexibilizarse suprimiendo el requisito de una separación legal entre los servicios de intermediación de datos y otros servicios de valor añadido que un servicio pueda ofrecer, sustituyéndola por una separación funcional, manteniendo al mismo tiempo ciertas salvaguardias. El régimen de control administrativo debe simplificarse. En lugar de un registro público nacional y otro de la Unión para los proveedores de servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas, solo deberían existir registros públicos de la Unión, a saber, uno para los proveedores de servicios de intermediación de datos y otro para las organizaciones de gestión de datos con fines altruistas. Las autoridades competentes que supervisen la concesión de la etiqueta y el cumplimiento por parte de las entidades de los requisitos para obtenerla deben ser independientes en esta tarea. Esto debe entenderse en el sentido de que deben ser jurídica y funcionalmente independientes de un servicio de intermediación de datos o de una organización de gestión de datos con fines altruistas, en particular a nivel de sus directivos de alto nivel. Las organizaciones gubernamentales deben poder apoyar financieramente a los servicios de intermediación de datos o las organizaciones de gestión de datos con fines altruistas, en particular dada la naturaleza emergente de estas entidades, siempre que sean entidades jurídicamente independientes. A fin de garantizar que las entidades reconocidas sean fácilmente identificables en toda la Unión, la Comisión estableció el Reglamento de Ejecución (UE) 2023/1622 sobre el diseño de logotipos comunes para identificar a los proveedores de servicios de intermediación de datos y a las organizaciones de gestión de datos con fines altruistas reconocidos en la Unión.
- (9) El Reglamento (UE) 2023/2854 elimina los obstáculos al acceso a los datos y al uso de los mismos, impulsa la innovación y la competitividad basadas en los datos y protege los incentivos de quienes invierten en tecnologías de datos.
- (10) El capítulo II del Reglamento (UE) 2023/2854 exige a los tenedores de datos que pongan los datos, entre ellos los datos protegidos como secretos comerciales, a

circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DO L 119 de 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

disposición de los usuarios y de los terceros que estos seleccionen, siempre que se mantengan las medidas de confidencialidad establecidas por el tenedor de datos. Este requisito de mantener la confidencialidad completa la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo³⁰, que establece la norma para la protección de los secretos comerciales dentro de la Unión. Sin embargo, la revelación de secretos comerciales a entidades de terceros países puede aumentar los riesgos para su integridad y confidencialidad cuando exista exposición a jurisdicciones con protecciones inadecuadas o dificultades en su aplicación efectiva, lo que podría dar lugar a un uso no autorizado, daños económicos e inseguridad jurídica.

- (11) Es necesario reforzar el Reglamento (UE) 2023/2854 mediante la introducción de un motivo adicional para que los tenedores de datos denieguen la revelación de secretos comerciales, que complete las disposiciones existentes que permiten la denegación sobre la base de la demostración por parte del tenedor de datos de una alta probabilidad de perjuicio económico grave. En virtud de la nueva disposición, los tenedores de datos podrán negarse a revelar secretos comerciales si demuestran un alto riesgo de obtención, utilización o revelación ilícitas a entidades sujetas a regímenes de protección inadecuada, no equivalentes o marcos jurídicos menos efectivos que las normas aplicables de la Unión. La nueva disposición también abarca los casos en los que el marco jurídico del tercer país, en teoría, es sólido o supera las normas de la Unión, pero carece de una aplicación adecuada en la práctica. Estos riesgos ponen de manifiesto la posibilidad de que los secretos comerciales se adquieran, utilicen o revelen infringiendo el Derecho de la Unión, lo que amenaza la integridad y confidencialidad de los secretos comerciales.
- (12) La activación del mecanismo de denegación debe seguir siendo voluntaria, y la demostración solo debe hacerse tras su activación. No debe exigirse a los tenedores de datos que lleven a cabo un análisis o demostraciones a gran escala del nivel de protección de los secretos comerciales en terceros países o por parte de una entidad de un tercer país como condición previa para poder justificar su negativa a compartir datos o a revelar secretos comerciales. En su demostración, los tenedores de datos pueden tener en cuenta diversos factores, como normas jurídicas insuficientes o inadecuadas, una aplicación deficiente o arbitraria, infracciones históricas, obligaciones extranjeras de revelación que entren en conflicto con el Derecho de la Unión, recursos o vías de recurso limitados para las entidades de la Unión, el uso estratégico indebido de tácticas procesales para debilitar a los competidores o influencia política indebida. Dada la diversidad de entidades, terceros países y escenarios de intercambio de datos implicados, los tenedores de datos deben centrar su evaluación y demostración en los riesgos pertinentes y actuar en consecuencia, en particular estableciendo salvaguardias adecuadas o activando el mecanismo de denegación. Las denegaciones deben ser claras, proporcionadas y adaptadas a las circunstancias específicas de cada caso, en lugar de aplicarse de manera sistemática o generalizada en todo un tercer país.

³⁰ Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

- (13) Una protección insuficiente de los secretos comerciales y los retos a la hora de hacerlos cumplir en terceros países pueden causar un perjuicio irreparable a las empresas europeas. Por lo tanto, el objetivo es reforzar las salvaguardias para los secretos comerciales evitando su filtración hacia personas físicas o jurídicas establecidas en jurisdicciones que entrañen tales riesgos o que estén sujetas a esas jurisdicciones. Esto incluye a las entidades con sede en la Unión controladas por entidades de terceros países, que pueden actuar de mala fe o como frentes para entidades de terceros países. Además, el objetivo es evitar la exposición directa a entidades de terceros países que operan en la Unión y que están sujetas a dichas jurisdicciones. Estar sujeta a la jurisdicción de un tercer país significa que la persona física o jurídica está jurídicamente regida, controlada o, de otro modo, vinculada por las leyes o la autoridad reguladora de un tercer país. Las filiales de empresas matrices de terceros países pueden explotar estas jurisdicciones para eludir o evadir la legislación de la Unión. El control directo o indirecto se refiere a la capacidad de ejercer una influencia decisiva o dominante sobre la gestión o las decisiones estratégicas de otra entidad, ya sea a través de la propiedad del capital o de los derechos de voto, la participación financiera, acuerdos contractuales o entidades intermediarias. El control puede ejercerse directamente o por otros medios, incluso sin participación mayoritaria. Los tenedores de datos deben hacer todo lo posible por obtener la información pertinente, lo que puede incluir búsquedas en registros públicos o solicitarla directamente al usuario o tercero, garantizando al mismo tiempo que el proceso no resulte indebidamente intrusivo.
- (14) La protección de los secretos comerciales frente a estas vulnerabilidades es esencial para que las industrias europeas mantengan su posición en el mercado y su ventaja competitiva. Si bien los tenedores de datos pueden ejercer su discrecionalidad a la hora de proteger sus secretos comerciales, la negativa a compartir datos debe limitarse a circunstancias excepcionales y justificadas, a fin de preservar los objetivos del Reglamento (UE) 2023/2854 de fomentar la innovación basada en los datos y una economía digital próspera en la Unión. Deben mantenerse las salvaguardias contra el uso indebido del mecanismo de denegación, en particular la obligación del tenedor de datos de demostrar, de manera debidamente justificada, que la revelación entraña un alto riesgo y de notificar esta circunstancia a las autoridades competentes. Esta demostración debe facilitarse por escrito sin demora indebida al usuario o a un tercero y ser proporcionada al caso en cuestión. Todas las partes implicadas deben tratar la decisión y la demostración de apoyo como reservados con el fin de mantener el carácter confidencial de los secretos comerciales en cuestión. Los usuarios y terceros, según el caso, podrán impugnar la decisión del tenedor de datos ante la autoridad competente, ante los tribunales o a través de organismos de resolución de litigios.
- (15) Para simplificar el marco de intercambio de datos entre empresas y administraciones públicas en virtud del Reglamento (UE) 2023/2854 y aclarar ambigüedades que anteriormente imponían obligaciones de mayor alcance a las empresas, es necesario restringir el ámbito de aplicación del capítulo V de dicho Reglamento de «necesidad excepcional» a «emergencia pública». El concepto de «emergencia pública», que se define en el artículo 2, apartado 29, del Reglamento (UE) 2023/2854, garantiza, por tanto, que las obligaciones establecidas en dicho capítulo se invoquen únicamente en situaciones urgentes y bien definidas, reduciendo de esta manera los retos técnicos, administrativos y jurídicos a los que se enfrentaban las empresas en el marco del anterior régimen. Esto garantizaría que las solicitudes de datos fueran pertinentes y proporcionadas para responder a las emergencias públicas, mitigarlas o apoyar la recuperación posterior. Dado que el marco actualizado de la Unión relativo a las

estadísticas europeas con arreglo al Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo³¹ no aborda las emergencias públicas, es fundamental conservar el papel de las estadísticas oficiales en virtud del capítulo V del Reglamento (UE) 2023/2854 para garantizar la claridad y la eficacia en tales situaciones. También es necesario aclarar el régimen de compensación para las situaciones en las que las microempresas y las pequeñas empresas están obligadas a facilitar datos para hacer frente a una emergencia pública, en cuyo caso dichas empresas pueden reclamar una compensación.

- (16) Con el fin de mitigar las incertidumbres jurídicas que podrían desalentar los modelos de negocio innovadores, es necesario abordar las importantes ambigüedades y cargas de cumplimiento asociadas a las disposiciones relativas a los contratos inteligentes para la ejecución de acuerdos de intercambio de datos en virtud del artículo 36 del Reglamento (UE) 2023/2854. La ausencia de normas armonizadas y de definiciones claras para conceptos clave como «solidez», «control de acceso» y «coherencia con las condiciones del acuerdo», junto con el requisito de «un mecanismo que permita [...] poner fin a la operación o interrumpirla» potencialmente incompatible con arquitecturas descentralizadas o públicas de cadena de bloques basadas en libros mayores inmutables, planteaba retos a los innovadores desde una perspectiva de costes y oportunidades. Además, la ambigüedad en torno a la realización de una evaluación de conformidad con arreglo al artículo 36, apartado 2, de dicho Reglamento corre el riesgo de imponer cargas desproporcionadas. Por lo tanto, la eliminación del artículo 36 del Reglamento (UE) 2023/2854 fomentaría el desarrollo y la introducción en el mercado de nuevos modelos de negocio, favorecería la innovación y reduciría los obstáculos para las tecnologías emergentes.
- (17) Algunos servicios de tratamiento de datos, que no entran en el modelo de prestación de infraestructura como servicio (IaaS, por sus siglas en inglés), están hechos a la medida de las necesidades o del ecosistema de un cliente. La prestación de esos servicios de tratamiento de datos se basa en negociaciones precontractuales y contractuales que se dilatan mucho en el tiempo para determinar los requisitos específicos del cliente y los consiguientes esfuerzos técnicos para personalizar el servicio de tratamiento de datos y ofrecer una solución personalizada. Se trata de servicios que no están disponibles para la venta y que se personalizan de acuerdo con las necesidades de un cliente para ofrecer una solución a medida en la que el proveedor ha adaptado la mayoría de las características y funciones del servicio de tratamiento de datos a las necesidades específicas del cliente, lo que implica otro cliente no podría utilizar la mayoría de las características y funciones sin una adaptación previa por parte del proveedor. Estos servicios difieren de los servicios de tratamiento de datos a medida a que se refiere el artículo 31, apartado 1, del

³¹ Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164, ELI: <http://data.europa.eu/eli/reg/2009/223/oj>).

Reglamento (UE) 2023/2854. Los servicios de tratamiento de datos a medida son servicios en los que la mayoría de las características principales se han creado a medida para satisfacer las necesidades específicas de un cliente o en los que dichos servicios de tratamiento de datos no se ofrecen a gran escala comercial a través del catálogo de servicios del proveedor. Para evitar costes y cargas administrativas adicionales relacionados con la necesidad de reabrir y renegociar los contratos celebrados antes del 12 de septiembre de 2025 o en esa fecha, es necesario aclarar que, con la excepción de la obligación de reducir y, en última instancia, eliminar los costes por cambio y los costes de salida de datos, los servicios a medida prestados con arreglo a contratos celebrados antes del 12 de septiembre de 2025 o en esa fecha no deben entrar en el ámbito de aplicación del capítulo VI del Reglamento (UE) 2023/2854.

- (18) Por razones relacionadas con la planificación financiera y la atracción de inversiones, los proveedores de servicios de tratamiento de datos, especialmente las pymes y las pequeñas empresas de mediana capitalización, pueden preferir contratos de duración determinada y ofrecerlos. Es necesario aclarar que los proveedores de servicios de tratamiento de datos pueden incluir disposiciones relativas a sanciones proporcionadas por rescisión anticipada en dichos contratos, siempre que no constituyan un obstáculo para el cambio de proveedor. Además, los proveedores de servicios de tratamiento de datos que son pymes o pequeñas empresas de mediana capitalización se ven especialmente lastrados por la necesidad de ajustar los contratos existentes para la prestación de servicios de tratamiento de datos al Reglamento (UE) 2023/2854. Por lo tanto, es necesario establecer un régimen específico para dichos proveedores si prestan servicios de tratamiento de datos distintos de IaaS, sobre la base de contratos celebrados antes del 12 de septiembre de 2025 o en esa fecha. Teniendo en cuenta el objetivo del Reglamento (UE) 2023/2854 de permitir el cambio entre servicios de tratamiento de datos y dado que los costes por cambio de proveedor, en particular los costes de salida de datos, constituyen un grave obstáculo al cambio, los nuevos regímenes más flexibles para los servicios de tratamiento de datos a medida o prestados por pymes o pequeñas empresas de mediana capitalización no deben socavar la retirada gradual de dichos costes. Debe considerarse que nunca han existido disposiciones contractuales contrarias a dicho objetivo si están incluidas en acuerdos contractuales sobre la prestación de servicios comprendidos en el ámbito de aplicación de esos dos nuevos regímenes específicos.
- (19) El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo³² introdujo un principio clave para apoyar la economía de los datos en la Unión, respaldando de manera concreta la libertad de establecimiento y la libre prestación de servicios. La «libre circulación de datos» en la Unión, que quedó aclarada mediante la prohibición de imponer la localización de datos, sigue siendo un principio fundamental que proporciona seguridad jurídica a las empresas, por lo que debe mantenerse en el Reglamento (UE) 2023/2854. La disposición no afecta al tratamiento de datos en la

³² Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DO L 303 de 28.11.2018, p. 59, ELI: <http://data.europa.eu/eli/reg/2018/1807/oj>).

medida en que se lleve a cabo en el marco de una actividad que no entre en el ámbito de aplicación del Derecho de la Unión, en particular en lo que respecta a la seguridad nacional, de conformidad con el artículo 4 del Tratado de la Unión Europea (TUE). Al mismo tiempo, otras disposiciones del Reglamento (UE) 2018/1807 se sustituyen por normas más recientes. En particular, el capítulo VI del Reglamento (UE) 2023/2854 introdujo un marco jurídico horizontal moderno que abordaba el cambio entre servicios de tratamiento de datos y dejó prácticamente obsoleto el artículo 6 del Reglamento (UE) 2018/1807. La coexistencia de estas disposiciones ha aumentado la complejidad jurídica para las empresas. Por consiguiente, procede derogar el Reglamento (UE) 2018/1807.

- (20) El concepto de «seguridad pública», en el sentido del artículo 52 del TFUE y según la interpretación del Tribunal de Justicia, abarca la seguridad interna y externa de un Estado miembro, así como cuestiones de orden público, para, en particular, permitir la investigación, detección y enjuiciamiento de infracciones penales. Presupone la existencia de una amenaza real y suficientemente grave que afecte a uno de los intereses fundamentales de la sociedad, tales como una amenaza al funcionamiento de las instituciones y los servicios públicos esenciales y la supervivencia de la población, así como el riesgo de una perturbación grave de las relaciones exteriores o la coexistencia pacífica de las naciones, o un riesgo para los intereses militares. De conformidad con el principio de proporcionalidad, los requisitos de localización de datos justificados por motivos de seguridad pública deben ser adecuados al objetivo perseguido, y no deben ir más allá de lo que sea necesario para alcanzar dicho objetivo.
- (21) Tanto la Directiva (UE) 2019/1024 como el capítulo II del Reglamento (UE) 2022/868 regulan la reutilización de la información del sector público con fines de innovación. La interacción de ambos conjuntos de normas ha creado inseguridad jurídica, principalmente para los organismos del sector público. Por lo tanto, es necesaria una armonización de las normas en un único instrumento jurídico con el fin de aportar una mayor coherencia y seguridad jurídicas.
- (22) Dado que tanto la Directiva (UE) 2019/1024 como el Reglamento (UE) 2022/868 comparten el objetivo de mejorar la reutilización de la información del sector público, y con el fin de simplificar las normas tanto desde la perspectiva de los organismos del sector público como de los reutilizadores de la información del sector público, procede derogar la Directiva (UE) 2019/1024 y el Reglamento (UE) 2022/868, armonizar ambos regímenes y consolidar las normas en un único capítulo en virtud del presente Reglamento. Esta solución aumentará la armonización de dichas normas en toda la Unión, reducirá la carga administrativa asociada a la interpretación y aplicación de la legislación nacional y facilitará a las empresas el desarrollo de servicios y productos transfronterizos. Al designar los organismos competentes, los Estados miembros deben velar por que, incluso cuando se designen organismos competentes sectoriales, todos los sectores pertinentes queden cubiertos en última instancia. Debe entenderse que las modificaciones del presente Reglamento no alteran la interpretación de las diferentes definiciones y términos, salvo que se especifique claramente.
- (23) Los datos y documentos susceptibles de ser puestos a disposición del público para su reutilización, y los datos y documentos que están protegidos por motivos de confidencialidad comercial, en particular secretos comerciales, profesionales y empresariales, secreto estadístico, protección de los derechos de propiedad intelectual de terceros o protección de los datos personales, suelen estar en poder de los mismos organismos del sector público. Por tanto, es necesario armonizar las definiciones y los

principios comunes aplicables a toda la información del sector público y abordar las cuestiones relativas a la interacción de los dos conjuntos de normas.

- (24) Las normas existentes deben simplificarse para aumentar la claridad y la coherencia. No obstante, los dos regímenes de reutilización deben seguir siendo distintos y su respectivo ámbito de aplicación debe seguir dependiendo de las características de los datos o documentos y del contexto de su reutilización. Los organismos del sector público deben aplicar el régimen de datos abiertos siempre que sea posible. Solo cuando determinen que los datos o un documento contienen información que corresponde a determinadas categorías de datos protegidos deberán limitar su disponibilidad pública y valorar ponerlos a disposición para su reutilización como datos protegidos.
- (25) Las empresas emergentes, las pequeñas empresas y las empresas que se consideran medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión³³ y las empresas de sectores con capacidades digitales menos desarrolladas tienen dificultades para reutilizar datos y documentos. Al mismo tiempo, en la economía digital han surgido varias empresas muy grandes con un poder económico considerable gracias a la acumulación y agregación de grandes volúmenes de datos y a la infraestructura tecnológica necesaria para su monetización. Estas empresas muy grandes incluyen empresas que prestan servicios básicos de plataforma y que están designadas como guardianes de acceso en virtud del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo³⁴ y están sujetas a obligaciones especiales para hacer frente a los desequilibrios. Para hacer frente a estos desequilibrios y reforzar la competencia y la innovación, los organismos del sector público deben poder introducir condiciones especiales en las licencias relativas a la reutilización de datos y documentos por parte de empresas muy grandes. Estas condiciones deben ser proporcionadas y basarse en criterios objetivos, teniendo en cuenta el poder económico, la capacidad de la entidad para adquirir datos o la designación como guardián de acceso en virtud del Reglamento EUR 2022/1925, entre otros criterios similares, cuando proceda. Dichas condiciones especiales podrán referirse, entre otras cosas, a los cánones y tasas o a los fines de la reutilización.
- (26) Con el fin de fomentar la innovación y mantener una competencia leal en el mercado digital de la Unión, es imperativo garantizar que el acceso a los datos del sector público y su reutilización beneficien a una amplia variedad de participantes en el mercado y no refuercen involuntariamente las posiciones dominantes existentes. Las empresas muy grandes, y en particular las empresas designadas como guardianes de acceso en virtud del Reglamento (UE) 2022/1925, tienen un poder y una influencia significativos en el mercado interior. Para evitar que estas empresas aprovechen su considerable poder de mercado en detrimento de la competencia leal y la innovación,

³³ Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36, ELI: <http://data.europa.eu/eli/reco/2003/361/oj>).

³⁴ Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (DO L 265 de 12.10.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/1925/oj>).

los organismos del sector público deben poder establecer unos cánones y tasas más elevados por la reutilización de datos públicos abiertos y datos protegidos. Estos cánones y tasas más elevados deben ser proporcionados y basarse en criterios objetivos, teniendo en cuenta el poder económico y la capacidad de la entidad para adquirir datos. Esta medida sirve para salvaguardar las oportunidades de las empresas más pequeñas y de los nuevos participantes en el mercado para innovar y competir en la economía digital.

- (27) El presente Reglamento propone una serie de modificaciones específicas del Reglamento (UE) 2016/679 en aras de la claridad y la simplificación, a la vez que se preserva el mismo nivel de protección de datos. El artículo 4 del Reglamento (UE) 2016/679 establece que por datos personales debe entenderse toda información sobre una persona física identificada o identificable. A fin de determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que razonablemente puedan utilizarse para identificar directa o indirectamente a la persona física. Teniendo en cuenta la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) relativa a la definición de datos personales, es necesario aclarar en mayor medida cuándo debe considerarse que una persona física es identificable. La existencia de información adicional que permita identificar al interesado no significa, por sí sola, que deba considerarse que los datos seudonimizados constituyen, en todos los casos y para cada persona o entidad, datos personales a efectos de la aplicación del Reglamento (UE) 2016/679. En particular, debe aclararse que la información no debe considerarse datos personales de una entidad determinada cuando dicha entidad no disponga de medios que puedan utilizarse razonablemente para identificar a la persona física a la que se refiere la información. Una posible transmisión posterior de esa información a terceros que dispongan de medios que les permitan razonablemente identificar a la persona física a la que se refiere la información, como la verificación cruzada con otros datos a su disposición, hace que esa información se convierta en datos personales únicamente para aquellos terceros que dispongan de tales medios. Una entidad cuya información no constituya datos personales, en principio, no entra en el ámbito de aplicación del Reglamento (UE) 2016/679. A este respecto, el TJUE ha dictaminado que no es razonablemente probable que se utilice un medio de identificación del interesado cuando el riesgo de identificación parezca en realidad insignificante, en el sentido de que la identificación de dicho interesado está prohibida por la ley o es imposible en la práctica, por ejemplo, porque implicaría un esfuerzo desproporcionado en términos de tiempo, costes y mano de obra. Un ejemplo de prohibición de la reidentificación puede encontrarse en las obligaciones de los usuarios de datos de salud recogidas en el artículo 61, apartado 3, del Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo³⁵. La Comisión, junto con el Comité Europeo de Protección de Datos, debe apoyar a los responsables del tratamiento en la aplicación de esta definición actualizada estableciendo criterios técnicos en un acto de ejecución.

³⁵ Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 (DO L, 2025/327, 5.3.2025, ELI: <http://data.europa.eu/eli/reg/2025/327/oj>).

- (28) A fin de evaluar si la investigación cumple las condiciones de la investigación científica a efectos del presente Reglamento, pueden tenerse en cuenta elementos como el enfoque metodológico y sistemático aplicado durante la realización de la investigación en el ámbito específico. La investigación y el desarrollo tecnológico deben llevarse a cabo en entornos académicos, industriales o de otro tipo, incluidas las pymes (artículo 179, apartado 2, del TFUE), y deben ser siempre de alta calidad y ajustarse a los principios de fiabilidad, honestidad, respeto y responsabilidad (verificabilidad).
- (29) Conviene reiterar que las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. En tales casos, no es necesario determinar, sobre la base del artículo 6, apartado 4, del presente Reglamento, si la finalidad del tratamiento ulterior es compatible con la finalidad para la que se recogieron inicialmente los datos personales.
- (30) Una IA fiable es fundamental para propiciar el crecimiento económico y apoyar la innovación con unos resultados que sean socialmente beneficiosos. El desarrollo y el uso de sistemas de IA y los modelos subyacentes, como los grandes modelos de lenguaje y los modelos de vídeo generativos, se basan en datos, entre los que se incluyen datos personales, en diversas fases del ciclo de vida de la IA, como la fase de entrenamiento, pruebas y validación, y en algunos casos pueden conservarse en el sistema o en el modelo de IA. Por lo tanto, el tratamiento de datos personales en este contexto puede llevarse a cabo a efectos de un interés legítimo en el sentido del artículo 6 del Reglamento (UE) 2016/679, cuando proceda. Esto no afecta a la obligación del responsable del tratamiento de garantizar que el desarrollo o el uso (despliegue) de la IA en un contexto específico o para fines específicos se ajuste a otra legislación nacional o de la Unión, o de garantizar el cumplimiento cuando su uso esté expresamente prohibido por la ley. Tampoco afecta a su obligación de garantizar el cumplimiento de todas las demás condiciones del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, así como de todos los demás requisitos y principios de dicho Reglamento.
- (31) Cuando el responsable del tratamiento, a la luz del enfoque basado en el riesgo que informa de la escalabilidad de las obligaciones en virtud del presente Reglamento, pondere el interés legítimo perseguido por el responsable del tratamiento o por un tercero y los intereses, derechos y libertades del interesado, debe tenerse en cuenta si el interés perseguido por el primero es beneficioso para el interesado y el conjunto de la sociedad, lo que puede ocurrir, por ejemplo, cuando el tratamiento de datos personales sea necesario para detectar y eliminar sesgos, protegiendo así a los interesados de la discriminación, o cuando el tratamiento de datos personales tenga por objeto garantizar resultados exactos y seguros para un uso beneficioso, como mejorar la accesibilidad a determinados servicios. También deben tenerse en cuenta, entre otras cosas, las expectativas razonables del interesado sobre la base de su relación con el responsable del tratamiento y las salvaguardias adecuadas para minimizar las repercusiones en los derechos de los interesados, tales como proporcionar una mayor transparencia a los interesados, reconocer un derecho incondicional a oponerse al tratamiento de sus datos personales y respetar las indicaciones técnicas integradas en un servicio que limiten el uso de datos para el desarrollo de IA por parte de terceros, el uso de otras técnicas de última generación de protección de la privacidad para el entrenamiento de la IA y medidas técnicas adecuadas para minimizar eficazmente los

riesgos derivados, por ejemplo, de la regurgitación o la fuga de datos y otras acciones previstas o previsibles.

- (32) El tratamiento de datos personales con fines de investigación científica y la aplicación de las disposiciones del RGPD sobre investigación científica están supeditados a la adopción de garantías adecuadas para los derechos y libertades de los interesados, de conformidad con el artículo 89, apartado 1, del RGPD. Para ello, el RGPD equilibra el derecho a la protección de los datos personales, de conformidad con el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, con la libertad de ciencia, de conformidad con el artículo 13 de la Carta. Por consiguiente, el tratamiento de datos personales con fines de investigación científica persigue un interés legítimo en el sentido del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, siempre que dicha investigación no sea contraria al Derecho de la Unión o de los Estados miembros. Esto se entiende sin perjuicio de la obligación del responsable del tratamiento de garantizar el cumplimiento de todas las demás condiciones del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, así como de todos los demás requisitos y principios de dicho Reglamento.
- (33) El desarrollo de determinados sistemas y modelos de IA puede implicar la recogida de grandes cantidades de datos, en particular datos personales y categorías especiales de datos. Pueden existir categorías especiales de datos personales de forma residual en los conjuntos de datos de entrenamiento, pruebas o validación o conservarse en el sistema o en el modelo de IA, aunque las categorías especiales de datos personales no sean necesarias para los fines del tratamiento. Con el fin de no obstaculizar de manera desproporcionada el desarrollo y el funcionamiento de la IA, y teniendo en cuenta la capacidad del responsable del tratamiento para identificar y eliminar categorías especiales de datos personales, deben permitirse una excepción a la prohibición del tratamiento de categorías especiales de datos personales prevista en el artículo 9, apartado 2, del Reglamento (UE) 2016/679. La excepción solo debe aplicarse cuando el responsable del tratamiento haya adoptado medidas técnicas y organizativas adecuadas de manera eficaz para evitar el tratamiento de dichos datos, adopte las medidas adecuadas durante todo el ciclo de vida de un sistema o modelo de IA y, una vez identificados dichos datos, los elimine de manera efectiva. Si la eliminación exige un esfuerzo desproporcionado, en particular cuando la eliminación de categorías especiales de datos memorizados en el sistema o modelo de IA requiera la reingeniería de tal sistema o modelo, el responsable del tratamiento debe proteger eficazmente dichos datos de la posibilidad de ser utilizados para inferir resultados, revelarse o ponerse de cualquier otro modo a disposición de terceros. Esta excepción no debe aplicarse cuando el tratamiento de categorías especiales de datos personales sea necesario para los fines del tratamiento. En este caso, el responsable del tratamiento debe basarse en las excepciones previstas en el artículo 9, apartado 2, letras a) a j), del Reglamento (UE) 2016/679.
- (34) Por datos biométricos, tal como se definen en el artículo 4, apartado 14, del Reglamento (UE) 2016/679, se entiende el tratamiento de determinadas características de una persona física a través de un medio técnico específico, que permite o confirma la identificación única de dicha persona. El concepto de datos biométricos incluye dos funciones distintas: la identificación de una persona física o la verificación (también denominada autenticación) de la identidad que esta declara, ambas basadas en procesos técnicos diferentes. El proceso de identificación se basa en una búsqueda «uno a varios» de los datos biométricos del interesado en una base de datos, mientras que el proceso de verificación se fundamenta en una comparación «uno a uno» de los

datos biométricos facilitados por el propio interesado, que, de este modo, afirma su identidad. También deben permitirse excepciones a la prohibición de tratar datos biométricos recogida en el artículo 9, apartado 1, del Reglamento (UE) 2016/679 cuando la verificación de la identidad declarada del interesado sea necesaria para un fin que el responsable del tratamiento persigue y se apliquen garantías adecuadas que permitan que el interesado tenga el control exclusivo del proceso de verificación. Por ejemplo, cuando los datos biométricos se almacenen de forma segura únicamente por parte del interesado o se almacenen de forma segura por parte del responsable del tratamiento en una forma cifrada de última generación y la clave de cifrado o medios equivalentes están únicamente en poder del interesado, no es probable que dicho tratamiento entrañe riesgos significativos para sus derechos y libertades fundamentales. El responsable no llega a conocer los datos biométricos, o únicamente lo hace durante un período muy limitado durante el proceso de verificación.

- (35) El artículo 15 del Reglamento (UE) 2016/679 confiere a los interesados el derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a determinada información adicional. El derecho de acceso debe permitir al interesado conocer y verificar la legalidad del tratamiento, así como ejercer los demás derechos que le confiere el Reglamento (UE) 2016/679. En cambio, debe aclararse en el artículo 12 del Reglamento que el derecho de acceso, que desde el principio es favorable a los interesados, no debe ser objeto de abuso en el sentido de que los interesados abusen de él para fines distintos de la protección de sus datos. Por ejemplo, se produciría un abuso del derecho de acceso si el interesado pretendiera hacer que el responsable del tratamiento denegara una solicitud de acceso, con el fin de exigir posteriormente el pago de una indemnización, posiblemente bajo la amenaza de interponer una reclamación por daños y perjuicios. Otros ejemplos de abuso incluyen situaciones en las que los interesados hacen un uso excesivo del derecho de acceso con la única intención de causar daños o perjuicios al responsable del tratamiento o cuando una persona presenta una solicitud, pero al mismo tiempo se ofrece a retirarla a cambio de obtener algún tipo de beneficio del responsable del tratamiento. Además, con el fin de que la carga de los responsables del tratamiento se mantenga a un nivel razonable, estos deberían soportar una carga de la prueba menor para acreditar el carácter excesivo de una solicitud que la requerida para demostrar que una solicitud es manifiestamente infundada. La razón es que el carácter manifiestamente infundado de una solicitud depende de hechos que recaen principalmente en el ámbito de responsabilidad del responsable del tratamiento, mientras que el carácter excesivo de una solicitud se refiere al comportamiento posiblemente abusivo de un interesado, que recae principalmente fuera de la esfera de influencia del responsable del tratamiento, por lo que es posible que este solo pueda probar tal abuso hasta un nivel razonable. En cualquier caso, al solicitar el acceso con arreglo al artículo 15 del Reglamento (UE) 2016/679, el interesado debe ser lo más específico posible. Las solicitudes demasiado amplias e indiferenciadas también deben considerarse excesivas.
- (36) El artículo 13 del Reglamento (UE) 2016/679 exige que el responsable del tratamiento facilite al interesado determinada información sobre el tratamiento de sus datos personales, así como determinada información adicional necesaria para garantizar un tratamiento leal y transparente, tal como se define en los apartados 1, 2 y 3 de dicha disposición. De conformidad con el artículo 13, apartado 4, del Reglamento (UE) 2016/679, esta obligación no se aplica cuando y en la medida en que el interesado ya disponga de la información. Para reducir aún más la carga de los responsables del tratamiento, sin socavar las posibilidades del interesado de ejercer sus derechos en

virtud del capítulo III del Reglamento, esta excepción debe ampliarse a situaciones en las que no sea probable que el tratamiento entrañe un alto riesgo, en el sentido del artículo 35 del Reglamento, y existan motivos razonables para suponer que el interesado ya dispone de la información a que se refiere el apartado 1, letras a) y c), a la luz del contexto en el que se han recogido los datos personales, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento. Estas deben ser las situaciones en las que el contexto de la relación entre el responsable del tratamiento y el interesado es muy claro y está muy delimitado y la actividad del responsable del tratamiento no implica un uso intensivo de datos, como la relación entre un artesano y sus clientes, en la que el ámbito del tratamiento se limita a los datos mínimos necesarios para prestar el servicio. La actividad del responsable del tratamiento no implica un uso intensivo de datos cuando recoge una pequeña cantidad de datos personales y sus operaciones de tratamiento no son complejas, lo que no ocurre, por ejemplo, en el ámbito del empleo. En tales circunstancias, es decir, cuando el tratamiento no implique un uso intensivo de datos, no sea complejo y cuando el responsable del tratamiento recoja una pequeña cantidad de datos personales, debe ser razonable esperar, por ejemplo, que el interesado disponga de información sobre la identidad y los datos de contacto del responsable del tratamiento, así como sobre la finalidad del tratamiento cuando este se lleve a cabo para la ejecución de un contrato en el que el interesado sea parte, o cuando el interesado haya dado su consentimiento para dicho tratamiento, de conformidad con los requisitos establecidos en el Reglamento (UE) 2016/679. Lo mismo debe aplicarse a las asociaciones y clubes deportivos en los que el tratamiento de datos personales se limite a la gestión de la afiliación, la comunicación con los miembros y la organización de actividades. No obstante, esta excepción a las obligaciones del artículo 13 se entiende sin perjuicio de las obligaciones independientes del responsable del tratamiento en virtud del artículo 15 de dicho Reglamento, que se aplica en caso de que el interesado solicite acceso sobre la base de esta última disposición. Cuando no se aplique la excepción a las obligaciones del artículo 13, con el fin de equilibrar la necesidad de ofrecer una información completa y fácilmente comprensible para el interesado, los responsables del tratamiento podrán adoptar un enfoque por niveles a la hora de facilitar la información requerida, en particular permitiendo a los usuarios acceder a información adicional mediante navegación.

- (37) Cuando el tratamiento tenga lugar con fines de investigación científica y resulte imposible facilitar la información al interesado o suponga un esfuerzo desproporcionado, no debería ser necesario facilitar la información prevista en el artículo 13 del presente Reglamento. El responsable del tratamiento debe hacer esfuerzos razonables para obtener los datos de contacto cuando estos estén fácilmente disponibles y su obtención no requiera un esfuerzo desproporcionado. La provisión de la información implicaría un esfuerzo desproporcionado, en particular, cuando el responsable del tratamiento, en el momento de la recogida de los datos personales, no supiera o no previera el tratamiento de datos personales con fines de investigación científica en una fase posterior, en cuyo caso podría no disponer fácilmente de los datos de contacto de los interesados. En tales situaciones, el responsable del tratamiento debe informar indirectamente a los interesados, por ejemplo, poniendo la información a disposición del público. La puesta a disposición de dicha información debe garantizar que se llegue al mayor número posible de interesados afectados. Los medios pertinentes para poner la información a disposición del público deben determinarse en función del contexto del proyecto de investigación y de los interesados implicados.

- (38) El artículo 22 del Reglamento (UE) 2016/679 establece normas que rigen el tratamiento de datos personales cuando el responsable del tratamiento toma decisiones, basadas únicamente en el tratamiento automatizado, que tienen efectos jurídicos o efectos igualmente significativos para el interesado. A fin de proporcionar una mayor seguridad jurídica, debe aclararse que las decisiones basadas únicamente en el tratamiento automatizado están permitidas cuando se cumplen una serie de condiciones específicas, tal como se establece en el Reglamento (UE) 2016/679. Asimismo, debe aclararse que, al evaluar si una decisión es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento de datos, tal como se establece en el artículo 22, apartado 2, letra a), del Reglamento (UE) 2016/679, no debe exigirse que la decisión pueda adoptarse únicamente mediante tratamiento automatizado. Esto significa que el hecho de que la decisión también pueda ser adoptada por una persona no impide que el responsable del tratamiento adopte la decisión únicamente mediante tratamiento automatizado. Cuando existan varias soluciones de tratamiento automatizado igualmente eficaces, el responsable del tratamiento debe utilizar la menos intrusiva.
- (39) A fin de reducir la carga para los responsables del tratamiento, garantizando al mismo tiempo que las autoridades de control tengan acceso a la información pertinente y puedan actuar en caso de infracción del Reglamento, el umbral para la notificación de una violación de la seguridad de los datos personales a la autoridad de control con arreglo al artículo 33 del Reglamento (UE) 2016/679 debe ajustarse al previsto para la comunicación de una violación de la seguridad de los datos personales al interesado con arreglo al artículo 34 de dicho Reglamento. Cuando no resulte probable que una violación de datos entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento no debe estar obligado a notificarla a la autoridad de control competente. El umbral más elevado para la notificación de una violación de la seguridad de los datos a la autoridad de control no afecta a la obligación del responsable del tratamiento de documentar la violación de conformidad con el artículo 33, apartado 5, del Reglamento (UE) 2016/679, ni a su obligación de poder demostrar su conformidad con dicho Reglamento, en virtud de su artículo 5, apartado 2. A fin de facilitar el cumplimiento por parte de los responsables del tratamiento y un enfoque armonizado en la Unión, el Comité debe elaborar un modelo común para la notificación de las violaciones de la seguridad de los datos a la autoridad de control competente y una lista común de circunstancias en las que es probable que una violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de una persona física. La Comisión debe tener debidamente en cuenta la propuesta elaborada por el Comité y revisarla, en caso necesario, antes de su adopción. A fin de tener en cuenta las nuevas amenazas para la seguridad de la información, el modelo común y la lista deben revisarse al menos cada tres años y actualizarse cuando sea necesario. La falta de una lista común de circunstancias en las que sea probable que una violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de una persona física no debe afectar a las obligaciones de los responsables del tratamiento de notificar dichas violaciones.
- (40) El artículo 35 del Reglamento (UE) 2016/679 exige a los responsables del tratamiento que lleven a cabo una evaluación de impacto relativa a la protección de datos cuando sea probable que el tratamiento de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas. Las autoridades de control establecidas conforme a dicho Reglamento están obligadas a establecer y publicar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a

la protección de datos. Además, el Reglamento establece que las autoridades de control podrán establecer y publicar una lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. Con el fin de contribuir de manera efectiva al objetivo de convergencia de las economías y garantizar eficazmente la libre circulación de datos personales entre los Estados miembros, aumentar la seguridad jurídica, facilitar el cumplimiento por parte de los responsables del tratamiento y garantizar una interpretación armonizada del concepto de alto riesgo para los derechos y libertades de los interesados, debe facilitarse una lista única de operaciones de tratamiento a escala de la UE que sustituya a las listas nacionales existentes. Además, debe exigirse la publicación de una lista del tipo de operaciones de tratamiento para las que no se requiere una evaluación de impacto relativa a la protección de datos, que actualmente es opcional. Las listas de operaciones de tratamiento deben ser elaboradas por el Comité y adoptadas por la Comisión como acto de ejecución. A fin de facilitar el cumplimiento por parte de los responsables del tratamiento, el Comité también debe preparar un modelo y una metodología comunes para llevar a cabo evaluaciones de impacto relativas a la protección de datos, que serán adoptadas por la Comisión como acto de ejecución. La Comisión debe tener debidamente en cuenta las propuestas elaboradas por el Comité y revisarlas, en caso necesario, antes de su adopción. A fin de tener en cuenta los avances tecnológicos, las listas, el modelo común y la metodología deben revisarse al menos cada tres años y actualizarse cuando sea necesario.

- (41) El Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo³⁶ se aplica al tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión. Por su parte, la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo³⁷ se aplica al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. El Reglamento (UE) 2018/1725 y la Directiva (UE) 2016/680 deben ajustarse a las modificaciones del Reglamento (UE) 2016/679 que introduce el presente Reglamento.
- (42) Como se aclara en el considerando 5 del Reglamento (UE) 2018/1725, siempre que las disposiciones del Reglamento (UE) 2018/1725 sigan los mismos principios que las disposiciones del Reglamento (UE) 2016/679, estos dos conjuntos de disposiciones

³⁶ Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

³⁷ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>).

deben interpretarse de manera homogénea, con arreglo a la jurisprudencia del TJUE. El régimen del Reglamento (UE) 2018/1725 debe entenderse como equivalente al régimen del Reglamento (UE) 2016/679. Por lo tanto, el presente Reglamento también modifica las disposiciones del Reglamento (UE) 2018/1725 a las que afectan las modificaciones del Reglamento (UE) 2016/679, en la medida en que estas últimas también son pertinentes en el contexto del tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión.

- (43) A fin de proporcionar un marco sólido y coherente de protección de datos en la Unión, tras la adopción del presente Reglamento deben realizarse las adaptaciones necesarias de la Directiva (UE) 2016/680 y de cualquier otro acto jurídico de la Unión aplicable a dicho tratamiento de datos personales, de manera que puedan aplicarse en una fecha lo más cercana posible a la entrada en vigor de las modificaciones del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725.
- (44) El almacenamiento de datos personales en un equipo terminal, o la obtención de acceso a datos personales ya almacenados en el mismo, y el posterior tratamiento de dichos datos deben regularse con arreglo a un marco jurídico único, a saber, el Reglamento (UE) 2016/679, cuando el abonado al servicio de comunicaciones electrónicas o el usuario del equipo terminal sea una persona física. Las modificaciones presentadas en el presente Reglamento siguen ofreciendo los niveles más elevados de protección de los datos personales, al tiempo que simplifican las experiencias de los interesados a la hora de ejercer sus derechos y expresar sus preferencias en línea. Las modificaciones se refieren, en particular, al almacenamiento de información en dicho equipo y al acceso o la recogida por otros medios de información de dicho equipo que implique el tratamiento de datos personales a través de *cookies* o tecnologías similares para obtener información del equipo terminal. Las normas pertinentes también deben aplicarse con independencia de que el equipo terminal sea propiedad de la persona física o de otra persona física o jurídica.

El almacenamiento de datos personales en un equipo terminal, o la obtención de acceso a datos personales ya almacenados en el mismo, debe seguir estando permitido únicamente sobre la base del consentimiento. Al igual que en el enfoque de la Directiva 2002/58/CE, este requisito no debe impedir el almacenamiento de datos personales, o la obtención de acceso a datos personales ya almacenados, en el equipo terminal de una persona física, cuando ello se base en el Derecho de la Unión o de los Estados miembros en el sentido del artículo 6 del Reglamento (UE) 2016/679 y cumpla todas las condiciones de legalidad establecidas en dicha disposición, y se haga para los objetivos establecidos en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

Con vistas a reducir la carga asociada al cumplimiento normativo y proporcionar claridad jurídica a los responsables del tratamiento, y dado que determinados fines del tratamiento plantean un bajo riesgo para los derechos y libertades de los interesados o que dicho tratamiento puede ser necesario para prestar un servicio solicitado por el interesado, es necesario establecer una lista limitativa de fines para los que el tratamiento debe permitirse sin consentimiento. Por lo que se refiere al almacenamiento de datos personales en un equipo terminal, o a la obtención de acceso a datos personales ya almacenados en el mismo, y al tratamiento posterior necesario para tales fines, el presente Reglamento debe establecer, por tanto, que el tratamiento sea lícito. El responsable del tratamiento, por ejemplo, un prestador de servicios de comunicación, podrá encomendar a un encargado del tratamiento, como una empresa de estudios de mercado, que lleve a cabo el tratamiento en su nombre.

Para el tratamiento ulterior de datos personales con fines distintos de los establecidos en la lista limitativa, deben aplicarse el artículo 6 y, cuando corresponda, el artículo 9 del Reglamento (UE) 2016/679. Corresponde al responsable del tratamiento, a la luz del principio de responsabilidad proactiva, elegir la base jurídica adecuada para el tratamiento previsto. Para poder invocar el interés legítimo con arreglo al artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679 como motivo para el tratamiento ulterior de datos personales, el responsable del tratamiento debe demostrar que persigue su interés legítimo o el de un tercero, que el tratamiento es necesario para alcanzar la finalidad de dicho interés legítimo y que los intereses o los derechos fundamentales del interesado no prevalecen sobre los intereses perseguidos por el responsable del tratamiento. En este contexto, los responsables del tratamiento deben tener plenamente en cuenta los siguientes elementos: si el interesado es un menor de edad; las expectativas razonables del interesado; las repercusiones en la persona, ya sea debido a la magnitud de los datos tratados o a la sensibilidad de los mismos; la magnitud del tratamiento en cuestión, en el sentido de que el tratamiento no puede ser particularmente amplio, ya sea por su cantidad o por la variedad de categorías de datos; el tratamiento debe basarse en datos que se limiten a lo necesario y no puede basarse en el seguimiento de grandes partes de la actividad en línea de los interesados; y otros factores pertinentes, según proceda. El tratamiento no debe dar lugar a un seguimiento continuo de la vida privada del interesado.

Cuando el responsable del tratamiento no pueda invocar el interés legítimo como fundamento jurídico para el tratamiento ulterior, el tratamiento debe basarse en otro motivo contemplado en el artículo 6, apartado 1, del Reglamento (UE) 2016/679, en particular en el consentimiento de conformidad con sus artículos 6 y 7, siempre que se cumplan todos los principios recogidos en dicho Reglamento.

- (45) Los interesados que han denegado una solicitud de consentimiento se enfrentan a menudo a una nueva solicitud para dar su consentimiento cada vez que visitan el servicio en línea del mismo responsable del tratamiento. Esto puede tener efectos perjudiciales para los interesados, que pueden dar su consentimiento con el único fin de evitar la repetición de solicitudes. Por consiguiente, el responsable del tratamiento debe estar obligado a respetar la preferencia del interesado de denegar una solicitud de consentimiento durante al menos un período determinado.
- (46) Los interesados deben tener la posibilidad de basarse en indicaciones automatizadas y legibles por máquina de su elección de dar su consentimiento, denegar una solicitud de consentimiento u oponerse al tratamiento de datos. Tales indicaciones deben ajustarse al estado de la técnica y deben poder aplicarse a la configuración de un navegador web o a la cartera europea de identidad digital, tal como se establece en el Reglamento (UE) n.º 914/2014, o a cualquier otro medio adecuado. Las normas establecidas en el presente Reglamento deben apoyar la aparición de soluciones orientadas al mercado con interfaces adecuadas. El responsable del tratamiento debe estar obligado a respetar las indicaciones automatizadas y legibles por máquina de las preferencias del interesado una vez que haya normas disponibles. A la luz de la importancia del periodismo independiente en una sociedad democrática y con el fin de no socavar la base económica para ello, los prestadores de servicios de comunicación no deben estar obligados a respetar las indicaciones de lectura mecanizada de las preferencias del interesado. La obligación de los proveedores de navegadores web de proporcionar los medios técnicos para que los interesados puedan expresar sus preferencias con respecto al tratamiento no debe socavar la posibilidad de que los prestadores de servicios de comunicación soliciten el consentimiento de los interesados.

- (47) La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, revisada por última vez en 2009, proporciona un marco para la protección del derecho a la intimidad, en particular la confidencialidad de las comunicaciones. Asimismo, concreta la aplicación del Reglamento (UE) 2016/679 en relación con el tratamiento de datos personales en el contexto de los servicios de comunicaciones electrónicas. Protege la intimidad y la integridad del equipo terminal del usuario o abonado utilizado para dichas comunicaciones. La disposición actual del artículo 5, apartado 3, de la Directiva 2002/58/CE debe seguir siendo aplicable en la medida en que el abonado o usuario no sea una persona física y la información almacenada o a la que se acceda no constituya ni dé lugar al tratamiento de datos personales.
- (48) Procede derogar el artículo 4 de la Directiva 2002/58/CE. Este artículo establece requisitos para los proveedores de servicios de comunicaciones electrónicas disponibles al público en lo que respecta a la protección de la seguridad de sus servicios y a los requisitos de notificación. Posteriormente, la Directiva (UE) 2022/2555 ha establecido nuevos requisitos en lo que respecta a las medidas para la gestión de riesgos de ciberseguridad y la notificación de incidentes para dichos proveedores. Con el fin de reducir el solapamiento de obligaciones para las entidades del sector de las comunicaciones electrónicas, debe derogarse el artículo 4 de la Directiva 2002/58/CE. Por lo que respecta a la seguridad del tratamiento de los datos personales de conformidad con el artículo 4, apartados 1 y 1 *bis* de la Directiva 2002/58/CE y a la notificación de las violaciones de la seguridad de los datos personales de conformidad con el artículo 4, apartados 3 a 5, de esta misma Directiva, el Reglamento (UE) 2016/679 ya establece normas exhaustivas y actualizadas. Por consiguiente, estas normas deben aplicarse a los proveedores de servicios de comunicaciones electrónicas disponibles al público y a los proveedores de redes públicas de comunicaciones, lo que garantizaría de este modo la aplicación de un único régimen a los responsables y encargados del tratamiento.
- (49) Varios actos jurídicos horizontales o sectoriales de la Unión exigen la notificación del mismo evento a diferentes autoridades utilizando diferentes medios y canales técnicos. En este sentido, el punto de entrada único para la notificación de incidentes debe permitir a las entidades cumplir las obligaciones de notificación en virtud de la Directiva (UE) 2022/2555, el Reglamento (UE) 2016/679, el Reglamento (UE) 2022/2554, el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2022/2557 mediante la presentación de notificaciones a través de una interfaz única. Además, el punto de entrada único debe ofrecer a las entidades la posibilidad de recuperar información que hayan presentado previamente al utilizarlo, ayudando así a las entidades a hacer un seguimiento de su cumplimiento de las obligaciones de notificación en relación con incidentes específicos.
- (50) Para garantizar la seguridad del punto de entrada único, la ENISA debe adoptar medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos planteados para la seguridad del punto de entrada único y la información que se presenta o se difunde a través de este. Al evaluar el riesgo, así como la idoneidad y proporcionalidad de dichas medidas, la ENISA debe tener en cuenta el carácter sensible de la información presentada o difundida con arreglo a los actos jurídicos pertinentes de la Unión. La ENISA debe consultar a las autoridades competentes con arreglo a los actos jurídicos pertinentes de la Unión a la hora de elaborar las medidas técnicas, operativas y organizativas necesarias para implantar, mantener y explotar de forma segura el punto de entrada único, haciendo uso de los

grupos y redes de cooperación ya existentes de los Estados miembros establecidos en virtud de dichos actos.

- (51) Antes de permitir la notificación de incidentes, la ENISA debe realizar una prueba piloto del funcionamiento del punto de entrada único, que debe incluir una prueba exhaustiva de las especificidades y los requisitos de las notificaciones para los actos jurídicos pertinentes de la Unión. Sobre la base de los resultados de la prueba piloto, la Comisión debe evaluar el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad del punto de entrada único. Al llevar a cabo dicha evaluación, la Comisión debe consultar a la red de equipos de respuesta a incidentes de seguridad informática (CSIRT) y a las autoridades competentes en virtud de los actos jurídicos pertinentes de la Unión, haciendo uso de los grupos y redes de cooperación ya existentes de los Estados miembros establecidos en virtud de dichos actos. Cuando la Comisión considere que el punto de entrada único garantiza el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad, debe publicar un anuncio a tal efecto en el *Diario Oficial de la Unión Europea*. En caso de que la Comisión considere que el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad no están garantizados, la ENISA debe adoptar todas las medidas correctoras necesarias, seguidas de una nueva evaluación por parte de la Comisión.
- (52) Para garantizar la continuidad y la interoperabilidad con las soluciones técnicas nacionales existentes que facilitan la notificación de incidentes, la ENISA debe tener en cuenta, en la medida de lo posible, dichas soluciones técnicas nacionales a la hora de elaborar las especificaciones relativas a las medidas técnicas, operativas y organizativas necesarias para implantar, mantener y explotar de forma segura el punto de entrada único. La ENISA también debe tener en cuenta protocolos y herramientas técnicos, como interfaces de programación de aplicaciones y normas legibles por máquina, que permitan a las entidades integrar las obligaciones de notificación de incidentes en los procesos empresariales y a las autoridades conectar el punto de entrada único con sus sistemas nacionales de notificación.
- (53) Para garantizar que el punto de entrada único permita a las entidades pertinentes presentar el tipo de información y el formato exigidos con arreglo a los actos jurídicos pertinentes de la Unión, la ENISA debe consultar a la Comisión y a las autoridades competentes en virtud de dichos actos. Cuando un acto jurídico de la Unión no esté plenamente armonizado en lo que respecta al tipo de información y al formato de las notificaciones, los Estados miembros deben informar a la ENISA acerca de sus disposiciones nacionales.
- (54) Sobre la base del Reglamento (UE) 2022/2554, el sector financiero se ha situado a la vanguardia de la aplicación de un marco armonizado, exhaustivo y eficaz, también en lo que respecta a la notificación de incidentes. Con el fin de simplificar el cumplimiento, procede armonizar el marco de notificación de incidentes establecido en virtud del Reglamento (UE) 2022/2554 con el punto de entrada único, al mismo tiempo que se garantizan la continuidad y la estabilidad del marco de notificación existente, y teniendo en cuenta que el punto de entrada único solo estará operativo una vez se haya evaluado que el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad están garantizados. Además, el Reglamento (UE) 2022/2554 ha introducido modelos de notificación normalizados que optimizan para el sector financiero el contenido de las notificaciones de incidentes graves relacionados con las TIC. La experiencia adquirida con la adopción de estos modelos proporciona información valiosa y mejores prácticas que deben tenerse en cuenta a la hora de especificar el tipo de información, el formato y el procedimiento de una notificación a

efectos de su presentación a través del punto de entrada único con arreglo a la Directiva (UE) 2022/2555, la Directiva (UE) 2022/2557 o el Reglamento (UE) 2016/679, cuando proceda. Para ello, la Comisión debe tener debidamente en cuenta las normas técnicas de regulación adoptadas en virtud del Reglamento (UE) 2022/2554, que especifican el contenido de la notificación inicial, así como del informe intermedio y el informe final, relativos a incidentes graves relacionados con las TIC. Este enfoque tiene por objeto garantizar la coherencia, promover sinergias y reducir la carga administrativa de las entidades al minimizar el número de campos de datos que estas deben completar, facilitando de esta manera procesos de notificación más eficientes y racionalizados.

- (55) En virtud de los actos jurídicos pertinentes de la Unión, las autoridades competentes deben compartir en una fase posterior determinada información específica sobre incidentes para facilitar una supervisión y coordinación eficaces. Por consiguiente, el punto de entrada único debe diseñarse para admitir y facilitar el intercambio de información a ese nivel para cada acto jurídico pertinente de la Unión, garantizando que sean posibles flujos de datos adecuados entre las autoridades de una forma segura, oportuna y eficiente, en caso de que los Estados miembros decidan hacer uso de esta característica adicional.
- (56) Para garantizar que la notificación de incidentes se lleve a cabo a través del punto de entrada único, la Directiva (UE) 2022/2555, el Reglamento (UE) 2016/679, el Reglamento (UE) 2022/2554, el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2022/2557 deben, por tanto, modificarse en consecuencia. El punto de entrada único debe empezar a utilizarse a efectos de la notificación de incidentes en virtud de dichos actos en un plazo de dieciocho meses a partir de la entrada en vigor del presente Reglamento. Cuando la Comisión active los mecanismos de notificación que retrasan la fecha de aplicación a veinticuatro meses a partir de la entrada en vigor del Reglamento, las disposiciones correspondientes de la Directiva (UE) 2022/2555, el Reglamento (UE) n.º 910/2014, el Reglamento (UE) 2022/2554 y la Directiva (UE) 2022/2557 deben seguir aplicándose a efectos del cumplimiento de las obligaciones de notificación establecidas en las disposiciones.
- (57) En el caso excepcional de que una imposibilidad técnica impida la presentación de notificaciones de incidentes a través del punto de entrada único, las entidades deben cumplir sus obligaciones de notificación por medios alternativos. Para ello, los destinatarios de las notificaciones de incidentes con arreglo a los actos jurídicos pertinentes de la Unión deben garantizar que pueden recibir dichas notificaciones de incidentes a través de medios alternativos y deben poner a disposición del público información relativa a dichos medios alternativos.
- (58) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo³⁸, emitió su dictamen el [FECHA]. El Comité Europeo de Protección de

³⁸ Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el

Datos, al que se consultó de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725, emitió su dictamen el [FECHA].

- (59) El Reglamento (UE) 2019/1150 establece un conjunto específico de normas obligatorias a escala de la Unión para garantizar un entorno comercial dentro del mercado interior en línea que sea equitativo, predecible, sostenible y confiable. El Reglamento (UE) 2022/2065 y el Reglamento (UE) 2022/1925 proporcionan un marco regulador integral para crear entornos en línea seguros, predecibles y confiables para todos los usuarios finales de servicios en línea, y establecen unas condiciones de competencia equitativas para las empresas en los mercados digitales. En aras de la simplificación de la legislación de la Unión en el ámbito de los servicios de intermediación en línea y las plataformas en línea, y dado que los objetivos y las disposiciones sustantivas del Reglamento sobre las relaciones entre plataformas y empresas están contemplados en gran medida en el Reglamento de Servicios Digitales y el Reglamento de Mercados Digitales, procede derogar el Reglamento (UE) 2019/1050. El Reglamento (UE) 2022/2065 y el Reglamento (UE) 2022/1925 contribuyen a un marco regulador plenamente armonizado para los servicios y los mercados digitales, al aproximar las medidas nacionales relativas a los requisitos aplicables a los prestadores de servicios intermediarios y a la disputabilidad y equidad de los servicios básicos de plataforma prestados por los guardianes de acceso. A efectos de la seguridad jurídica, determinadas definiciones recogidas en el artículo 2, las disposiciones sobre restricciones y suspensiones del artículo 4, así como sobre el sistema interno de tramitación de reclamaciones del artículo 11 del Reglamento (UE) 2019/1150, que son objeto de remisión por otros actos jurídicos, en particular la Directiva (UE) 2023/2831 relativa a la mejora de las condiciones laborales en el trabajo en plataformas, así como el artículo 15 que garantiza la aplicación, seguirán temporalmente en vigor hasta que se modifiquen los actos originales.
- (60) Dado el carácter técnico de las modificaciones propuestas en el presente Reglamento y a la urgencia de establecer un marco jurídico simplificado, el presente Reglamento debe entrar en vigor inmediatamente tras su publicación en el *Diario Oficial de la Unión Europea*. Cuando proceda, deben concederse períodos transitorios para que los Estados miembros y las entidades reguladas se adapten a las normas.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Modificaciones del Reglamento (UE) 2023/2854

El Reglamento (UE) 2023/2854 se modifica como sigue:

1. El artículo 1 se modifica como sigue:
 - a) en el apartado 1, se insertan las letras siguientes:

Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

«e *bis*) el registro voluntario de los servicios de intermediación de datos;
e *ter*) un marco para la inscripción voluntaria en un registro de las entidades que recojan y traten datos cedidos con fines altruistas;
e *quater*) la creación de un Comité Europeo de Innovación en materia de Datos;
e *quinquies*) los requisitos de localización de datos y la disponibilidad de estos para las autoridades competentes;
e *sexies*) la reutilización de determinados datos y documentos que obren en poder de organismos del sector público o de determinadas empresas públicas, así como de los datos de investigación;»;

b) en el apartado 2, se añaden las letras siguientes:

«g) el capítulo VII *bis* se aplica a los datos personales y a los datos no personales;

h) el capítulo VII *ter* se aplica a todo dato no personal;

i) el capítulo VII *quater* se aplica a los datos personales y a los datos no personales, a saber:

i) los documentos que obren en poder de organismos del sector público de los Estados miembros

1) a que se refiere el artículo 32 *decies*, apartado 1, letra a), que obren en poder de las empresas públicas

2) a que se refiere el artículo 32 *decies*, apartado 1, letra b);

ii) los datos de investigación a que se refiere el artículo 32 *decies*, apartado 1, letra c);

iii) determinadas categorías de datos protegidos a que se refiere el artículo 32 *decies*, apartado 1, letra a).»;

c) en el apartado 3, la letra g) se sustituye por el texto siguiente:

«g) los participantes en espacios de datos.»;

d) se suprime el apartado 7;

e) se añaden los apartados 11, 12 y 13 siguientes:

«11. El capítulo VII *ter* del presente Reglamento se entiende sin perjuicio de las disposiciones legales, reglamentarias y administrativas relativas a la organización interna de los Estados miembros por las que se atribuyan a autoridades u organismos de Derecho público competencias o responsabilidades para el tratamiento de datos sin remuneración contractual de personas o entidades privadas, así como de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que establecen la aplicación de esas competencias o responsabilidades.

12. Cuando la normativa de la Unión o nacional específica de un sector exija a los organismos del sector público, los proveedores de servicios de intermediación de datos o las organizaciones reconocidas de gestión de datos con fines altruistas cumplir requisitos específicos adicionales de carácter técnico, administrativo u organizativo que estén relacionados con los capítulos

VII *bis* y VII *ter*, también mediante un régimen de autorización o certificación, las disposiciones de dicha normativa de la Unión o nacional serán igualmente de aplicación. Cualquier requisito específico adicional de ese tipo deberá ser no discriminatorio y proporcionado y estar justificado objetivamente.

13. Por lo que respecta a los datos y documentos incluidos en el ámbito de aplicación de la sección II del capítulo VII *quater*, el capítulo VII *quater* del presente Reglamento no afecta a la posibilidad de que los Estados miembros adopten normas más estrictas o detalladas, siempre que dichas normas permitan una reutilización más amplia de los datos y documentos.».

2. El artículo 2 se modifica como sigue:

a) se insertan los puntos 4 *bis*, 4 *ter* y 4 *quater* siguientes:

«4 *bis*) “consentimiento”: el “consentimiento” tal como se define en el artículo 4, punto 11, del Reglamento (UE) 2016/679;

4 *ter*) “permiso”: la concesión a los usuarios de datos del derecho al tratamiento de datos no personales;

4 *quater*) “acceso”: toda utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos;»;

b) el punto 13 se sustituye por el texto siguiente:

«13) “tenedor de datos”: una persona física o jurídica que tiene el derecho o la obligación, con arreglo al presente Reglamento, al Derecho de la Unión aplicable o a la normativa nacional adoptada de conformidad con el Derecho de la Unión, de utilizar y poner a disposición datos, incluidos, cuando se haya pactado contractualmente, los datos del producto o los datos de servicios relacionados que haya extraído o generado durante la prestación de un servicio relacionado;»;

c) se insertan los puntos 28 *bis* y 28 *ter* siguientes:

«28 *bis*) “organismo de Derecho público”: cualquier organismo que reúna todas las características siguientes:

a) que se haya creado específicamente para satisfacer necesidades de interés general que no tengan carácter industrial o mercantil;

b) que esté dotado de personalidad jurídica;

c) cuya actividad esté mayoritariamente financiada por el Estado, los entes territoriales u otros organismos de Derecho público; o bien su dirección esté sujeta a la supervisión de dichas autoridades u organismos; o que tenga un órgano de administración, de dirección o de vigilancia compuesto por miembros de los cuales más de la mitad sean nombrados por las autoridades estatales, regionales o locales u otros organismos de Derecho público;

28 *ter*) “empresa pública”: toda empresa en la que los organismos de un sector público pueden ejercer, directa o indirectamente, una influencia dominante por el hecho de tener la propiedad o una participación financiera en la empresa, o en virtud de las normas que la rigen. Se considerará que los organismos del sector público

ejercen una influencia dominante, directa o indirectamente, en cualquiera de los casos siguientes en que dichos organismos, directa o indirectamente:

- a) posean la mayoría del capital suscrito de la empresa;
 - b) controlen la mayoría de los votos correspondientes a las participaciones emitidas por la empresa;
 - c) puedan designar a más de la mitad de los miembros del órgano de administración, de dirección o de vigilancia de la empresa;»;
- d) se insertan los puntos 38 *bis* y 38 *ter* siguientes:

«38 *bis*) “servicio de intermediación de datos”: todo servicio cuyo objeto sea establecer una relación de carácter económico para el intercambio de datos entre un número indeterminado de interesados o tenedores de datos y usuarios de datos a través de medios técnicos, jurídicos o de otro tipo, incluidos los servicios destinados al ejercicio de los derechos de los interesados en relación con los datos personales, y que:

- 1) no tengan como objetivo principal la intermediación de contenidos protegidos por derechos de autor;
- 2) no sean adquiridos conjuntamente por varias personas jurídicas para su uso exclusivo entre ellas;

38 *ter*) “cesión altruista de datos”: todo intercambio voluntario de datos basado en el consentimiento de los interesados para que se traten sus datos personales, o en el permiso de los tenedores de datos para que se usen sus datos no personales, sin ánimo de obtener o recibir una gratificación que exceda de una compensación relativa a los costes en que incurran a la hora de facilitar sus datos, con objetivos de interés general tal como se disponga en el Derecho nacional, en su caso, como, por ejemplo, la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, elaboración y difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica de interés general;»;

- e) se añaden los puntos 44 a 63 siguientes:

44) “mediana empresa”: mediana empresa tal como se define en el artículo 2 del anexo I de la Recomendación 2003/361/CE;

45) “pequeña empresa de mediana capitalización”: empresa pequeña de mediana capitalización según se define en el punto 2 del anexo de la Recomendación (UE) 2025/1099 de la Comisión;

46) “universidad”: un organismo del sector público que imparta enseñanza superior postsecundaria conducente a la obtención de títulos académicos;

47) “licencia tipo”: conjunto de condiciones de reutilización predefinidas en formato digital, preferiblemente compatibles con licencias modelo públicas disponibles en línea;

48) “documento”:

- a) todo contenido que no sea digital, sea cual sea su soporte (papel o grabación sonora, visual o audiovisual); o
- b) cualquier parte de tal contenido;

50) “datos dinámicos”: datos y documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, debido, en particular, a su volatilidad o rápida obsolescencia; los datos generados por los sensores suelen considerarse datos dinámicos;

51) “datos de investigación”: datos, distintos de las publicaciones científicas, recopilados o elaborados en el transcurso de actividades de investigación científica y utilizados como prueba en el proceso de investigación, o comúnmente aceptados en la comunidad investigadora como necesarios para validar las conclusiones y los resultados de la investigación;

52) “reutilización”: el uso por personas físicas o jurídicas de documentos que obran en poder de:

- a) organismos del sector público, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos en la misión de servicio público para la que se produjeron, excepto para el intercambio de documentos entre organismos del sector público en el marco de sus actividades de servicio público; o
- b) empresas públicas, a tenor del capítulo VII *quater*, sección 2, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos de prestar servicios de interés general para el que se produjeron, excepto para el intercambio de documentos entre empresas públicas y organismos del sector público que se realice exclusivamente en el desarrollo de las actividades de servicio público de los organismos del sector público;

53) “conjuntos de datos de alto valor”: datos y documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y debido al número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales datos y documentos;

54) “determinadas categorías de datos protegidos”: datos y documentos que obran en poder de organismos del sector público y que están protegidos por las siguientes razones:

- a) confidencialidad comercial, incluidos los secretos comerciales, profesionales o empresariales;
- b) confidencialidad estadística;
- c) protección de los derechos de propiedad intelectual de terceros; o
- d) protección de los datos personales, en la medida en que dichos datos no entren en el ámbito de aplicación de la sección 2 del capítulo VII *quater*;

56) “entorno de tratamiento seguro”: el entorno físico o virtual y los medios organizativos para garantizar el cumplimiento del Derecho de la Unión, en particular, por lo que respecta a los derechos de los interesados, los derechos de propiedad intelectual y la confidencialidad comercial y estadística, la integridad y la accesibilidad, así como para garantizar el cumplimiento del Derecho nacional aplicable y permitir que la entidad encargada de proporcionar el entorno de tratamiento seguro determine y supervise todas las acciones de tratamiento, incluida la presentación, el almacenamiento, la descarga y la exportación de datos, así como el cálculo de datos derivados mediante algoritmos computacionales;

57) “reutilizador”: persona física o jurídica a la que se ha concedido el derecho a reutilizar datos o documentos en poder de un organismo del sector público o de una empresa pública con arreglo al capítulo VII *quater* o datos de investigación o determinadas categorías de datos protegidos;

58) “formato legible por máquina”: formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna;

59) “formato abierto”: formato de archivo independiente de plataformas y puesto a disposición del público sin restricciones que impidan la reutilización de los documentos;

60) “norma formal abierta”: norma establecida por escrito que especifica los criterios de interoperabilidad de la aplicación informática;

61) “margen de beneficio razonable de la inversión”: porcentaje de la tarifa total, además de la cantidad necesaria para recuperar los costes elegibles, no superior a cinco puntos porcentuales por encima del tipo de interés fijo del BCE;

62) “requisito de localización de datos”: cualquier obligación, prohibición, condición, restricción u otro requisito previsto en las disposiciones legales, reglamentarias o administrativas de los Estados miembros o que se derive de prácticas administrativas generales y coherentes en un Estado miembro y en organismos de Derecho público, también en el ámbito de la contratación pública sin perjuicio de la Directiva 2014/24/UE, que imponga el tratamiento de datos en el territorio de un determinado Estado miembro o dificulte el tratamiento de datos en cualquier otro Estado miembro;

63) “seudonimización”: la seudonimización tal como se define en el artículo 4, punto 5, del Reglamento (UE) 2016/679.».

3. En el artículo 4, el apartado 8 se sustituye por el texto siguiente:

«8. En circunstancias excepcionales, cuando el tenedor de datos que sea poseedor de un secreto comercial pueda demostrar que, a pesar de las medidas técnicas y organizativas adoptadas por el usuario de conformidad con el apartado 6 del presente artículo, es muy probable que sufra un perjuicio económico grave como consecuencia de la revelación de secretos comerciales o que la revelación de secretos comerciales al usuario plantea un alto riesgo de obtención, utilización o revelación ilícitas a entidades de terceros países, o entidades establecidas en la Unión bajo el control directo o indirecto de dichas entidades, que estén sujetas a jurisdicciones que ofrezcan una protección más débil o no equivalente en

comparación con la prevista en el Derecho de la Unión, dicho tenedor de datos podrá denegar, según el caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración estará debidamente justificada sobre la base de elementos objetivos, como la aplicabilidad de la protección de los secretos comerciales en terceros países, la naturaleza y el nivel de confidencialidad de los datos solicitados, así como la singularidad y la novedad del producto conectado. Se comunicará por escrito al usuario sin demora indebida. Cuando el tenedor de datos se niegue a compartir datos con arreglo al presente apartado, lo notificará a la autoridad competente designada en cumplimiento del artículo 37.».

4. En el artículo 5, el apartado 11 se sustituye por el texto siguiente:

«11. En circunstancias excepcionales, cuando el tenedor de datos que sea poseedor de un secreto comercial pueda demostrar que, a pesar de las medidas técnicas y organizativas adoptadas por el tercero de conformidad con el apartado 9 del presente artículo, es muy probable que sufra un perjuicio económico grave como consecuencia de la revelación de secretos comerciales o que la revelación de secretos comerciales al tercero plantea un alto riesgo de obtención, utilización o revelación ilícitas a entidades de terceros países, o entidades establecidas en la Unión bajo el control directo o indirecto de dichas entidades, que estén sujetas a jurisdicciones que ofrezcan una protección más débil o no equivalente en comparación con la prevista en el Derecho de la Unión, dicho tenedor de datos podrá denegar, según el caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración estará debidamente justificada sobre la base de elementos objetivos, como la aplicabilidad de la protección de los secretos comerciales en terceros países, la naturaleza y el nivel de confidencialidad de los datos solicitados, así como la singularidad y la novedad del producto conectado. Se comunicará por escrito al tercero sin demora indebida. Cuando el tenedor de datos se niegue a compartir datos con arreglo al presente apartado, lo notificará a la autoridad competente designada en cumplimiento del artículo 37.».

5. El título del capítulo V se sustituye por el texto siguiente:

«PONER DATOS A DISPOSICIÓN DE LOS ORGANISMOS DEL SECTOR PÚBLICO, LA COMISIÓN, EL BANCO CENTRAL EUROPEO Y LOS ORGANISMOS DE LA UNIÓN EN RAZÓN DE UNA EMERGENCIA PÚBLICA»

6. Se suprimen los artículos 14 y 15.
7. Se inserta el artículo 15 *bis* siguiente:

«Artículo 15 bis

Obligación los tenedores de datos de poner a disposición datos en razón de una emergencia pública

1. Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión demuestre una necesidad excepcional de utilizar determinados datos para desempeñar sus funciones estatutarias de interés público al responder a una emergencia pública, mitigarla o apoyar la recuperación tras esta, podrá solicitar a los tenedores de datos que sean personas jurídicas, distintas de los organismos del sector público, que pongan a disposición dichos datos, incluidos los

metadatos necesarios para interpretar y utilizar tales datos. Previa solicitud debidamente motivada, los tenedores de datos pondrán los datos y metadatos a disposición del organismo del sector público solicitante, la Comisión, el Banco Central Europeo o el organismo de la Unión. Estas solicitudes también podrán formularse cuando se requiera la elaboración de estadísticas oficiales en relación con una emergencia pública.

2. Cuando los datos solicitados sean necesarios para responder a una emergencia pública y el organismo solicitante con arreglo al apartado 1 no pueda obtener tales datos por otros medios en el momento oportuno y de manera eficaz en condiciones equivalentes, la solicitud se referirá a datos no personales. Cuando el suministro de datos no personales sea insuficiente para hacer frente a la emergencia pública, también podrán solicitarse y, cuando sea posible, facilitarse datos personales en forma seudonimizada, sujetos a medidas técnicas y organizativas adecuadas para garantizar su protección.
3. Cuando los datos solicitados sean necesarios para mitigar o apoyar la recuperación tras una emergencia pública, los organismos solicitantes con arreglo al apartado 1, actuando sobre la base del Derecho de la Unión o nacional, podrán solicitar datos no personales específicos cuya carencia les impidan mitigar o apoyar la recuperación tras una emergencia pública. Tales solicitudes no se efectuarán a microempresas ni a pequeñas empresas.».
8. En el artículo 16, el apartado 2 se sustituye por el texto siguiente:

«2. El presente capítulo no se aplicará a las actividades realizadas por los organismos del sector público, a la Comisión, al Banco Central Europeo ni a los organismos de la Unión relativas a la prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas o de ejecución de sanciones penales, ni a la administración aduanera o tributaria. El presente capítulo no afectará al Derecho de la Unión o nacional que regule tales actividades.».
9. El artículo 17 se modifica como sigue:
 - a) el apartado 1 se modifica como sigue:
 - i) el texto de la parte introductoria se sustituye por el texto siguiente:

«Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión solicite datos con arreglo al artículo 15 *bis*, deberá:»;
 - ii) las letras b) y c) se sustituyen por el texto siguiente:
 - «b) demostrar que se cumplen las condiciones para presentar una solicitud con arreglo al artículo 15 *bis*;
 - c) explicar la finalidad de la solicitud, la utilización prevista de los datos solicitados, incluso, cuando proceda, por un tercero de conformidad con el apartado 4 del presente artículo, la duración de dicha utilización y, en su caso, la forma en que el tratamiento de los datos personales responde a la emergencia pública;»;
 - b) el apartado 2 se modifica como sigue:
 - i) la letra c) se sustituye por el texto siguiente:

«c) guardar proporción con la emergencia pública y estar debidamente motivada, por lo que respecta a la granularidad y el volumen de los datos solicitados y la frecuencia de acceso a los datos solicitados;»;

ii) se suprime la letra e);

c) se suprimen los apartados 5 y 6.

10. El artículo 18 se modifica como sigue:

a) en el apartado 2, el texto de la parte introductoria se sustituye por el texto siguiente:

«2. Sin perjuicio de las necesidades específicas relativas a la disponibilidad de datos definidas en el Derecho de la Unión o nacional, el tenedor de datos podrá denegar o solicitar la modificación de una solicitud de poner a disposición los datos con arreglo al presente capítulo sin demora indebida y, en cualquier caso, a más tardar cinco días hábiles después de la recepción de una solicitud con arreglo al artículo 15 *bis*, apartado 2, y sin demora indebida y, en cualquier caso, a más tardar treinta días hábiles después de la recepción de una solicitud en virtud del artículo 15 *bis*, apartado 3, por cualquiera de los motivos siguientes:»;

b) se suprime el apartado 5.

11. El artículo 19 se modifica como sigue:

a) en el apartado 1, el texto de la parte introductoria se sustituye por el texto siguiente:

«Un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión que reciba datos de conformidad con una solicitud presentada con arreglo al artículo 15 *bis*:»;

b) el apartado 3 se sustituye por el texto siguiente:

«3. La revelación de secretos comerciales a un organismo del sector público, a la Comisión, al Banco Central Europeo o a un organismo de la Unión se exigirá solo en la medida en que sea estrictamente necesario para cumplir la finalidad de una solicitud en virtud del artículo 15 *bis*. En tal caso, el tenedor de datos o, si no se trata de la misma persona, el poseedor del secreto comercial, identificará los datos protegidos como secretos comerciales, también en los metadatos pertinentes. El organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión adoptarán, antes de la revelación de los secretos comerciales, todas las medidas técnicas y organizativas necesarias y adecuadas para preservar la confidencialidad de los secretos comerciales, incluido, en su caso, el uso de cláusulas contractuales tipo, normas técnicas y la aplicación de códigos de conducta.».

12. El artículo 20 se sustituye por el texto siguiente:

«Artículo 20

Compensación por la puesta a disposición de datos conforme al capítulo V

1. Los tenedores de datos pondrán a disposición de forma gratuita los datos necesarios para responder a una emergencia pública con arreglo al artículo 15 *bis*, apartado 2. El organismo del sector público, la Comisión, el Banco Central

Europeo o el organismo de la Unión que haya recibido los datos dará reconocimiento público al tenedor de datos si este así lo solicita.

2. El tenedor de datos tendrá derecho a una compensación justa por poner a disposición datos en cumplimiento de una solicitud presentada con arreglo al artículo 15 *bis*, apartado 3. Tal compensación cubrirá los costes técnicos y organizativos soportados para dar cumplimiento a la solicitud, incluidos, en su caso, los costes de anonimización, seudonimización, agregación y de adaptación técnica, más un margen razonable. A petición del organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, el tenedor de datos proporcionará información sobre la base de cálculo de los costes y del margen razonable.

3. No obstante lo dispuesto en el apartado 1 del presente artículo, un tenedor de datos que sea una microempresa o una pequeña empresa podrá solicitar una compensación por la puesta a disposición de datos en respuesta a una solicitud con arreglo al artículo 15 *bis*, apartado 2, con arreglo a las condiciones establecidas en el apartado 2 del presente artículo.

4. Los tenedores de datos no tendrán derecho a una compensación por la puesta de datos a disposición en cumplimiento de una solicitud realizada con arreglo al artículo 15 *bis*, apartado 3, cuando la tarea específica desempeñada en interés público sea la elaboración de estadísticas oficiales y el Derecho nacional no permita la compra de datos. Los Estados miembros notificarán a la Comisión los casos en que el Derecho nacional no permita la compra de datos para la elaboración de estadísticas oficiales.».

13. El artículo 21 se modifica como sigue:

a) el título se sustituye por el texto siguiente:

«Intercambio de datos con organizaciones de investigación u organismos estadísticos obtenidos en el contexto de una emergencia pública»;

b) el apartado 5 se sustituye por el texto siguiente:

«5. Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión tenga la intención de transmitir o poner a disposición datos en aplicación del apartado 1, lo notificará sin demora indebida al tenedor de datos del que haya recibido los datos, indicando los elementos siguientes.

- a) la identidad y los datos de contacto de la organización o persona que recibe los datos;
- b) la finalidad de la transmisión o puesta a disposición de los datos;
- c) el período durante el cual se utilizarán los datos y la protección técnica;
- d) las medidas organizativas adoptadas, también cuando se trate de datos personales o secretos comerciales.».

14. El artículo 22 *bis* siguiente se inserta antes del capítulo VI:

«Artículo 22 *bis*

Derecho a presentar una reclamación

Cuando surja un litigio en relación con una solicitud de datos con arreglo al artículo 15 *bis*, como su denegación, su modificación, el nivel de compensación, o la transmisión o puesta a disposición de datos, el tenedor de datos, el organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión podrán presentar una reclamación ante la autoridad competente del Estado miembro en el que esté establecido el tenedor de datos, designada de conformidad con el artículo 37.».

15. En el artículo 31, se insertan los apartados 1 *bis* y 1 *ter* siguientes:

«1 *bis*. Las obligaciones establecidas en el capítulo VI, a excepción del artículo 29, y en el artículo 34 no se aplicarán a los servicios de tratamiento de datos distintos de los mencionados en el artículo 30, apartado 1, cuando el proveedor haya adaptado la mayoría de las características y funcionalidades del servicio de tratamiento de datos a las necesidades específicas del cliente, si la prestación de dichos servicios se basa en un contrato celebrado antes del 12 de septiembre de 2025 o en esa fecha.

El proveedor de dichos servicios de tratamiento de datos no estará obligado a renegociar o modificar un contrato para la prestación de tales servicios antes de su expiración si el contrato se celebró antes del 12 de septiembre de 2025 o en esa fecha. Cualquier disposición contractual contenida en el contrato que sea contraria al artículo 29, apartados 1, 2 o 3, se considerará nula y sin valor ni efecto alguno.

1 *ter*. Un proveedor de un servicio de tratamiento de datos podrá incluir disposiciones sobre sanciones proporcionadas por rescisión anticipada en un contrato de duración determinada relativo a la prestación de servicios de tratamiento de datos distintos de los mencionados en el artículo 30, apartado 1.

Cuando el proveedor de servicios de tratamiento de datos sea una pequeña y mediana empresa o una pequeña empresa de mediana capitalización, las obligaciones establecidas en el capítulo VI, a excepción del artículo 29, y en el artículo 34 no se aplicarán a los servicios de tratamiento de datos distintos de los mencionados en el artículo 30, apartado 1, si la prestación de dichos servicios se basa en un contrato celebrado antes del 12 de septiembre de 2025 o en esa fecha.

Cuando el proveedor de un servicio de tratamiento de datos sea una pequeña y mediana empresa o una pequeña empresa de mediana capitalización, el proveedor no estará obligado a renegociar o modificar un contrato para la prestación de un servicio de tratamiento de datos distinto de los mencionados en el artículo 30, apartado 1, antes de su vencimiento si dicho contrato se celebró antes del 12 de septiembre de 2025 o en esa fecha. Toda disposición contractual contenida en dicho contrato que sea contraria al artículo 29, apartados 1, 2 o 3, se considerará nula y sin valor ni efecto alguno.».

16. El artículo 32 se modifica como sigue:

- a) los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Los proveedores de servicios de tratamiento de datos, el organismo del sector público que ponga a disposición datos o documentos de conformidad con el capítulo VII *quater*, sección 3, la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VII *quater*, sección 3, los proveedores de servicios de

intermediación de datos o las organizaciones reconocidas de gestión de datos con fines altruistas adoptarán todas las medidas técnicas, organizativas y jurídicas adecuadas, lo que incluye la celebración de contratos, para impedir el acceso y la transferencia internacionales y por parte de las administraciones públicas de terceros países de datos no personales que se encuentren en la Unión, cuando dicha transferencia o acceso entren en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate, sin perjuicio de lo dispuesto en los apartados 2 o 3.

2. Las resoluciones o sentencias de órganos jurisdiccionales de un tercer país y las decisiones de autoridades administrativas de un tercer país en las que se exija a un proveedor de servicios de tratamiento de datos, al organismo del sector público que ponga a disposición datos o documentos de conformidad con el capítulo VII *quater*, sección 3, a la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VII *quater*, sección 3, a un proveedor de servicios de intermediación de datos o a una organización reconocida de gestión de datos con fines altruistas transferir o dar acceso a datos no personales incluidos en el ámbito de aplicación del presente Reglamento que se encuentren en la Unión solo se reconocerá o ejecutará de cualquier forma si se basan en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el tercer país solicitante y la Unión o entre el tercer país solicitante y un Estado miembro.»;

b) en el apartado 3, párrafo primero, la parte introductoria se sustituye por el texto siguiente:

«3. En ausencia de un acuerdo internacional de los contemplados en el apartado 2, cuando un proveedor de servicios de tratamiento de datos, el organismo del sector público que ponga a disposición datos o documentos de conformidad con el capítulo VII *quater*, sección 3, la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VII *quater*, sección 3, un proveedor de servicios de intermediación de datos o una organización reconocida de gestión de datos con fines altruistas sea el destinatario de una resolución o sentencia de un órgano jurisdiccional de un tercer país o de una decisión de una autoridad administrativa de un tercer país de transferir o dar acceso a datos no personales incluidos en el ámbito de aplicación del presente Reglamento que se encuentren en la Unión y el cumplimiento de dicha resolución, sentencia o decisión entrañe el riesgo de que el destinatario entre en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate, la transferencia a dichos datos o el acceso a los mismos por parte de dicha autoridad de un tercer país solo tendrá lugar cuando:»;

los apartados 4 y 5 se sustituyen por el texto siguiente:

«4. Si se cumplen las condiciones establecidas en los apartados 2 o 3, el proveedor de servicios de tratamiento de datos, el organismo del sector público que ponga a disposición datos o documentos de conformidad con el capítulo VII *quater*, sección 3, la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VII *quater*, sección 3, el proveedor de servicios de intermediación de datos o la organización reconocida de gestión de datos con fines altruistas proporcionará

la cantidad mínima de datos permitida en respuesta a una solicitud, sobre la base de la interpretación razonable de dicha solicitud por parte del proveedor o del organismo o autoridad nacional competente a que se refiere el apartado 3, párrafo segundo.

5. El proveedor de servicios de tratamiento de datos, el organismo del sector público que ponga a disposición datos o documentos de conformidad con el capítulo VII *quater*, sección 3, la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VII *quater*, sección 3, el proveedor de servicios de intermediación de datos o la organización reconocida de gestión de datos con fines altruistas informará a la persona física o jurídica cuyos derechos e intereses puedan verse afectados de la existencia de una solicitud de acceso a sus datos presentada por una autoridad de un tercer país antes de atender dicha solicitud, excepto en los casos en que la solicitud sirva a fines de aplicación de la ley y mientras sea necesario para preservar la eficacia de las actividades correspondientes de aplicación de la ley.».

17. Se suprime el artículo 36.
18. Se insertan los capítulos VII *bis*, VII *ter* y VII *quater* siguientes:

**«CAPÍTULO VII *bis*
SERVICIOS DE INTERMEDIACIÓN DE DATOS
Y ORGANIZACIONES DE GESTIÓN DE DATOS CON FINES ALTRUISTAS»**

Artículo 32 *bis*

Registros públicos de la Unión

- 1) La Comisión llevará y actualizará periódicamente registros públicos de la Unión de:
 - a) proveedores de servicios de intermediación de datos reconocidos y de
 - b) organizaciones reconocidas de gestión de datos con fines altruistas.
- 2) Los proveedores de servicios de intermediación de datos inscritos en el registro público de la Unión a que se refiere el apartado 1, letra a), podrán utilizar la denominación “proveedor de servicios de intermediación de datos reconocido en la Unión” en su comunicación oral y escrita, así como el logotipo común a que se refiere el apartado 4.
- 3) Las organizaciones de gestión de datos con fines altruistas inscritas en el registro público de la Unión a que se refiere el apartado 1, letra b), podrán utilizar la denominación “organización de gestión de datos con fines altruistas reconocida en la Unión” en sus comunicación oral y escrita, así como el logotipo común a que se refiere el apartado 4.
- 4) Con objeto de garantizar que los proveedores de servicios de intermediación de datos reconocidos en la Unión sean fácilmente identificables en toda la Unión, se faculta a la Comisión para adoptar actos de ejecución que establezcan un diseño para el logotipo común. Tales actos de ejecución se adoptarán de conformidad con el procedimiento consultivo a que se refiere el artículo 46, apartado 1 *bis*.

Artículo 32 *ter*

Autoridades competentes para la inscripción en el registro de proveedores de servicios de intermediación de datos y de organizaciones de gestión de datos con fines altruistas

- 1) Cada Estado miembro designará una o varias autoridades nacionales competentes para garantizar la aplicación y ejecución del presente capítulo de conformidad con el artículo 37, apartado 1.
- 2) Las autoridades competentes estarán creadas de manera que se garantice su independencia respecto de cualquier proveedor de servicios de intermediación de datos reconocido u organización reconocida de gestión de datos con fines altruistas.

Artículo 32 quater

Requisitos generales para la inscripción en el registro de proveedores de servicios de intermediación de datos reconocidos

Para poder inscribirse en el registro público de la Unión a que se refiere el artículo 32 *bis*, apartado 1, letra a), los proveedores de servicios de intermediación de datos deberán cumplir todos los requisitos siguientes:

- a) no utilizar los datos para los que prestan servicios de intermediación de datos con fines distintos de ponerlos a disposición de los usuarios de datos;
- b) que los datos que recojan con respecto a cualquier actividad de una persona física o jurídica a efectos de la prestación del servicio de intermediación de datos, incluidos los datos de fecha, hora y geolocalización, la duración de la actividad y las conexiones con otras personas físicas o jurídicas establecidas por la persona que utilice el servicio de intermediación de datos, se utilicen únicamente para el desarrollo de dicho servicio de intermediación de datos;
- c) que, cuando ofrezcan herramientas y servicios adicionales a los tenedores de datos o a los interesados con el fin específico de facilitar el intercambio de datos, como el almacenamiento temporal, la curación, la conversión, el cifrado, la anonimización y la seudonimización, dichas herramientas y servicios solo se utilicen a petición explícita o con la aprobación del tenedor de datos o del interesado;
- d) que, cuando los proveedores de servicios de intermediación de datos que no sean microempresas ni pequeñas empresas ofrezcan a sus clientes servicios de valor añadido distintos de los servicios a que se refiere la letra c), cumplan las siguientes condiciones:
 - i) que los servicios de valor añadido sean solicitados explícitamente por el usuario;
 - ii) que los datos no se utilicen para fines distintos de la prestación del servicio de valor añadido;
 - iii) que los servicios de valor añadido se ofrezcan a través de una entidad funcionalmente independiente;
 - iv) que la empresa que desee ofrecer servicios de valor añadido no esté designada como guardián de acceso de conformidad con el artículo 3 del Reglamento (UE) 2022/1925;
 - v) que las condiciones comerciales, incluida la fijación de precios, para la prestación de servicios de intermediación de datos a un titular o usuario de datos no dependan de si el tenedor o usuario de datos utiliza servicios

de valor añadido prestados por el proveedor de servicios de intermediación de datos o por una entidad vinculada;

- e) que los proveedores de servicios de intermediación de datos que ofrezcan servicios a los interesados actúen en el mejor interés de estos cuando faciliten el ejercicio de sus derechos, en particular, informándolos y, cuando corresponda, asesorándolos de manera concisa, transparente, inteligible y fácilmente accesible sobre los usos previstos de los datos por los usuarios de datos y las condiciones generales aplicables a dichos usos antes de que los interesados presten su consentimiento.

Artículo 32 *quinquies*

Requisitos generales para la inscripción en el registro de organizaciones reconocidas de gestión de datos con fines altruistas

Para poder inscribirse en el registro público de la Unión a que se refiere el artículo 32 *bis*, apartado 1, letra b), las organizaciones de gestión de datos con fines altruistas deberán cumplir todos los requisitos siguientes:

- a) ejercer actividades de cesión altruista de datos;
- b) ser una entidad jurídica constituida con arreglo al Derecho nacional para cumplir objetivos de interés general, según se disponga en el Derecho nacional, cuando corresponda;
- c) ejercer su actividad sin ánimo de lucro y ser jurídicamente independiente de cualquier entidad que ejerza su actividad con fines lucrativos;
- d) ejercer sus actividades de cesión altruista de datos a través de una estructura que esté funcionalmente separada de sus restantes actividades.

Artículo 32 *sexies*

Registro

- 1) Los proveedores de servicios de intermediación de datos que cumplan los requisitos establecidos en el artículo 32 *quater* podrán presentar una solicitud de inscripción en el registro público de la Unión de proveedores de servicios de intermediación de datos reconocidos a la autoridad competente a que se refiere el artículo 32 *ter* del Estado miembro en el que tengan su establecimiento principal.

Las organizaciones de gestión de datos con fines altruistas que cumplan los requisitos establecidos en el artículo 32 *quinquies* podrán presentar una solicitud de inscripción en el registro público de la Unión de organizaciones reconocidas de gestión de datos con fines altruistas a la autoridad competente a que se refiere el artículo 32 *ter* del Estado miembro en el que tengan su establecimiento principal.

- 2) Los proveedores de servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas que no tengan su establecimiento principal en la Unión designarán un representante legal en uno de los Estados miembros. El representante legal contará con un mandato para que las autoridades competentes, los interesados y los tenedores de datos se pongan en contacto con él además o en lugar del proveedor de servicios de intermediación de datos o de la organización de gestión de datos con fines altruistas. El representante legal cooperará con las autoridades competentes y les demostrará de forma exhaustiva, previa solicitud, las medidas y disposiciones adoptadas por el proveedor de servicios de intermediación de datos o por la organización de gestión de datos con fines altruistas a fin de garantizar el cumplimiento del presente Reglamento.

Se considerará que el proveedor de servicios de intermediación de datos o la organización de gestión de datos con fines altruistas está bajo la jurisdicción del Estado miembro en el que esté ubicado el representante legal. La designación de un representante legal se entenderá sin perjuicio de las acciones legales que pudieran emprenderse contra el proveedor de servicios de intermediación de datos o la organización de gestión de datos con fines altruistas.

- 3) Las autoridades competentes establecerán los formularios de solicitud necesarios.
- 4) Cuando un proveedor de servicios de intermediación de datos haya presentado toda la información necesaria con arreglo al apartado 3 del presente artículo y cumpla los requisitos establecidos en el artículo 32 *quater*, la autoridad competente adoptará, en un plazo de doce semanas a partir de la recepción de la solicitud de registro, una decisión sobre si el proveedor cumple los criterios establecidos en el artículo 32 *quater*. Cuando el proveedor cumpla los criterios, la autoridad competente presentará la información pertinente a la Comisión, que la inscribirá en el registro público de la Unión como proveedor de servicios de intermediación de datos reconocido.

El párrafo primero también se aplicará cuando una organización de gestión de datos con fines altruistas haya presentado toda la información necesaria con arreglo al apartado 2 y cumpla los requisitos de registro establecidos en el artículo 32 *quinquies*.

La inscripción en el registro público de la Unión tendrá validez en todos los Estados miembros.

- 5) La autoridad competente podrá cobrar tasas por el registro de conformidad con el Derecho nacional. Tales tasas serán proporcionadas y objetivas y se basarán en los costes administrativos relacionados con la supervisión del cumplimiento. En el caso de las pequeñas empresas de mediana capitalización, las pequeñas y medianas empresas y las empresas emergentes, la autoridad competente podrá cobrar una tasa con descuento o eximir de ella.
- 6) Las entidades registradas notificarán a la autoridad competente cualquier cambio posterior en la información facilitada durante el proceso de solicitud o cuando cesen sus actividades de intermediación de datos o de cesión altruista de datos en la Unión.
- 7) La autoridad competente comunicará sin demora y por medios electrónicos a la Comisión toda notificación contemplada en el apartado 6. La Comisión actualizará sin demora indebida el registro público de la Unión.

Artículo 32 *septies*

Obligaciones de las organizaciones reconocidas de gestión de datos con fines altruistas

- 1) La organización reconocida de gestión de datos con fines altruistas comunicará a los interesados o a los tenedores de datos, de una manera clara y sencilla de entender, antes de todo tratamiento de sus datos, los elementos siguientes:
 - a) los objetivos de interés general y, en su caso, los fines específicos, explícitos y legítimos con que se tratarán los datos personales, y para los que permite que sus datos sean tratados por un usuario de datos;
 - b) la ubicación del tratamiento que se efectúe en un tercer país y sobre los objetivos de interés general para los que lo permita, cuando sea la propia organización reconocida de gestión de datos con fines altruistas la que efectúe el tratamiento.

- 2) La organización reconocida de gestión de datos con fines altruistas no utilizará los datos para objetivos distintos de los de interés general para los que el interesado o el titular de datos permita el tratamiento. La organización reconocida de gestión de datos con fines altruistas no utilizará prácticas de mercadotecnia engañosas para solicitar la entrega de datos.
- 3) La organización reconocida de gestión de datos con fines altruistas proporcionará medios electrónicos para obtener el consentimiento de los interesados o el permiso para tratar los datos facilitados por los tenedores de datos, así como para su retirada.
- 4) La organización reconocida de gestión de datos con fines altruistas informará sin demora a los tenedores de datos en caso de transferencia, acceso o utilización no autorizados de los datos no personales que haya compartido.
- 5) Cuando la organización reconocida de gestión de datos con fines altruistas facilite el tratamiento de datos por terceros, en particular, proporcionando herramientas para obtener el consentimiento de los interesados o el permiso para tratar los datos facilitados por los tenedores de datos, especificará, cuando corresponda, el tercer país en el que se pretenda utilizar los datos.

Artículo 32 *octies*

Supervisión del cumplimiento

- 1) Las autoridades competentes a que se refiere el artículo 32 *ter* controlarán y supervisarán, por iniciativa propia o a petición de una persona física o jurídica, si los proveedores de servicios de intermediación de datos reconocidos y las organizaciones reconocidas de gestión de datos con fines altruistas cumplen los requisitos establecidos en el presente capítulo, en particular si siguen cumpliendo los requisitos de registro establecidos en el mismo.
- 2) Las autoridades competentes estarán facultadas para solicitar a los proveedores de servicios de intermediación de datos reconocidos o a las organizaciones reconocidas de gestión de datos con fines altruistas, o a su representante legal, toda la información que sea necesaria para verificar el cumplimiento de los requisitos establecidos en el presente capítulo. Toda solicitud de información guardará proporción con respecto al cumplimiento de la tarea y estará motivada.
- 3) Cuando la autoridad competente halle que un proveedor de servicios de intermediación reconocido o una organización reconocida de gestión de datos con fines altruistas no cumple uno o varios de los requisitos del presente capítulo, notificará sus observaciones a dicha entidad, o a su representante legal, y le dará la oportunidad de manifestar su opinión al respecto en un plazo de treinta días a partir de la recepción de la notificación.
- 4) La autoridad competente estará facultada para exigir el cese del incumplimiento a que se refiere el apartado 3, bien inmediatamente, bien dentro de un plazo razonable, y adoptará medidas adecuadas y proporcionadas con el objetivo de garantizar el cumplimiento.
- 5) Si un proveedor de servicios de intermediación de datos reconocido o una organización reconocida de gestión de datos con fines altruistas no cumple uno o varios de los requisitos establecidos en el presente capítulo, incluso después de haber sido notificada de conformidad con el apartado 3, dicha entidad:

- a) perderá su derecho a utilizar la denominación a que se refiere el artículo 32 *bis* en su comunicación oral y escrita;
- b) será eliminada del registro público de la Unión a que se refiere el artículo 32 *bis*.

La autoridad competente hará pública toda decisión por la que se revoque el derecho a utilizar la denominación a que se refiere el párrafo primero, letra a).».

«CAPÍTULO VII *ter*

Libre circulación de datos no personales en la Unión»

«Artículo 32 *nonies*

Prohibición de los requisitos de localización de los datos no personales dentro de la Unión

- 1) Los requisitos de localización de datos para los datos no personales estarán prohibidos, a menos que estén justificados por razones de seguridad pública de conformidad con el principio de proporcionalidad o establecidos sobre la base del Derecho de la Unión.
- 2) Los Estados miembros comunicarán inmediatamente a la Comisión cualquier proyecto de acto que introduzca un nuevo requisito de localización de datos o modifique uno existente, de conformidad con los procedimientos establecidos en los artículos 5, 6 y 7 de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo.».

«CAPÍTULO VII *quater*

Reutilización de datos y documentos que obren en poder de organismos del sector público

SECCIÓN 1

DISPOSICIONES GENERALES

Artículo 32 *decies*

Objeto y ámbito de aplicación

- 1) El presente capítulo establece un conjunto de normas que regulan la reutilización y las disposiciones prácticas para facilitar la reutilización de los elementos siguientes:
 - a) los datos y documentos existentes que obren en poder de los organismos del sector público de los Estados miembros, incluidas determinadas categorías de datos protegidos;
 - b) los documentos y datos existentes que obren en poder de empresas públicas:
 - i) que lleven a cabo su actividad en los ámbitos a que se refiere el capítulo II de la Directiva 2014/25/UE del Parlamento Europeo y del Consejo;

- ii) que actúen como operadores de servicio público con arreglo al artículo 2 del Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo;
 - iii) que actúen como compañías aéreas que cumplen obligaciones de servicio público con arreglo al artículo 16 del Reglamento (CE) n.º 1008/2008 del Parlamento Europeo y del Consejo; o
 - iv) que actúen como armadores comunitarios que cumplen obligaciones de servicio público con arreglo al artículo 4 del Reglamento (CEE) n.º 3577/92 del Consejo;
- c) los datos de investigación, con arreglo a las condiciones establecidas en el artículo 32 *unvicies*.
- 2) El presente capítulo no se aplicará a los elementos siguientes:
- a) los datos y los documentos cuyo suministro sea una actividad que se salga del ámbito de la misión de servicio público de los organismos del sector público afectados, definida con arreglo a la legislación o a otras normas de obligado cumplimiento del Estado miembro, o en ausencia de tales normas, definida con arreglo a la práctica administrativa común del Estado miembro en cuestión, siempre y cuando el ámbito de las misiones de servicio público sea transparente y se someta a revisión;
 - b) los datos y documentos que obren en poder de empresas públicas:
 - i) producidos fuera del ámbito de la prestación de servicios de interés general, según se defina en la legislación o en otras normas de obligado cumplimiento del Estado miembro;
 - ii) relativos a actividades sometidas directamente a la competencia y, por tanto, conforme al artículo 34 de la Directiva 2014/25/UE, no sujetas a las normas de contratación;
 - c) los datos y documentos, como los datos sensibles, a los que no pueda accederse en virtud de regímenes de acceso del Estado miembro por motivos de protección de la seguridad nacional (a saber, la seguridad del Estado), la defensa o la seguridad pública;
 - d) los datos y documentos que obren en poder de organismos públicos de radiodifusión y sus filiales, así como los datos que obren en poder de otros organismos o sus filiales para el cumplimiento de una misión de servicio público de radiodifusión.
- 3) La sección 2 del presente capítulo no se aplicará a los elementos siguientes:
- a) los datos o documentos, por ejemplo los datos o documentos sensibles, a los que no pueda accederse en virtud de regímenes de acceso de los Estados miembros por motivos, entre otros, de:
 - i) confidencialidad estadística;
 - ii) confidencialidad comercial (incluidos secretos comerciales, profesionales o empresariales);
 - b) los datos o documentos cuyo acceso esté limitado en virtud de regímenes de acceso de los Estados miembros,

- i) incluidos, entre otros, aquellos casos en los que los ciudadanos o personas jurídicas tengan que demostrar un interés particular en obtener acceso a los documentos;
 - ii) por motivos de protección de los datos personales, y las partes de datos o documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales o como un menoscabo de la protección de la intimidad y la integridad de las personas, en particular de conformidad con la legislación nacional o de la Unión sobre protección de datos personales; logotipos, divisas e insignias;
- c) los datos o documentos sobre los que existan derechos de propiedad intelectual por parte de terceros;
 - d) los datos o documentos conservados por instituciones culturales que no sean bibliotecas, incluidas las universitarias, museos y archivos;
 - e) los datos o documentos en poder de instituciones educativas de nivel secundario e inferior y, en el caso de todas las demás instituciones educativas, los datos distintos de los contemplados en el apartado 1, letra c);
 - f) los datos o documentos distintos de los mencionados en el apartado 1, letra c), que obren en poder de organizaciones que realizan actividades de investigación y organizaciones que financian la investigación, incluidas las organizaciones creadas para la transferencia de los resultados de la investigación;
 - g) datos o documentos cuyo acceso esté excluido o limitado por motivos de información relativa a la protección de entidades críticas o de infraestructuras críticas, tal como se define en el artículo 2, puntos 1 y 4, de la Directiva (UE) 2022/2557.
- 4) La sección 3 del presente capítulo no se aplicará a los elementos siguientes:
- a) los datos y documentos que no pertenezcan a determinadas categorías de datos protegidos;
 - b) los datos y documentos que obren en poder de empresas públicas;
 - c) los datos y documentos que obren en poder de centros culturales y de enseñanza;
 - d) los datos y documentos contemplados en la sección 2 del presente capítulo.
- 5) El presente capítulo se basa en los regímenes de acceso nacionales y de la Unión, y se entiende sin perjuicio de ellos, en particular en lo que se refiere a la concesión de acceso a documentos oficiales y a su divulgación.
- 6) Las obligaciones impuestas de conformidad con el presente capítulo solo se aplicarán en la medida en que sean compatibles con las disposiciones de los acuerdos internacionales sobre protección de los derechos de propiedad intelectual, en particular el Convenio de Berna para la protección de las obras literarias y artísticas (Convenio de Berna), el Acuerdo sobre aspectos de los derechos de propiedad intelectual relacionados con el comercio (Acuerdo ADPIC) y el Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor.

- 7) Los organismos del sector público no ejercerán el derecho del fabricante de una base de datos, previsto en el artículo 7, apartado 1, de la Directiva 96/9/CE, para evitar la reutilización de datos o documentos o restringir la reutilización más allá de los límites establecidos por el presente capítulo.
- 8) El presente capítulo regula la reutilización de los datos y documentos existentes que obran en poder de los organismos del sector público y las empresas públicas de los Estados miembros, incluidos los datos y documentos a los que se aplica la Directiva 2007/2/CE del Parlamento Europeo y del Consejo.
- 9) El presente capítulo se entenderá sin perjuicio del Derecho de la Unión y del Derecho nacional, así como de los acuerdos internacionales en los que la Unión o los Estados miembros sean parte sobre la protección de las categorías de datos o documentos a que se refiere el artículo 2, punto 54.

Artículo 32 undecies

No discriminación

- 1) Toda condición aplicable a la reutilización de datos o documentos deberá ser no discriminatoria, transparente, proporcionada y estar objetivamente justificada en relación con las categorías de datos o documentos y los fines de la reutilización y la naturaleza de los datos o documentos cuya reutilización se permite. Dichas condiciones no podrán utilizarse para restringir la competencia. Este principio se aplicará igualmente a categorías comparables de reutilización, incluida la reutilización transfronteriza.
- 2) Si un organismo del sector público reutiliza datos o documentos como parte de sus actividades comerciales ajenas a su misión de servicio público, deberán aplicarse a la entrega de los datos o documentos para dichas actividades las mismas tarifas y condiciones que se apliquen a los demás reutilizadores.

Artículo 32 duodecies

Acuerdos exclusivos

- 1) La reutilización de datos o documentos estará abierta a todos los agentes potenciales del mercado, incluso en caso de que uno o más de los agentes exploten ya productos con valor añadido basados en estos datos o documentos. Quedan prohibidos los acuerdos u otros pactos o prácticas relativos a la reutilización de datos o documentos que tengan por objeto o efecto conceder derechos exclusivos o restringir la disponibilidad de datos o documentos para su reutilización por entidades distintas de las partes en dichos acuerdos, mecanismos o prácticas.
- 2) No obstante lo dispuesto en el apartado 1, cuando sea necesario un derecho exclusivo para la prestación de un servicio de interés general, dicho derecho podrá concederse en la medida necesaria para la prestación del servicio o el suministro del producto en las siguientes condiciones:
 - a) el derecho exclusivo se concede mediante un acto administrativo o un acuerdo contractual de conformidad con el Derecho de la Unión y el Derecho nacional aplicable y de conformidad con los principios de transparencia, igualdad de trato y no discriminación;

- b) los acuerdos que conceden el derecho exclusivo, incluidas las razones por las que es necesario concederlo, son transparentes y se ponen a disposición del público en línea, de una forma que se ajuste a la legislación pertinente de la Unión en materia de contratación pública y al Derecho nacional;
 - c) excepto en el caso de los derechos exclusivos relacionados con la digitalización de recursos culturales, la validez del motivo de la concesión de derechos exclusivos relativos a los datos y documentos incluidos en el ámbito de aplicación de la sección 2 estará sujeta a revisión periódica y, en cualquier caso, se revisará cada tres años;
 - d) los acuerdos exclusivos establecidos a partir del 16 de julio de 2019 se pondrán a disposición del público en línea al menos dos meses antes de su entrada en vigor. Las condiciones finales de tales acuerdos serán transparentes y se pondrán a disposición del público en línea.
- 3) No obstante lo dispuesto en el apartado 1, cuando exista un derecho exclusivo relacionado con la digitalización de los recursos culturales, el período de exclusividad no será superior, por regla general, a diez años. En el caso de que dicho período sea superior a diez años, su duración será conforme con el Derecho de la Unión y el Derecho nacional aplicables y se revisará al undécimo año y, si procede, cada siete años a partir de entonces.
- 4) Cuando exista un derecho exclusivo en el sentido del apartado 3 deberá facilitarse gratuitamente al organismo del sector público en cuestión, como parte de dichos acuerdos, una copia de los recursos culturales digitalizados. Esa copia estará disponible para su reutilización una vez finalizado el período de exclusividad.
- 5) Para determinadas categorías de datos protegidos, la duración de un derecho exclusivo a reutilizar datos no excederá de doce meses. Cuando se celebre un contrato, la duración de este será la misma que la del derecho exclusivo.
- 6) Los acuerdos u otros pactos o prácticas que, sin conceder expresamente un derecho exclusivo, tengan como objetivo, o quepa esperar razonablemente que impliquen, una disponibilidad limitada para la reutilización de datos y documentos incluidos en el ámbito de aplicación de la sección 2 por parte de entidades distintas de las partes de dichos acuerdos, se pondrán a disposición del público en línea al menos dos meses antes de su entrada en vigor. El efecto de estos acuerdos jurídicos o prácticos sobre la disponibilidad de datos para su reutilización estará sujeto a revisiones periódicas y, en cualquier caso, se someterá a revisión cada tres años. Las condiciones finales de tales acuerdos serán transparentes y se pondrán a disposición del público en línea.
- 7) En el caso de los acuerdos exclusivos existentes, se aplicará lo siguiente:
- a) los acuerdos exclusivos relativos a los datos y documentos incluidos en el ámbito de aplicación de la sección 2 existentes el 17 de julio de 2013 a los que no se apliquen las excepciones contempladas en los apartados 2 y 3 y que fuesen celebrados por organismos del sector público concluirán cuando expire el contrato y, en cualquier caso, a más tardar el 18 de julio de 2043;
 - b) los acuerdos exclusivos relativos a los datos y documentos incluidos en el ámbito de aplicación de la sección 2 existentes el 16 de julio de 2019 a los que no se apliquen las excepciones contempladas en los apartados 2 y 3 y que fuesen celebrados por empresas públicas concluirán cuando expire el contrato y, en cualquier caso, a más tardar el 17 de julio de 2049.

Artículo 32 *terdecies*

Principios generales relativos a las tarifas

- 1) Las tarifas establecidas en las secciones 2 o 3 serán transparentes, no discriminatorias, proporcionadas y objetivamente justificadas y no restringirán la competencia.
- 2) En el caso de tarifas estándar para la reutilización de datos o documentos, las condiciones aplicables, así como el importe de dichas tarifas, incluida su base de cálculo, se fijarán de antemano y se publicarán, mediante medios electrónicos cuando resulte posible y oportuno.
- 3) Cuando se trate de tarifas para la reutilización distintas de las mencionadas en el apartado 1, los factores que se tendrán en cuenta para el cálculo de dichas tarifas se indicarán por adelantado. Cuando se solicite, el titular de los datos o documentos de que se trate también indicará cómo se han calculado dichas tarifas en relación con una solicitud de reutilización concreta.
- 4) Los organismos del sector público garantizarán que el pago de las tarifas también pueda efectuarse en línea, a través de servicios transfronterizos de pago de uso generalizado, sin discriminación por razón del lugar de establecimiento del proveedor del servicio de pago, el lugar de emisión del instrumento de pago o la ubicación de la cuenta de pago dentro de la Unión.

Artículo 32 *quaterdecies*

Información sobre las vías de recurso

Los organismos del sector público se asegurarán de que los solicitantes de reutilización de datos o documentos estén informados de las vías de recurso de que disponen para impugnar las decisiones y las prácticas que les afecten.

SECCIÓN 2

REUTILIZACIÓN DE DATOS ABIERTOS DE LAS ADMINISTRACIONES PÚBLICAS

Subsección 1 *Ámbito de aplicación y principios generales*

Artículo 32 *quincecies*

Principio general de reutilización de los datos abiertos de las administraciones públicas

- 1) Los datos o documentos incluidos en el ámbito de aplicación de la presente sección serán reutilizables para fines comerciales o no comerciales de conformidad con la sección 1 y la sección 2, subsección 3.
- 2) En el caso de los datos o documentos respecto de los que las bibliotecas, incluidas las universitarias, los museos y los archivos posean derechos de propiedad intelectual, y en el caso de los datos o documentos que obren en poder de empresas públicas, cuando se permita la reutilización de dichos datos o documentos, tales datos o documentos podrán ser reutilizados para fines comerciales o no comerciales de conformidad con la sección 1 y la sección 2, subsección 3.

Subsección 2

Solicitudes de reutilización

Artículo 32 *sexdecies*

Tratamiento de las solicitudes de reutilización

- 1) Los organismos del sector público tramitarán, por medios electrónicos cuando resulte posible y oportuno, las solicitudes de reutilización y pondrán el documento a disposición del solicitante con vistas a su reutilización o, si es necesaria una licencia, ultimarán la oferta de licencia al solicitante en un plazo razonable coherente con los plazos establecidos para el tratamiento de solicitudes de acceso a los datos o documentos.
- 2) Cuando no se haya establecido ningún plazo ni otras normas que regulen la entrega oportuna de los datos o documentos, los organismos del sector público tramitarán la solicitud y entregarán los datos o documentos al solicitante con vistas a su reutilización o, si es necesaria una licencia, ultimarán la oferta de licencia al solicitante lo antes posible o, en cualquier caso, en un plazo de veinte días hábiles, a partir del momento de su recepción. Dicho plazo podrá ampliarse en otros veinte días hábiles para solicitudes extensas o complejas. En tales casos, se notificará al solicitante lo antes posible y, en cualquier caso, en el curso de las tres semanas siguientes a la solicitud inicial que se necesita más tiempo para tramitarla y las razones que lo justifican.
- 3) En caso de adoptarse una decisión negativa, los organismos del sector público comunicarán al solicitante los motivos de la denegación con arreglo a las disposiciones aplicables del régimen de acceso de dicho Estado miembro o de las disposiciones del presente Reglamento, en particular el artículo 32 *decies*, apartado 2, letras a) a c), y apartado 3, letras a) a d), o el artículo 32 *quindecies* (principios generales, sección sobre reutilización de datos abiertos de la administración pública). Si la Decisión negativa se basa en el artículo 32 *decies*, apartado 3, letra d), el organismo del sector público incluirá una referencia a la persona física o jurídica titular de los derechos, cuando esta sea conocida, o, alternativamente, al cedente del que el organismo del sector público haya obtenido el material en cuestión. Las bibliotecas, incluidas las universitarias, los museos y los archivos no estarán obligados a incluir tal referencia.
- 4) Las vías de recurso incluirán la posibilidad de revisión por un órgano de revisión imparcial con la experiencia técnica adecuada, como la autoridad nacional de competencia, la autoridad reguladora del acceso a los datos o documentos correspondiente, una autoridad nacional de supervisión establecida de conformidad con el Reglamento (UE) 2016/679 o una autoridad judicial nacional, cuyas decisiones sean vinculantes para el organismo del sector público afectado.
- 5) A efectos del presente artículo, los Estados miembros definirán dispositivos prácticos para facilitar la reutilización eficaz de los datos o documentos. Dichos dispositivos podrán incluir, en particular, modalidades para proporcionar información adecuada sobre los derechos previstos en el presente Reglamento y ofrecer ayuda y orientación pertinentes.
- 6) El presente artículo no se aplicará a las siguientes entidades:
 - a) empresas públicas;

- b) centros de enseñanza, organizaciones que realizan actividades de investigación y organizaciones que financian la investigación.

Subsección 3

Condiciones de la reutilización

Artículo 32 *septdecies*

Formatos disponibles

- 1) Sin perjuicio de la subsección 5, los organismos del sector público y las empresas públicas facilitarán sus datos o documentos en cualquier formato o lengua en que existan previamente y, siempre que sea posible y apropiado, por medios electrónicos, en formas o formatos que sean abiertos, legibles por máquina, accesibles, fáciles de localizar y reutilizables, conjuntamente con sus metadatos. Tanto el formato como los metadatos cumplirán, cuando sea posible, normas formales abiertas.
- 2) Los Estados miembros animarán a los organismos del sector público y a las empresas públicas a elaborar y facilitar datos o documentos incluidos en el ámbito de aplicación de la presente sección con arreglo al principio de “documentos abiertos desde el diseño y por defecto”.
- 3) El apartado 1 no supone que los organismos del sector público estén obligados, para cumplir dicho apartado, a crear datos o documentos, adaptarlos o facilitar extractos de ellos, cuando esto suponga un esfuerzo desproporcionado que conlleve algo más que una operación simple.
- 4) Con arreglo a la presente Directiva, no podrá exigirse a los organismos del sector público que mantengan la producción y el almacenamiento de determinados tipos de datos o documentos con vistas a su reutilización por una entidad del sector privado o público.
- 5) Los organismos del sector público pondrán a disposición datos dinámicos para su reutilización inmediatamente después de su recopilación, a través de las API adecuadas y, cuando proceda, en forma de descarga masiva.
- 6) Cuando la puesta a disposición de datos dinámicos para su reutilización inmediatamente después de su recopilación, con arreglo al apartado 5, pueda superar las capacidades financieras y técnicas del organismo del sector público, suponiendo así un esfuerzo desproporcionado, esos datos dinámicos se pondrán a disposición para su reutilización en un plazo o con restricciones técnicas temporales que no perjudiquen indebidamente la explotación de su potencial económico y social.
- 7) Los apartados 1 a 6 se aplicarán a los datos o documentos que obren en poder de las empresas públicas y que estén disponibles para su reutilización.
- 8) Los conjuntos de datos de alto valor, tal que relacionados conforme al artículo 32 *terdecies*, apartado 1, se pondrán a disposición para su reutilización en un formato legible por máquina, a través de las API adecuadas y, cuando proceda, en forma de descarga masiva.

Artículo 32 *octodecies*

Principios que rigen la tarificación de los datos abiertos de las administraciones públicas

- 1) La reutilización de datos o documentos en el ámbito de aplicación de la presente sección será gratuita. No obstante, el organismo del sector público que posea los datos podrá recuperar los costes marginales en que se incurra para la reproducción,

puesta a disposición y difusión de tales datos o documentos, así como para la anonimización de datos personales y las medidas adoptadas para proteger información comercial confidencial.

- 2) El apartado 1 no se aplicará a las entidades siguientes:
 - a) los organismos del sector público a los que se exija generar ingresos para cubrir una parte sustancial de sus costes relativos a la realización de sus misiones de servicio público;
 - b) las bibliotecas, incluidas las universitarias, los museos y los archivos;
 - c) las empresas públicas.
- 3) Los Estados miembros publicarán en línea una lista de organismos del sector público a que se refiere el apartado 2, letra a).
- 4) En los casos a los que se hace referencia en el apartado 2, letras a) y c), el precio total se calculará conforme a criterios objetivos, transparentes y comprobables. Los Estados miembros establecerán dichos criterios. Los ingresos totales obtenidos por suministrar datos o documentos y autorizar su reutilización durante el ejercicio contable apropiado no superarán el coste de su recogida, producción, reproducción, difusión y almacenamiento de datos, incrementado por un margen de beneficio razonable de la inversión y, en su caso, anonimización de datos personales y medidas adoptadas para proteger información comercial confidencial. Las tarifas se calcularán conforme a los principios contables aplicables.
- 5) Cuando sean los organismos del sector público mencionados en el apartado 2, letra b), los que apliquen tarifas, los ingresos totales obtenidos por suministrar y autorizar la reutilización de datos o documentos durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión, almacenamiento de datos, conservación y compensación de derechos y, en su caso, anonimización de datos personales y medidas adoptadas para proteger información comercial confidencial, incrementado por un margen de beneficio razonable de la inversión. Las tarifas se calcularán conforme a los principios contables aplicables a los organismos del sector público correspondientes.
- 6) Los organismos del sector público podrán establecer tarifas más elevadas que las previstas en los apartados 1, 4 y 5 para la reutilización de datos y documentos por parte de empresas muy grandes. Tales tasas serán proporcionadas y se basarán en criterios objetivos, teniendo en cuenta el poder económico o la capacidad de la entidad para adquirir datos, incluida, en particular, la designación como guardián de acceso con arreglo al Reglamento (UE) 2022/1925. Además de los elementos enumerados en el apartado 1 del presente artículo, dichos gastos podrán cubrir el coste de recogida, producción, difusión, reproducción y almacenamiento de los datos y, en su caso, el coste de la anonimización o las medidas para proteger la confidencialidad de los datos o documentos, incrementado por un margen de beneficio razonable de la inversión.
- 7) Los usuarios podrán reutilizar gratuitamente:
 - a) a reserva de lo dispuesto en el artículo 32 *tervicies*, apartados 3, 4 y 5, los conjuntos de datos de alto valor, tal que relacionados de conformidad con el apartado 1 de dicho artículo;
 - b) los datos de investigación contemplados en el artículo 32 *decies*, apartado 1, letra c).

Artículo 32 *novodecies*

Licencias tipo

- 1) La reutilización de datos o documentos no estará sujeta a condiciones, a menos que dichas condiciones sean objetivas, proporcionadas, no discriminatorias y estén justificadas por un objetivo de interés público.
- 2) Cuando la reutilización esté sujeta a condiciones, tales condiciones no restringirán sin necesidad las posibilidades de reutilización y no se usarán para restringir la competencia.
- 3) En los Estados miembros en que se utilicen licencias, los organismos del sector público velarán por que las licencias tipo para la reutilización de documentos del sector público, que podrán adaptarse para responder a aplicaciones concretas de la licencia, estén disponibles en formato digital y puedan ser procesadas electrónicamente.
- 4) Los organismos del sector público podrán establecer condiciones especiales para la reutilización de datos y documentos por parte de empresas muy grandes. Tales condiciones deberán ser proporcionadas y basarse en criterios objetivos. Se establecerán teniendo en cuenta el poder económico o la capacidad de la entidad para adquirir datos, incluida, en particular, una designación como guardián de acceso con arreglo al Reglamento (UE) 2022/1925.

Artículo 32 *vicies*

Disposiciones prácticas

- 1) Los Estados miembros crearán dispositivos prácticos que faciliten la búsqueda de los datos o documentos disponibles para su reutilización, tales como listados de datos o documentos principales con los metadatos pertinentes, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina, y portales conectados a los listados descentralizados. En la medida de lo posible, los Estados miembros facilitarán la búsqueda lingüística de los datos o documentos en varios idiomas, en particular permitiendo la agregación de metadatos a escala de la Unión.

Los Estados miembros también promoverán la creación por los organismos del sector público de dispositivos prácticos que faciliten la conservación de los datos o documentos disponibles para su reutilización.

- 2) Los Estados miembros en cooperación con la Comisión, continuarán los esfuerzos de simplificación del acceso a conjuntos de datos, en particular proporcionando un único punto de acceso y poniendo progresivamente a disposición conjuntos de datos adecuados que obren en poder de organismos del sector público en relación con todos los datos o documentos a los que aplica la presente sección, así como con datos que obren en poder de las instituciones de la Unión, en formatos que sean accesibles, fáciles de localizar y reutilizables por medios electrónicos.

Subsección 4

Datos de investigación

Artículo 32 *unvicies*

Datos de investigación

- 1) Los Estados miembros apoyarán la disponibilidad de los datos de investigación mediante la adopción de políticas nacionales y actuaciones pertinentes destinadas a

hacer que los datos de la investigación financiada públicamente sean plenamente accesibles (“políticas de acceso abierto”) en aplicación del principio de apertura por defecto y de compatibilidad con los principios FAIR. En este contexto, deberán tenerse en cuenta las inquietudes relacionadas con los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos de conformidad con el principio “tan abiertos como sea posible, tan cerrados como sea necesario”. Estas políticas de acceso abierto se dirigirán a las organizaciones que realizan actividades de investigación y a las organizaciones que financian la investigación.

- 2) Sin perjuicio del artículo 32 *quindecies*, apartado 3, letra d), los datos de investigación serán reutilizables para fines comerciales o no comerciales de conformidad con la sección 1 y la sección 2, subsección 3, en la medida en que sean financiados con fondos públicos y en que investigadores, organizaciones que realizan actividades de investigación u organizaciones que financian la investigación ya los hayan puesto a disposición del público a través de un repositorio institucional o temático. En este contexto, deberán tenerse en cuenta los intereses comerciales legítimos, las actividades de transferencia de conocimientos y los derechos de propiedad intelectual preexistentes.

Subsección 5

Conjuntos de datos de alto valor

Artículo 32 *duovicies*

Categorías temáticas de conjuntos de datos de alto valor

- 1) Las categorías temáticas de conjuntos de datos de alto valor serán las establecidas en el anexo I.
- 2) La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 45, apartado 2 *bis*, para modificar el anexo I mediante la inclusión de nuevas categorías temáticas de conjuntos de datos de alto valor que reflejen los avances tecnológicos y del mercado.

Artículo 32 *tervicies*

Conjuntos de datos de alto valor y modalidades de publicación y reutilización

- 1) La Comisión adoptará actos de ejecución que establezcan una lista de conjuntos de datos específicos de alto valor que se engloben dentro de las categorías que figuran en el anexo I y que obren en poder de organismos del sector público y de empresas públicas entre los datos o documentos a los que se aplica la presente sección.

Dichos datos de alto valor:

- a) estarán disponibles gratuitamente, a reserva de los apartados 3, 4 y 5;
- b) serán legibles por máquina;
- c) se suministrarán a través de API; y
- d) se proporcionarán en forma de descarga masiva, cuando proceda.

Dichos actos de ejecución podrán especificar los acuerdos organizativos relativos a la publicación y de reutilización de los tipos de conjuntos de datos de alto valor. Esos acuerdos serán compatibles con las licencias tipo abiertas.

Los acuerdos podrán incluir condiciones aplicables a la reutilización, el formato de los datos y los metadatos, así como acuerdos técnicos para la difusión. Las inversiones que hagan los Estados miembros en iniciativas en materia de datos abiertos, como las inversiones en el desarrollo y el despliegue de determinadas normas, se tendrán en cuenta y se ponderarán frente a los potenciales beneficios derivados de la inclusión en la lista.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 46, apartado 2.

- 2) La definición de conjuntos de datos específicos de alto valor contemplados en el apartado 1 se basará en la valoración de su potencial para:
 - a) generar beneficios socioeconómicos o medioambientales importantes y servicios innovadores;
 - b) beneficiar a un gran número de usuarios, en particular pymes y pequeñas empresas de mediana capitalización;
 - c) contribuir a generar ingresos; y
 - d) ser combinados con otros conjuntos de datos.

Al objeto de definir tales tipos específicos de conjuntos de datos de alto valor, la Comisión llevará a cabo consultas adecuadas, también a nivel de expertos, elaborará una evaluación de impacto y garantizará la complementariedad con los actos jurídicos vigentes, como la Directiva 2010/40/UE del Parlamento Europeo y del Consejo, con respecto a la reutilización de datos o documentos. La evaluación de dicho impacto incluirá un análisis coste-beneficio y un análisis sobre si el hecho de que organismos del sector público, a los que se exige generar ingresos para sufragar una parte importante de sus costes relativos a la realización de sus misiones de servicio público, proporcionen de manera gratuita conjuntos de datos de alto valor podría tener un impacto sustancial en el presupuesto de dichos organismos. Cuando se vean afectados los conjuntos de datos de alto valor en posesión de empresas públicas, la evaluación de impacto prestará especial consideración a la función de las empresas públicas en un entorno económico competitivo.

- 3) Como excepción a lo dispuesto en el apartado 1, párrafo segundo, letra a), los actos de ejecución a los que se refiere dicho apartado establecerán que la disponibilidad gratuita de conjuntos de datos de alto valor no se aplicará a conjuntos de datos específicos que obren en poder empresas públicas, cuando el hecho de poner a disposición dichos conjuntos de datos de manera gratuita pudiera provocar una distorsión de la competencia en los mercados correspondientes.
- 4) El requisito de poner a disposición de forma gratuita conjuntos de datos de alto valor en virtud del apartado 1, párrafo segundo, letra a), no se aplicará a las bibliotecas, incluidas las universitarias, los museos y los archivos.
- 5) Cuando el hecho de que organismos del sector público a los que se exige generar ingresos para sufragar una parte importante de sus costes relativos a la realización de sus misiones de servicio público pongan a disposición de forma gratuita conjuntos de datos de alto valor pueda tener un impacto sustancial en el presupuesto de los organismos implicados, los Estados miembros podrán eximir a dichos organismos del requisito de poner a disposición de forma gratuita esos conjuntos de datos de alto valor por un período que no superará los dos años a partir de la entrada en vigor del acto de ejecución correspondiente adoptado de conformidad con el apartado 1.

Sección 3

Reutilización de determinadas categorías de datos protegidos que obren en poder de organismos del sector público

Artículo 32 *quatervicies*

Condiciones de la reutilización

- 1) Los organismos del sector público que, con arreglo al Derecho nacional, sean competentes para conceder o denegar acceso para la reutilización de una o varias de las categorías de datos o documentos pertenecientes a determinadas categorías de datos protegidos publicarán las condiciones en las que se permite tal reutilización y el procedimiento para solicitarla por medio del punto único de información a que se refiere el artículo 32 *bis bis*. Cuando concedan o denieguen acceso para la reutilización, podrán prestarle asistencia los organismos competentes a que se refiere el artículo 32 *septvicies*, apartado 1.

Los Estados miembros velarán por que los organismos del sector público dispongan de los recursos necesarios para cumplir lo dispuesto en el presente artículo y en el artículo 32 *quinvicies*.

- 2) La reutilización de datos o documentos no afectará su carácter protegido y solo se permitirá:
 - a) respetando los derechos de propiedad intelectual;
 - b) si los datos considerados confidenciales de conformidad con el Derecho de la Unión o nacional en materia de secreto comercial o estadístico no se divulgan, como resultado de permitir la reutilización, a menos que dicha reutilización esté permitida sobre la base del consentimiento del interesado o del permiso del tenedor de los datos de conformidad con el apartado 5;
 - c) de conformidad con el Reglamento (UE) 2016/679.
- 3) Para garantizar la conservación del carácter protegido a que se refiere el apartado 2, los organismos del sector público podrán establecer los siguientes requisitos:
 - a) conceder acceso para la reutilización de datos o documentos únicamente cuando el organismo del sector público o el organismo competente, tras la solicitud de reutilización, se haya asegurado de que dichos datos o documentos:
 - i) hayan sido anonimizados, en el caso de los datos personales;
 - ii) hayan sido sometidos a otras formas de preparación de los datos personales;
 - iii) hayan sido modificados, agregados o tratados por cualquier otro método de control de la divulgación, en el caso de la información comercial de carácter confidencial, incluidos los secretos comerciales o los contenidos protegidos por derechos de propiedad intelectual;
 - b) que el acceso y la reutilización a distancia de los datos o documentos se lleven a cabo en un entorno de tratamiento seguro facilitado o controlado por el organismo del sector público;
 - c) que el acceso y reutilización de los datos o documentos se lleven a cabo en los locales físicos en los que se encuentre el entorno de tratamiento seguro de conformidad con unas normas de seguridad estrictas, siempre que no pueda

habilitarse el acceso a distancia sin que ello ponga en peligro los derechos e intereses de terceros.

En caso de reutilización autorizada de conformidad con el párrafo primero, letra a), inciso i), la reutilización de datos o documentos estará sujeta a las normas sobre datos abiertos de las administraciones públicas establecidas en la sección 2. Esto se entiende sin perjuicio de lo dispuesto en el artículo 32 *sexvicies*, que prevalece en caso de conflicto.

En el caso en que se permita la reutilización de conformidad con el párrafo primero, letras b) y c), los organismos del sector público impondrán condiciones que preserven la integridad del funcionamiento de los sistemas técnicos del entorno de tratamiento seguro utilizado.

- 4) El organismo del sector público se reservará el derecho de verificar el proceso, los medios y cualquier resultado del tratamiento de datos o documentos realizado por el reutilizador para preservar la integridad de la protección de los datos o documentos. También se reservará el derecho de prohibir la utilización de resultados que contengan información que ponga en peligro los derechos e intereses de terceros. La decisión de prohibir la utilización de los resultados deberá ser comprensible y transparente para el reutilizador.

A menos que el Derecho nacional establezca garantías específicas respecto de las obligaciones de confidencialidad aplicables en relación con la reutilización de determinadas categorías de datos protegidos, el organismo del sector público supeditará la utilización de los datos o documentos facilitados de conformidad con el apartado 3 a la observancia por parte del reutilizador de una obligación de confidencialidad que prohíba la divulgación de cualquier información que ponga en peligro los derechos e intereses de terceros y que el reutilizador pueda haber adquirido a pesar de las garantías establecidas. En caso de reutilización no autorizada de datos no personales, el reutilizador estará obligado a informar sin demora y, en su caso, con la ayuda del organismo del sector público, a las personas físicas o jurídicas cuyos derechos e intereses puedan verse afectados.

- 5) Cuando no pueda permitirse la reutilización de datos o documentos de conformidad con los apartados 3 y 4, la reutilización solo será posible:
 - a) cuando no exista una base jurídica distinta del consentimiento para transmitir los datos en virtud del Reglamento (UE) 2016/679, con el consentimiento de los interesados;
 - b) con el permiso de los tenedores de datos cuyos derechos e intereses puedan verse afectados por tal reutilización.

El organismo del sector público hará todo lo posible, de conformidad con el Derecho de la Unión y el Derecho nacional, por prestar asistencia a los posibles reutilizadores para obtener el consentimiento de los interesados o el permiso de los tenedores de datos cuyos derechos e intereses puedan verse afectados por dicha reutilización, cuando ello sea factible sin una carga desproporcionada para el organismo del sector público.

Cuando preste dicha asistencia, el organismo del sector público podrá ser asistido por los organismos competentes a que se refiere el artículo 32 *septvicies*.

Artículo 32 *quinvicies*

Requisitos para las transferencias de datos no personales a terceros países por parte de los reutilizadores

- 1) Cuando un reutilizador tenga la intención de transferir a un tercer país determinadas categorías de datos protegidos que no sean personales, informará al organismo del sector público de su intención de transferirlos y de la finalidad de la transferencia en el momento de solicitar la reutilización de los datos. En caso de reutilización basada en el permiso del tenedor de datos, el reutilizador informará, en su caso, asistido por el organismo del sector público, a la persona física o jurídica cuyos derechos e intereses puedan verse afectados de tal intención, de la finalidad y de las garantías adecuadas. El organismo del sector público no permitirá la reutilización a menos que la persona física o jurídica conceda su permiso para dicha transferencia.
- 2) Los organismos del sector público transmitirán datos no personales confidenciales o protegidos por derechos de propiedad intelectual a un reutilizador que tenga la intención de transferirlos a un tercer país distinto de los países designados de conformidad con el apartado 7 solo si el reutilizador se obliga contractualmente a:
 - a) cumplir las obligaciones impuestas de conformidad con los derechos de propiedad intelectual y el Derecho de la Unión o nacional en materia de secreto comercial o estadístico, incluso después de la transferencia de los datos al tercer país;
 - b) aceptar la jurisdicción de los órganos jurisdiccionales del Estado miembro del organismo del sector público transmisor con respecto a cualquier litigio relacionado con el respeto de los derechos de propiedad intelectual y el Derecho de la Unión o el Derecho nacional en materia de secreto comercial o estadístico.
- 3) La Comisión podrá adoptar actos de ejecución que establezcan cláusulas contractuales tipo para el cumplimiento de las obligaciones a que se refiere el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 46, apartado 2.
- 4) Los organismos del sector público proporcionarán, cuando proceda y en la medida de sus capacidades, orientaciones y asistencia a los reutilizadores para que cumplan las obligaciones a las que se refiere el apartado 2.
- 5) Cuando así lo justifique un número considerable de solicitudes en toda la Unión relativas a la reutilización de datos no personales en terceros países concretos, la Comisión podrá adoptar actos de ejecución en los que se declare que las disposiciones jurídicas, de supervisión y de ejecución de un tercer país:
 - a) garantizan una protección de la propiedad intelectual y de los secretos comerciales esencialmente equivalente a la garantizada por el Derecho de la Unión;
 - b) se aplican y hacen cumplir de manera efectiva; y
 - c) ofrecen vías de recurso judicial efectivas.
- 6) Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 46, apartado 2.
- 7) Los actos legislativos específicos de la Unión podrán considerar que determinadas categorías de datos no personales que obren en poder de organismos del sector

público son muy sensibles a efectos del presente artículo cuando su transferencia a terceros países pueda poner en peligro objetivos de las políticas públicas de la Unión, entre otros, la seguridad y salud públicas, o pueda entrañar el riesgo de la reidentificación de datos no personales anonimizados. Cuando se adopte dicho acto, la Comisión adoptará actos delegados de conformidad con el artículo 45 que completen el presente Reglamento con condiciones especiales aplicables a las transferencias de tales datos a terceros países.

Si un acto legislativo específico de la Unión a que se refiere el párrafo primero así lo exige, dichas condiciones especiales podrán incluir las condiciones contractuales aplicables a la transferencia de datos o disposiciones técnicas a ese respecto, limitaciones relativas a la reutilización de los datos en terceros países o relativas a las categorías de personas facultadas para transferir los datos a terceros países, o, en casos excepcionales, restricciones relativas a la transferencia de los datos a terceros países.

El reutilizador a quien se haya concedido el derecho a reutilizar datos no personales solo podrá transferir los datos a terceros países en los que se cumplan los requisitos establecidos en los apartados 2, 4 y 5.

Artículo 32 *sexvicies*

Tasas

- 1) Los organismos del sector público que permitan la reutilización de determinadas categorías de datos protegidos podrán cobrar tasas por permitir la reutilización de dichos datos.
- 2) Cuando los organismos del sector público apliquen tasas, adoptarán medidas para incentivar la reutilización de determinadas categorías de datos protegidos con fines no comerciales, como la investigación científica, y la reutilización por parte de las empresas emergentes, las pymes y las pequeñas empresas de mediana capitalización, de conformidad con las normas sobre ayudas estatales de la Unión. A este respecto, los organismos del sector público también podrán ofrecer los datos con un descuento en las tasas o de forma gratuita, en particular, a las empresas emergentes, las pymes, las pequeñas empresas de mediana capitalización, la sociedad civil y los centros educativos y de investigación. A tal fin, los organismos del sector público podrán elaborar una lista de categorías de reutilizadores a los que se faciliten los datos o documentos para reutilización con un descuento en las tasas o de forma gratuita. Se publicará dicha lista junto con los criterios seguidos para elaborarla.
- 3) Las tasas se calcularán en función de los costes relacionados con la tramitación de las solicitudes de reutilización de determinadas categorías de datos protegidos, y se limitarán a los costes necesarios en relación con:
 - a) la reproducción, la entrega y la difusión de los datos;
 - b) la adquisición de derechos;
 - c) la anonimización u otras formas de preparación de los datos personales y de los datos comerciales confidenciales con arreglo a lo dispuesto en el artículo 32 *quatervicies*, apartado 3 [condiciones de la reutilización];
 - d) el mantenimiento del entorno de tratamiento seguro;
 - e) la adquisición, por parte de terceros ajenos al sector público, del derecho de terceros de permitir la reutilización de conformidad con la presente sección; y la asistencia a los reutilizadores en la obtención del consentimiento de los

interesados y del permiso de los tenedores de datos cuyos derechos e intereses puedan verse afectados por la reutilización.

- 4) Los Estados miembros establecerán y publicarán los criterios y la metodología para calcular las tasas. Los organismos del sector público publicarán una descripción de las principales categorías de costes y las normas para su asignación.
- 5) Los organismos del sector público podrán cobrar tasas más elevadas que las permitidas de conformidad con los apartados 2 y 3 del presente artículo con respecto a las empresas muy grandes, sobre la base de criterios objetivos, teniendo en cuenta el poder económico o la capacidad de la entidad para adquirir datos, incluida, en particular, la designación como guardián de acceso con arreglo al Reglamento (UE) 2022/1925. Estas tasas calculadas serán proporcionadas. Además de los elementos enumerados en el apartado 3 del presente artículo, pueden cubrir el coste de recogida y producción de los datos, incrementado por un margen de beneficio razonable de la inversión.

Artículo 32 *septvicies*

Organismos competentes

- 1) A efectos del desempeño de las funciones a que se refiere el presente artículo, cada Estado miembro designará uno o varios organismos competentes de conformidad con el artículo 37, apartado 1, que podrán ser competentes para sectores concretos, pero que colectivamente deberán abarcar todos los sectores, a fin de ayudar a los organismos del sector público que concedan o denieguen el acceso para la reutilización de determinadas categorías de datos protegidos. Los Estados miembros podrán crear uno o más organismos competentes nuevos o servirse de organismos del sector público existentes o de servicios internos de organismos del sector público que cumplan las condiciones establecidas en la presente sección.
- 2) Podrá confiarse a los organismos competentes la facultad de conceder acceso para la reutilización de determinadas categorías de datos protegidos con arreglo al Derecho de la Unión o nacional que prevea la concesión de dicho acceso. Cuando concedan o denieguen el acceso para la reutilización, dichos organismos competentes estarán sujetos a lo dispuesto en los artículos 32 *duodecies*, 32 *quatervicies*, 32 *quinvicies*, 32 *sexvicies* y 32 *bis ter*.
- 3) Los organismos competentes dispondrán de los recursos jurídicos, financieros, técnicos y humanos adecuados para desempeñar las funciones que se les asignen, incluidos los conocimientos técnicos necesarios para poder cumplir con el Derecho de la Unión o nacional aplicable en lo referente a los regímenes de acceso relativos a las categorías de datos protegidos enumeradas en el artículo 2, punto 54.
- 4) La asistencia a que se refiere el apartado 1 comprenderá, cuando sea necesario, lo siguiente:
 - a) prestar apoyo técnico mediante la habilitación de un entorno de tratamiento seguro a fin de facilitar el acceso para la reutilización de los datos o documentos;
 - b) proporcionar orientación y apoyo técnico sobre la mejor manera de estructurar y almacenar los datos para que dichos datos o documentos sean fácilmente accesibles;
 - c) prestar apoyo técnico para la anonimización, la seudonimización y los métodos más avanzados de protección de la privacidad, no solo de los datos personales,

sino también de la información comercial confidencial, incluidos los secretos comerciales o el contenido protegido por derechos de propiedad intelectual;

- d) proporcionar asistencia a los organismos del sector público, cuando corresponda, para prestar asistencia a los reutilizadores a solicitar el consentimiento de los interesados para la reutilización o el permiso de los tenedores de datos en consonancia con sus decisiones específicas, lo que incluye asistencia sobre el territorio en el que se prevea efectuar el tratamiento de los datos y asistencia a los organismos del sector público en el establecimiento de mecanismos técnicos que permitan a los reutilizadores transmitir las solicitudes de consentimiento o permiso, cuando resulte factible en la práctica;
- e) suministrar asistencia a los organismos del sector público en la evaluación de la idoneidad de las obligaciones contractuales contraídas por un reutilizador, en virtud del artículo 32 *quinvicies*, apartado 2.

Artículo 32 *bis bis*

Punto único de información

- 1) Cada Estado miembro designará un punto único de información. Dicho punto facilitará información fácilmente accesible sobre la aplicación de los artículos 32 *quatervicies*, 32 *quinvicies* y 32 *sexvicies*.
- 2) El punto único de información será competente para recibir las consultas o solicitudes de reutilización de determinadas categorías de datos protegidos y las transmitirá, cuando resulte posible y adecuado, a través de medios automatizados, a los organismos del sector público competentes, o, en su caso, a los organismos competentes a los que se refiere el artículo 32 *septvicies*, apartado 1, cuando proceda.
- 3) El punto único de información podrá incluir un canal de información específico, simplificado y bien documentado para las pymes, las pequeñas empresas de mediana capitalización, las empresas emergentes y los centros de investigación que aborde sus necesidades y capacidades a la hora de solicitar la reutilización de las categorías de datos enumeradas en el artículo 2, punto 54.
- 4) El punto único de información pondrá a disposición, por medios electrónicos, una lista de activos consultable que contenga un resumen de todos los recursos documentales disponibles, entre ellos, en su caso, los recursos documentales que estén disponibles en puntos sectoriales, regionales o locales, con información pertinente en la que se describan los datos o documentos disponibles, que incluya, al menos, el formato y el tamaño de los datos y las condiciones para su reutilización.
- 5) La Comisión creará un punto único europeo de acceso que ofrezca un registro electrónico de datos o documentos consultable en los puntos únicos de información nacionales e información adicional sobre cómo solicitar datos o documentos a través de dichos puntos únicos de información nacionales.

Artículo 32 *bis ter*

Procedimiento de solicitud de reutilización

- 1) Salvo que se prevean plazos más breves en el Derecho nacional, los organismos del sector público competentes o los organismos competentes a que se refiere el artículo 32 *septuaginta tres*, apartado 1, adoptarán las decisiones sobre la solicitud de reutilización de determinadas categorías de datos protegidos en el plazo de dos meses a partir de la fecha de recepción de la solicitud.
 - 2) En caso de solicitudes de reutilización excepcionalmente extensas y complejas, el plazo de dos meses podrá ampliarse un máximo de treinta días. En tales casos, los organismos del sector público competentes o los organismos competentes a que se refiere el artículo 32 *septuaginta tres*, apartado 1, notificarán al solicitante lo antes posible que se necesita más tiempo para tramitar la solicitud y los motivos de la demora.
 - 3) Toda persona física o jurídica directamente afectada por una decisión adoptada de conformidad con el apartado 1 dispondrá de un derecho efectivo de recurso en el Estado miembro en el que se encuentre el organismo en cuestión. Ese derecho de recurso se establecerá en el Derecho nacional e incluirá la posibilidad de revisión por un órgano imparcial con los conocimientos especializados adecuados, como, por ejemplo, la autoridad nacional de defensa de la competencia, la autoridad reguladora del acceso a los documentos correspondiente, la autoridad de control establecida de conformidad con el Reglamento (UE) 2016/679 o un órgano jurisdiccional nacional, cuyas decisiones sean vinculantes para el organismo del sector público o el organismo competente en cuestión.».
19. El artículo 38 se sustituye por el texto siguiente:
- 1) «Sin perjuicio de cualquier otro recurso administrativo o acción judicial, toda persona física y jurídica tendrá derecho a presentar una reclamación individual o, cuando proceda, colectiva:
 - a) ante la autoridad competente pertinente del Estado miembro en el que tenga su residencia habitual, su lugar de trabajo o su lugar de establecimiento cuando considere que los derechos que le confiere el presente Reglamento han sido vulnerados;
 - b) ante la autoridad competente pertinente para la inscripción en el registro de servicios de intermediación de datos o la autoridad competente pertinente para la inscripción en el registro de organizaciones de gestión de datos con fines altruistas si va dirigida específicamente contra un proveedor de servicios de intermediación de datos reconocido o una organización reconocida de gestión de datos con fines altruistas en relación con cualquier asunto perteneciente al ámbito de aplicación del presente Reglamento.
 - 2) El coordinador de datos proporcionará, previa solicitud, toda la información necesaria a las personas físicas y jurídicas para la presentación de sus reclamaciones ante la correspondiente autoridad competente.
 - 3) La autoridad competente ante la que se haya presentado la reclamación informará al reclamante, con arreglo al Derecho nacional, sobre:
 - a) el curso del procedimiento y la decisión tomada; y
 - b) las vías de recurso judicial previstas en el artículo 39.».
20. En el artículo 40, se añade el apartado 6 siguiente:
- «6. El presente artículo no se aplicará al capítulo VII *quater*.».

21. Tras el artículo 41 se inserta el texto siguiente:

«CAPÍTULO IX *bis*

Comité Europeo de Innovación en materia de Datos».

22. Se inserta el artículo 41 *bis* siguiente:

«Artículo 41 *bis*

Comité Europeo de Innovación en materia de Datos

- 1) El Comité Europeo de Innovación en materia de Datos se crea como medio para asesorar y asistir a la Comisión en la coordinación de la aplicación del presente Reglamento y para servir de foro de debate para el desarrollo de una economía y unas políticas europeas en materia de datos.
- 2) Estará compuesto al menos por representantes de los Estados miembros competentes en asuntos relacionados con los datos, las autoridades competentes para la ejecución de los capítulos II, III, V, VII *bis* y VII *quater* del presente Reglamento, el Comité Europeo de Protección de Datos, el Supervisor Europeo de Protección de Datos, la ENISA, el representante de la UE para las pymes o un representante designado por la red de representantes para las pymes. La Comisión podrá decidir añadir más categorías de miembros. A la hora de nombrar expertos individuales, la Comisión procurará lograr un equilibrio geográfico y de género en la composición del grupo.
- 3) La Comisión decidirá sobre la composición de las diferentes configuraciones en las que el Comité desempeñará sus funciones.
- 4) La Comisión presidirá las reuniones del Comité Europeo de Innovación en materia de Datos.».

23. El artículo 42 se sustituye por el texto siguiente:

«Artículo 42

Función del CEID

- 1) El CEID apoyará la aplicación coherente del presente Reglamento del siguiente modo:
 - a) sirviendo de foro para los diálogos estratégicos sobre las políticas y la gobernanza de los datos, los flujos internacionales de estos y la evolución intersectorial pertinente para la economía de los datos europea;
 - b) asesorando y asistiendo a la Comisión en el desarrollo de una práctica coherente de las autoridades competentes en la aplicación de los capítulos II, III, V, VII, VII *bis* and VII *quater*;
 - c) facilitando la cooperación entre las autoridades competentes mediante el desarrollo de capacidades y el intercambio de información;
 - d) fomentando el intercambio de experiencias y buenas prácticas entre los Estados miembros en el ámbito de la reutilización de la información del sector público en colaboración con otros organismos de gobernanza pertinentes.».

24. El artículo 45 se modifica como sigue:

- a) el apartado 2 se sustituye por el texto siguiente:

«2. Los poderes para adoptar los actos delegados mencionados en el artículo 29, apartado 7, el artículo 32 *duovicies*, apartado 2, y el artículo 33, apartado 2, se otorgarán a la Comisión por un período indefinido.»;

b) el apartado 3 se sustituye por el texto siguiente:

«3. La delegación de poderes mencionada en el artículo 29, apartado 7, el artículo 32 *duovicies*, apartado 2, y el artículo 33, apartado 2, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.»;

c) el apartado 6 se sustituye por el texto siguiente:

«6. Los actos delegados adoptados en virtud del artículo 29, apartado 7, el artículo 32 *duovicies*, apartado 2, o el artículo 33, apartado 2, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.».

25. El artículo 46 se modifica como sigue:

a) en el apartado 1, la primera frase se sustituye por el texto siguiente:

«La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.»;

b) se inserta el apartado 1 *bis* siguiente:

«1 *bis*. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento (UE) n.º 182/2011.».

26. El artículo 49 se modifica como sigue:

a) el apartado 1 se modifica como sigue:

i) el texto de la parte introductoria se sustituye por el texto siguiente:

«1. A más tardar el 12 de septiembre de 2028, la Comisión llevará a cabo una evaluación de los capítulos II, III, IV, V, VI, VII y VIII y presentará un informe sobre sus principales conclusiones al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. En la evaluación se analizarán, en particular:»;

ii) la letra m) se sustituye por el texto siguiente:

«m) las repercusiones del presente Reglamento en las pymes y en las pequeñas empresas de mediana capitalización por lo que respecta a su capacidad para innovar y a la disponibilidad de servicios de tratamiento de datos para los usuarios en la Unión y la carga del cumplimiento de las nuevas obligaciones.»;

b) se inserta el apartado 2 *bis* siguiente:

«2 *bis*. A más tardar el [fecha = entrada en vigor más 5 años], la Comisión llevará a cabo una evaluación de los capítulos VII *bis*, VII *ter* and VII *quater* y presentará un informe sobre sus principales conclusiones al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo.

En el informe se analizarán, en particular:

- a) la situación de las inscripciones en el registro de los servicios de intermediación de datos y el tipo de servicios que ofrecen;
- b) el tipo de organizaciones de gestión de datos con fines altruistas inscritas en el registro y una síntesis de los fines de interés general para los que se intercambien datos, con miras a determinar criterios inequívocos a ese respecto.
- c) el alcance y las repercusiones sociales y económicas del capítulo VII *quater*, sección 2, en particular:
- d) la medida en que haya aumentado la reutilización de documentos del sector público a los cuales se aplica el capítulo VII *quater*, sección 2, especialmente por parte de las pymes y las pequeñas empresas de mediana capitalización;
- e) la repercusión de los conjuntos de datos de alto valor;
- f) la interacción entre las normas sobre protección de datos y las posibilidades de reutilización; y
- g) Los Estados miembros proporcionarán a la Comisión la información necesaria para la elaboración del informe.»;

c) el apartado 5 se sustituye por el texto siguiente:

«5. Sobre la base de los informes a que se refieren los apartados 1, 2 y 2 *bis*, la Comisión podrá presentar, en su caso, una propuesta legislativa al Parlamento Europeo y al Consejo para modificar el presente Reglamento.».

27. Se añade el anexo I tal como figura en el anexo II del presente Reglamento.

Artículo 2

Modificaciones del Reglamento (UE) 2018/1724

En el cuadro del anexo II del Reglamento (UE) 2018/1724, la entrada “Puesta en marcha, gestión y cierre de una empresa» se sustituye por el texto siguiente:

Sucesos vitales	Procedimientos	Resultado esperado sujeto a un examen de la solicitud por la autoridad competente de conformidad con su Derecho nacional, cuando corresponda
Puesta en marcha, gestión y cierre de	Notificación de actividades empresariales, permisos para ejercer una actividad empresarial, cambios de actividad empresarial y cese de una actividad empresarial sin procedimientos de insolvencia o	Acuse de recibo de la notificación o el cambio, o bien de la solicitud de permiso de actividad

una empresa	liquidación, excluidos el registro inicial de una actividad empresarial en el registro mercantil y los procedimientos relativos a la constitución o cualquier presentación posterior de sociedades en el sentido del artículo 54, párrafo segundo, del TFUE	empresarial
	Alta de un empleador (persona física) en sistemas obligatorios de pensiones y seguros	Confirmación del alta o número de registro de la seguridad social
	Alta de empleados en sistemas obligatorios de pensiones y seguros	Confirmación del alta o número de registro de la seguridad social
	Presentación de una declaración de impuesto sobre sociedades	Acuse de recibo de la declaración
	Notificación a los regímenes de la seguridad social de la finalización del contrato de un empleado, con exclusión de los procedimientos de despido colectivo	Acuse de recibo de la notificación
	Pago de las cotizaciones sociales de los empleados	Recibo u otra forma de confirmación del pago de las cotizaciones sociales de los empleados
	Inscripción en el registro como proveedor de servicios de intermediación de datos	Confirmación de la inscripción
	Inscripción como organización de gestión de datos con fines altruistas reconocida en la Unión	Confirmación de la inscripción

Artículo 3

Modificación del Reglamento (UE) 2016/679 [RGPD]

El Reglamento (UE) 2016/679 se modifica como sigue:

1. El artículo 4 se modifica como sigue:
 - a) en el punto 1, se añaden las frases siguientes:

«la información relativa a una persona física no es necesariamente datos personales para cualquier otra persona o entidad por el mero hecho de que otra entidad pueda identificar a esa persona física. La información no será personal para una entidad determinada cuando dicha entidad no pueda identificar a la persona física a la que se refiere la información teniendo en cuenta los medios que razonablemente puedan ser utilizados por dicha entidad. Dicha información no se convierte en personal para dicha entidad por el mero hecho de que un posible destinatario ulterior disponga de medios que razonablemente puedan ser utilizados para identificar a la persona física a la que se refiere la información;»;
 - b) se añaden los siguientes puntos:

«32) “equipo terminal”: un equipo terminal tal como se define en el artículo 1, punto 1, de la Directiva 2008/63/CE de la Comisión.

33) en el caso de las “redes de comunicaciones electrónicas”, se aplicará la definición del artículo 2, apartado 1, de la Directiva (UE) 2018/1972;

34) “navegador web”: un navegador web tal como se define en el artículo 2, punto 11, del Reglamento (UE) 2022/1925;

35) “servicio de medios de comunicación”: un servicio de medios de comunicación tal como se define en el artículo 2, punto 1, del Reglamento (UE) 2024/1083;

36) “prestador de servicios de medios de comunicación”: un prestador de servicios de medios de comunicación tal como se define en el artículo 2, punto 2, del Reglamento (UE) 2024/1083;

37) “interfaz en línea”: una interfaz en línea tal como se define en el artículo 3, letra m), del Reglamento (UE) 2022/2065;

38) “investigación científica”: toda investigación que también pueda apoyar la innovación, como el desarrollo tecnológico y la demostración. Estas acciones contribuirán a los conocimientos científicos existentes o aplicarán los conocimientos existentes de formas novedosas, se llevarán a cabo con el objetivo de contribuir al crecimiento del conocimiento general y el bienestar de la sociedad y se ajustarán a las normas éticas del ámbito de investigación pertinente. Esto no excluye que la investigación también pueda tener por objeto promover un interés comercial.»

2. En el artículo 5, apartado 1, el texto de la letra b) se sustituye por el texto siguiente:

«recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos se considerará compatible con los fines iniciales, independientemente de las condiciones del artículo 6, apartado 4, del presente Reglamento (“limitación de la finalidad”);».

3. El artículo 9 se modifica como sigue:

a) en el apartado 2, se añaden las letras siguientes:

«k) el tratamiento en el contexto del desarrollo y el funcionamiento de un sistema de IA, tal como se define en el artículo 3, punto 1, del Reglamento (UE) 2024/1689, o de un modelo de IA, conforme a las condiciones a que se refiere el apartado 5;

l) cuando el tratamiento de datos biométricos sea necesario para confirmar la identidad de un interesado (verificación), cuando los datos biométricos o los medios necesarios para la verificación estén bajo el control exclusivo del interesado.»;

b) se añade el apartado siguiente:

«5. Para el tratamiento a que se refiere el apartado 2, letra k), se aplicarán las medidas organizativas y técnicas adecuadas para evitar la recogida y, de otro

modo, el tratamiento de categorías especiales de datos personales. Cuando, a pesar de la aplicación de dichas medidas, el responsable del tratamiento detecte categorías especiales de datos personales en los conjuntos de datos utilizados para el entrenamiento, la prueba o la validación, o en el sistema o modelo de IA, eliminará dichos datos. Si la supresión de dichos datos requiere un esfuerzo desproporcionado, el responsable del tratamiento protegerá en cualquier caso eficazmente y sin demora indebida dichos datos a fin de que no puedan utilizarse para producir resultados, ni puedan ser divulgados o de cualquier otra forma puestos a disposición de terceros.»

4. En el artículo 12, el apartado 5 se sustituye por el texto siguiente:

«5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán proporcionadas gratuitamente. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, o también, en el caso de las solicitudes con arreglo al artículo 15 porque el interesado abusa de los derechos conferidos por el presente Reglamento con fines distintos de la protección de sus datos, el responsable del tratamiento podrá:

- a) cobrar una tasa razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada; o
- b) negarse a actuar respecto de la solicitud.

Corresponderá al responsable del tratamiento demostrar que la solicitud es manifiestamente infundada o que existen motivos razonables para creer que es excesiva.»

5. En el artículo 13, el apartado 4 se sustituye por el texto siguiente:

«4. Los apartados 1, 2 y 3 no se aplicarán cuando los datos personales se hayan recogido en el contexto de una relación clara y circunscrita entre los interesados y un responsable del tratamiento que ejerza una actividad que no requiera un uso intensivo de datos y existan motivos razonables para suponer que el interesado ya dispone de la información a que se refiere el apartado 1, letras a) y c), a menos que el responsable del tratamiento transmita los datos a otros destinatarios o categorías de destinatarios, transfiera los datos a un tercer país, aplique tomas de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartado 1, o sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de los interesados en el sentido del artículo 35.»

6. En el artículo 13, se añade el apartado 5 siguiente:

«5. El responsable del tratamiento no necesitará facilitar la información a que se refieren los apartados 1, 2 y 3 cuando el tratamiento tenga lugar con fines de investigación científica y el suministro de la información a que se refieren los apartados 1, 2 y 3 resulte imposible o pueda suponer un esfuerzo desproporcionado en aplicación de las condiciones y garantías a que se refiere el artículo 89, apartado 1, o en la medida en que sea probable que la obligación a que se refiere el apartado 1 del presente artículo imposibilite u obstaculice gravemente el logro de los objetivos de dicho tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades

e intereses legítimos del interesado, inclusive haciendo pública la información.».

7. Los apartados 1 y 2 del artículo 22 se sustituyen por el texto siguiente:

«1. Una decisión que surta efectos jurídicos para un interesado o le afecte significativamente de forma similar solo podrá basarse en un tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión:

- a) sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, con independencia de que la decisión pueda adoptarse por medios distintos de los meramente automatizados;
- b) esté autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o
- c) se base en el consentimiento explícito del interesado.».

8. El artículo 33 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. En caso de violación de la seguridad de los datos personales que pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento notificará sin demora indebida y, cuando sea posible, a más tardar noventa y seis horas después de haber tenido conocimiento de ella, la violación de la seguridad de los datos personales a través del punto de entrada único establecido con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555 a la autoridad de control competente de conformidad con los artículos 55 y 56. Si la notificación a la autoridad de control no tiene lugar en el plazo de noventa y seis horas, deberá ir acompañada de indicación de los motivos de la dilación.»;

b) se añade el apartado siguiente:

«1 *bis*. Hasta la creación del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555, los responsables del tratamiento seguirán notificando las violaciones de la seguridad de los datos personales directamente a la autoridad de control competente de conformidad con los artículos 55 y 56.»;

c) se añaden los apartados siguientes:

«6. El Comité elaborará y transmitirá a la Comisión una propuesta de plantilla común para notificar una violación de la seguridad de los datos personales a la autoridad de control competente a que se refiere el apartado 1, así como una lista de las circunstancias en las que es probable que una violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de una persona física. La propuesta se presentará a la Comisión en el plazo de [OP: fecha = a los nueve meses de la entrada en vigor del presente Reglamento]. La Comisión, prestando la debida atención, examinará la propuesta y la revisará, según sea necesario, y estará facultada para adoptarla

mediante un acto de ejecución de conformidad con el procedimiento de examen establecido en el artículo 93, apartado 2.

7. La plantilla y la lista a que se refiere el apartado 6 se revisarán al menos cada tres años y se actualizarán en aquellos casos en que sea necesario. El Comité presentará su evaluación y las posibles propuestas de actualización a la Comisión en tiempo oportuno. La Comisión, tras un atento examen de las propuestas, las revisará y estará facultada para adoptar cualquier actualización con arreglo al procedimiento establecido en el apartado 6.»

9. El artículo 35 se modifica como sigue:

a) los apartados 4, 5 y 6 se sustituyen por el texto siguiente:

«4. El Comité elaborará y transmitirá a la Comisión una propuesta de lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1.

5. El Comité elaborará y transmitirá a la Comisión una propuesta de lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

6. El Comité elaborará y transmitirá a la Comisión una propuesta de plantilla común y una metodología común para llevar a cabo evaluaciones de impacto relativas a la protección de datos.»;

b) se insertan los apartados siguientes:

«6 *bis*. Las propuestas relativas a las listas a que se refieren los apartados 4 y 5 y a la plantilla y la metodología a que se refiere el apartado 6 se presentarán a la Comisión en el plazo de [OP: fecha = a los nueve meses de la entrada en vigor del presente Reglamento]. La Comisión, prestando la debida atención, las examinará y las revisará, según sea necesario, y estará facultada para adoptarlas mediante un acto de ejecución de conformidad con el procedimiento de examen establecido en el artículo 93, apartado 2.

6 *ter*. Las listas, la plantilla y la metodología a que se refiere el apartado 6 *bis* se revisarán al menos cada tres años y se actualizarán en aquellos casos en que sea necesario. El Comité presentará su evaluación y las posibles propuestas de actualización a la Comisión en tiempo oportuno. La Comisión, tras un atento examen de las propuestas, las revisará y estará facultada para adoptar cualquier actualización con arreglo al procedimiento establecido en el apartado 6 *bis*.».

6 *quater*. Las listas del tipo de operaciones de tratamiento que están sujetas al requisito de una evaluación de impacto relativa a la protección de datos y del tipo de operaciones de tratamiento para las que no se requiere una evaluación de impacto relativa a la protección de datos confeccionadas y publicadas por las autoridades de control seguirán siendo válidas hasta que la Comisión adopte el acto de ejecución a que se refiere el apartado 6 *bis*.».

10. Se añade el artículo siguiente:

«Artículo 41 *bis*

1) La Comisión podrá adoptar actos de ejecución para especificar los medios y criterios para determinar si los datos resultantes de la seudonimización ya no constituyen datos personales para determinadas entidades.

- 2) A los efectos del apartado 1, la Comisión:
 - a) evaluará el estado de avance de la técnica en cuanto a las técnicas disponibles;
 - b) desarrollará criterios o categorías para que los responsables del tratamiento y los destinatarios evalúen el riesgo de reidentificación en relación con los destinatarios típicos de los datos.
- 3) La aplicación de los medios y criterios descritos en un acto de ejecución puede utilizarse como elemento para demostrar que los datos no pueden dar lugar a la reidentificación de los interesados.
- 4) La Comisión implicará estrechamente al CEPD en la elaboración de los actos de ejecución. El CEPD emitirá un dictamen sobre los proyectos de actos de ejecución en un plazo de ocho semanas a partir de la recepción del proyecto de la Comisión.
- 5) Los actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 3.».
11. El artículo 57, apartado 1, se modifica como sigue:
 - (a) se suprime la letra k).
12. En el artículo 64, apartado 1, se suprime la letra a).
13. En el artículo 70, apartado 1, se suprime la letra h).
14. En el apartado 1 del artículo 70 se insertan las letras siguientes:

«h *bis*) elaborará y transmitirá a la Comisión una propuesta de lista del tipo de operaciones de tratamiento que están sujetas al requisito de una evaluación de impacto relativa a la protección de datos y para las que no se requiere una evaluación de impacto relativa a la protección de datos, de conformidad con el artículo 35;

h *ter*) elaborará y transmitirá a la Comisión una propuesta de plantilla común y una metodología común para llevar a cabo evaluaciones de impacto relativas a la protección de datos, de conformidad con el artículo 35;

h *quater*) elaborará y transmitirá a la Comisión una propuesta de plantilla común para notificar una violación de la seguridad de los datos personales a la autoridad de control competente, así como una lista de las circunstancias en las que es probable que una violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de una persona física, de conformidad con el artículo 33.».
15. Después del artículo 88 se insertan los artículos siguientes:

«Artículo 88 *bis*

Tratamiento de datos personales en los equipos terminales de las personas físicas

- 1) El almacenamiento de datos personales, o la obtención de acceso a datos personales ya almacenados en el equipo terminal de una persona física solo se permite cuando dicha persona haya dado su consentimiento, de conformidad con el presente Reglamento.
- 2) El apartado 1 no será óbice para el almacenamiento de datos personales, ni la obtención de acceso a los datos personales ya almacenados en el equipo terminal de una persona física sobre la base del Derecho de la Unión o de los Estados miembros

en el sentido del artículo 6 y con sujeción a las condiciones de este, a fin de salvaguardar los objetivos a que se refiere el artículo 23, apartado 1.

- 3) El almacenamiento de datos personales o la obtención de acceso a los datos personales ya almacenados en el equipo terminal de una persona física sin consentimiento y el tratamiento posterior serán lícitos en la medida en que sean necesarios para cualquiera de los fines siguientes:
 - a) efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas;
 - b) prestar un servicio expresamente solicitado por el interesado;
 - c) crear información agregada sobre el uso de un servicio en línea para medir la audiencia de dicho servicio, cuando lo lleve a cabo el responsable del tratamiento de dicho servicio en línea únicamente para utilización propia;
 - d) mantener o restablecer la seguridad de un servicio prestado por el responsable del tratamiento y solicitado por el interesado o el equipo terminal utilizado para la prestación de dicho servicio.
- 4) Cuando el almacenamiento de datos personales o la obtención de acceso a datos personales ya almacenados en el equipo terminal de una persona física se base en el consentimiento, se aplicará lo siguiente:
 - a) el interesado podrá denegar las solicitudes de consentimiento de manera fácil e inteligible con un botón de un solo clic o medios equivalentes;
 - b) si el interesado da su consentimiento, el responsable del tratamiento no presentará una nueva solicitud de consentimiento para el mismo fin durante el período durante el cual el responsable del tratamiento pueda basarse legalmente en el consentimiento del interesado;
 - c) si el interesado deniega una solicitud de consentimiento, el responsable del tratamiento no podrá presentar una nueva solicitud de consentimiento para el mismo fin durante un período de al menos seis meses.

El presente apartado también se aplica al tratamiento posterior de datos personales basado en el consentimiento.

- 5) El presente artículo será aplicable a partir del ... [OP: insértese la fecha correspondiente a seis meses después de la entrada en vigor del presente Reglamento].

Artículo 88 *ter*

Indicaciones automatizadas y legibles por máquina de las opciones del interesado con respecto al tratamiento de datos personales en los equipos terminales de las personas físicas

- 1) Los responsables del tratamiento velarán por que sus interfaces en línea permitan a los interesados:
 - a) dar su consentimiento por medios automatizados y legibles por máquina, siempre que se cumplan las condiciones para el consentimiento establecidas en el presente Reglamento;

- b) denegar una solicitud de consentimiento y ejercer el derecho de oposición con arreglo al artículo 21, apartado 2, por medios automatizados y legibles por máquina.
- 2) Los responsables del tratamiento respetarán las decisiones tomadas por los interesados de conformidad con el apartado 1.
- 3) Los apartados 1 y 2 no se aplicarán a los responsables del tratamiento que sean prestadores de servicios de medios de comunicación cuando presten un servicio de medios de comunicación.
- 4) De conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, la Comisión solicitará a una o varias organizaciones europeas de normalización que elaboren normas para la interpretación de las indicaciones legibles por máquina de las opciones de los interesados.
- Se presumirá que las interfaces en línea de los responsables del tratamiento conformes con normas armonizadas o partes de ellas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* cumplen los requisitos que contemplan tales normas o partes de ellas establecidos en el apartado 1.
- 5) Los apartados 1 y 2 serán aplicables a partir del [OP: insértese la fecha correspondiente a veinticuatro meses después de la entrada en vigor del presente Reglamento].
- 6) Los proveedores de navegadores web que no sean pymes proporcionarán los medios técnicos que permitan a los interesados dar su consentimiento y denegar una solicitud de consentimiento y ejercer el derecho de oposición con arreglo al artículo 21, apartado 2, a través de los medios automatizados y legibles por máquina a que se refiere el apartado 1 del presente artículo, aplicados de conformidad con los apartados 2 a 5 del presente artículo.
- 7) El apartado 6 será aplicable a partir del ... [OP: insértese la fecha correspondiente a cuarenta y ocho meses después de la entrada en vigor del presente Reglamento].

Artículo 88 *quater*

Tratamiento en el contexto del desarrollo y el funcionamiento de la IA

Cuando el tratamiento de datos personales sea necesario para los intereses del responsable del tratamiento en el contexto del desarrollo y el funcionamiento de un sistema de IA, tal como se define en el artículo 3, punto 1, del Reglamento (UE) 2024/1689, o de un modelo de IA, dicho tratamiento podrá efectuarse en aras de intereses legítimos en el sentido del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, cuando proceda, excepto en aquellos casos en que otra legislación nacional o de la Unión exija explícitamente el consentimiento y tales intereses prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado que requieran protección de los datos personales, en particular cuando el interesado sea un niño.

Todo tratamiento de este tipo estará sujeto a medidas organizativas, técnicas y salvaguardias adecuadas para los derechos y libertades del interesado, como garantizar el respeto de la minimización de datos durante la fase de selección de las fuentes y el entrenamiento y la prueba de un sistema o modelo de IA, proteger contra la no divulgación de datos conservados

de forma residual en el sistema o modelo de IA para garantizar una mayor transparencia a los interesados y conceder a los interesados un derecho incondicional a oponerse al tratamiento de sus datos personales.».

Artículo 4

Modificaciones del Reglamento (UE) 2018/1725 [RPDUE]

El Reglamento (UE) 2018/1725 se modifica como sigue:

1. El artículo 3 se modifica como sigue:

a) en el punto 1, se añaden las frases siguientes:

«la información relativa a una persona física no es necesariamente datos personales para cualquier otra persona o entidad por el mero hecho de que otra entidad pueda identificar a esa persona física. La información no será personal para una entidad determinada cuando dicha entidad no pueda identificar a la persona física a la que se refiere la información teniendo en cuenta los medios que razonablemente puedan ser utilizados por dicha entidad. Dicha información no se convierte en personal para dicha entidad por el mero hecho de que un posible destinatario ulterior disponga de medios que razonablemente puedan ser utilizados para identificar a la persona física a la que se refiere la información;»;

b) el punto 25 se sustituye por el texto siguiente:

«25) en el caso de las “redes de comunicaciones electrónicas”, se aplicará la definición del artículo 2, apartado 1, de la Directiva (UE) 2018/1972;»;

c) se añaden los siguientes puntos:

«27) “aplicación para dispositivos móviles”: una aplicación para dispositivos móviles tal como se define en el artículo 3, punto 2, de la Directiva (UE) 2016/2102;

28) “interfaz en línea”: una interfaz en línea tal como se define en el artículo 3, letra m), del Reglamento (UE) 2022/2065;

29) “investigación científica”: toda investigación que también pueda apoyar la innovación, como el desarrollo tecnológico y la demostración. Estas acciones contribuirán a los conocimientos científicos existentes o aplicarán los conocimientos existentes de formas novedosas, se llevarán a cabo con el objetivo de contribuir al crecimiento del conocimiento general y el bienestar de la sociedad y se ajustarán a las normas éticas del ámbito de investigación pertinente. Esto no excluye que la investigación también pueda tener por objeto promover un interés comercial.».

2. En el artículo 4, apartado 1, el texto de la letra b) se sustituye por el texto siguiente:

«b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 13, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos se considerará compatible con los fines iniciales,

independientemente de las condiciones del artículo 6 del presente Reglamento (“limitación de la finalidad”);».

3. El artículo 10 se modifica como sigue:

a) en el apartado 2, se añaden las letras siguientes:

«k) el tratamiento en el contexto del desarrollo y el funcionamiento de un sistema de IA, tal como se define en el artículo 3, punto 1, del Reglamento (UE) 2024/1689, o de un modelo de IA, conforme a las condiciones a que se refiere el apartado 4;

l) cuando el tratamiento de datos biométricos sea necesario para confirmar la identidad de un interesado (verificación), cuando los datos biométricos o los medios necesarios para la verificación estén bajo el control exclusivo del interesado.»;

b) se añade el apartado 4 siguiente:

«4. Para el tratamiento a que se refiere el apartado 2, letra k), se aplicarán las medidas organizativas y técnicas adecuadas para evitar la recogida y, de otro modo, el tratamiento de categorías especiales de datos personales. Cuando, a pesar de la aplicación de dichas medidas, el responsable del tratamiento detecte categorías especiales de datos personales en los conjuntos de datos utilizados para el entrenamiento, la prueba o la validación, o en el sistema o modelo de IA, eliminará dichos datos. Si la supresión de dichos datos requiere un esfuerzo desproporcionado, el responsable del tratamiento protegerá en cualquier caso eficazmente y sin demora indebida dichos datos a fin de que no puedan utilizarse para producir resultados, ni puedan ser divulgados o de cualquier otra forma puestos a disposición de terceros.».

4. En el artículo 14, el apartado 5 se sustituye por el texto siguiente:

«5. La información facilitada en virtud de los artículos 15 y 16 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 17 a 24 y 35 serán proporcionadas gratuitamente. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, o también, en el caso de las solicitudes con arreglo al artículo 17 porque el interesado abusa de los derechos conferidos por el presente Reglamento con fines distintos de la protección de sus datos, el responsable del tratamiento podrá negarse a actuar respecto de la solicitud. Corresponderá al responsable del tratamiento demostrar que la solicitud es manifiestamente infundada o que existen motivos razonables para creer que es excesiva.».

5. En el artículo 15, se añade el siguiente apartado 5:

«5. El responsable del tratamiento no necesitará facilitar la información a que se refieren los apartados 1, 2 y 3 cuando el tratamiento tenga lugar con fines de investigación científica y el suministro de la información a que se refieren los apartados 1, 2 y 3 resulte imposible o pueda suponer un esfuerzo desproporcionado en aplicación de las condiciones y garantías a que se refiere el artículo 13, o en la medida en que sea probable que la obligación a que se refiere el apartado 1 del presente artículo imposibilite u obstaculice gravemente el logro de los objetivos de dicho tratamiento. En tales casos, el responsable

adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información.».

6. En el artículo 24, los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Una decisión que surta efectos jurídicos para un interesado o le afecte significativamente de forma similar solo podrá basarse en un tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión:

- a) sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, con independencia de que la decisión pueda adoptarse por medios distintos de los meramente automatizados;
- b) esté autorizada por el Derecho de la Unión que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o
- c) se base en el consentimiento explícito del interesado.».

7. En el artículo 34, el apartado 1 se sustituye por el texto siguiente:

«1. En caso de violación de la seguridad de los datos personales que pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento notificará sin demora indebida y, cuando sea posible, a más tardar noventa y seis horas después de haber tenido conocimiento de ella, la violación de la seguridad de los datos personales al Supervisor Europeo de Protección de Datos. Si la notificación al Supervisor Europeo de Protección de Datos no tiene lugar en el plazo de noventa y seis horas, deberá ir acompañada de indicación de los motivos de la dilación.».

8. En el artículo 37 se añaden los apartados siguientes:

«2) El almacenamiento de datos personales, o la obtención de acceso a datos personales ya almacenados en el equipo terminal de una persona física solo se permite cuando dicha persona haya dado su consentimiento, de conformidad con el presente Reglamento.

3) El apartado 1 no será óbice para el almacenamiento de datos personales, ni la obtención de acceso a los datos personales ya almacenados en el equipo terminal de una persona física sobre la base del Derecho de la Unión en el sentido del artículo 5 y con sujeción a las condiciones de este, a fin de salvaguardar los objetivos a que se refiere el artículo 25, apartado 1.

4) El almacenamiento de datos personales o la obtención de acceso a los datos personales ya almacenados en el equipo terminal de una persona física sin consentimiento y el tratamiento posterior serán lícitos en la medida en que sean necesarios para cualquiera de los fines siguientes:

- a) efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas;
- b) prestar un servicio expresamente solicitado por el interesado;
- c) crear información agregada sobre el uso de un servicio en línea para medir la audiencia de dicho servicio, cuando lo lleve a cabo el

responsable del tratamiento de dicho servicio en línea únicamente para utilización propia;

d) mantener o restablecer la seguridad de un servicio prestado por el responsable del tratamiento y solicitado por el interesado o el equipo terminal utilizado para la prestación de dicho servicio.

5) Cuando el almacenamiento de datos personales, o la obtención de acceso a datos personales ya almacenados, en el equipo terminal de una persona física se base en el consentimiento, se aplicará lo siguiente:

a) el interesado podrá denegar las solicitudes de consentimiento de manera fácil e inteligible con un botón de un solo clic o medios equivalentes;

b) si el interesado da su consentimiento, el responsable del tratamiento no presentará una nueva solicitud de consentimiento para el mismo fin durante el período durante el cual el responsable del tratamiento pueda basarse legalmente en el consentimiento del interesado;

c) si el interesado deniega una solicitud de consentimiento, el responsable del tratamiento no podrá presentar una nueva solicitud de consentimiento para el mismo fin durante un período de al menos seis meses.

El presente apartado también se aplica al tratamiento posterior de datos personales basado en el consentimiento.

6) El presente artículo será aplicable a partir del ... [OP: insértese la fecha correspondiente a seis meses después de la entrada en vigor del presente Reglamento].

7) Los responsables del tratamiento velarán por que sus interfaces en línea permitan a los interesados:

a) dar su consentimiento por medios automatizados y legibles por máquina, siempre que se cumplan las condiciones para el consentimiento establecidas en el presente Reglamento;

b) denegar una solicitud de consentimiento por medios automatizados y legibles por máquina.

8) Los responsables del tratamiento respetarán las decisiones tomadas por los interesados de conformidad con el apartado 7.

9) Se presumirá que las interfaces en línea de los responsables del tratamiento conformes con las normas armonizadas o partes de ellas a que se refiere el artículo 88 *ter*, apartado 4, del Reglamento (CE) 2016/679 cumplen los requisitos que contemplan tales normas o partes de ellas establecidos en el apartado 7.

10) Los apartados 7 a 9 serán aplicables a partir del [OP: insértese la fecha correspondiente a veinticuatro meses después de la entrada en vigor del presente Reglamento].

8) El artículo 39 se modifica como sigue:

a) el apartado 4 se sustituye por el texto siguiente:

«4. Las listas, la plantilla y la metodología adoptados por la Comisión a que se refiere el artículo 35, apartado 6 *bis*, del Reglamento (UE) 2016/679 deben aplicarse al tratamiento de datos personales en virtud del presente Reglamento.»;

b) se suprimen los apartados 5 y 6.

9) Se añade el artículo siguiente:

«Artículo 45 bis

Los criterios comunes adoptados por la Comisión a que se refiere el artículo 41 *bis* del Reglamento (UE) 2016/679 deben aplicarse al tratamiento de datos personales en virtud del presente Reglamento.».

Artículo 5

Modificaciones de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas)

La Directiva 2002/58/CE se modifica como sigue:

1. Se suprime el artículo 4.

2. En el apartado 3 del artículo 5 se añade el párrafo siguiente:

«El presente apartado no se aplicará si el abonado o usuario es una persona física y la información almacenada o a la que se ha accedido constituye o conduce al tratamiento de datos personales.».

Artículo 6

Modificaciones de la Directiva (UE) 2022/2555

La Directiva (UE) 2022/2555 se modifica como sigue:

1. Se inserta el artículo 23 *bis* siguiente:

«Artículo 23 bis

Punto de entrada único para la notificación de incidentes

1) La ENISA desarrollará y mantendrá un punto de entrada único para apoyar la obligación de notificar incidentes y sucesos relacionados en virtud de los actos jurídicos de la Unión cuando tales actos jurídicos de la Unión así lo dispongan (“punto de entrada único”). Sin perjuicio de lo dispuesto en el artículo 16 del Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, la ENISA podrá garantizar que el punto de entrada único se base en la plataforma única de notificación creada en virtud de dicho Reglamento.

2) La ENISA adoptará medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos planteados para la seguridad del punto de entrada único y la información presentada o difundida a través del punto de entrada único. La ENISA tendrá en cuenta el carácter sensible de la información presentada o difundida en virtud de los actos jurídicos de la Unión a que se refiere el apartado 1 y velará por que las autoridades competentes en virtud de dichos actos jurídicos de la

Unión tengan acceso a la información y la traten de conformidad con lo dispuesto en tales actos jurídicos.

- 3) La ENISA proporcionará y aplicará las especificaciones sobre las medidas técnicas, operativas y organizativas relativas al establecimiento, el mantenimiento y el funcionamiento seguro del punto de entrada único. La ENISA elaborará las especificaciones en cooperación con la Comisión, la red de CSIRT y las autoridades competentes en virtud de los actos jurídicos de la Unión a que se refiere el apartado 1. Las especificaciones garantizarán lo siguiente:
 - a) que se garantice la capacidad necesaria para la interoperabilidad con respecto a otras obligaciones de notificación pertinentes a que se refiere el apartado 1;
 - b) que se hayan implantado mecanismos técnicos para que las entidades y autoridades pertinentes en virtud de los actos jurídicos de la Unión a que se refiere el apartado 1 accedan a la información procedente del punto de entrada único, la presenten, la recuperen, la transmitan o traten de otro modo y que proporcionen protocolos y herramientas técnicas que permitan a las entidades y autoridades tratar posteriormente la información recibida dentro de sus sistemas;
 - c) que se tengan en cuenta debidamente las especificidades de los requisitos de notificación de incidentes establecidos en los actos jurídicos de la Unión a que se refiere el apartado 1;
 - d) que, cuando proceda, el punto de entrada único sea interoperable y compatible con las carteras europeas para empresas a que se refiere el [propuesta de Reglamento: insértese el título de la propuesta] y que las carteras europeas para empresas puedan utilizarse al menos para identificar y autenticar a las entidades que utilizan el punto de entrada único;
 - e) que las entidades que utilicen el punto de entrada único puedan recuperar y complementar la información que hayan presentado previamente a través del punto de entrada único;
 - f) que pueda utilizarse una única notificación de información presentada por una entidad a través del punto de entrada único para cumplir las obligaciones de notificación establecidas en cualquiera de los demás actos jurídicos de la Unión que prevén la notificación de incidentes al punto de entrada único.
- 4) Salvo disposición en contrario en los actos jurídicos de la Unión a que se refiere el apartado 1 del presente artículo, la ENISA no tendrá acceso a las notificaciones presentadas a través del punto de entrada único.
- 5) En un plazo de [dieciocho] meses a partir de la entrada en vigor del presente Reglamento, y una vez consultadas la Comisión y a las autoridades competentes pertinentes en virtud de los respectivos actos jurídicos de la Unión, la ENISA probará el funcionamiento del punto de entrada único para cada acto jurídico de la Unión añadido, lo que incluirá pruebas que tengan en cuenta las especificidades y los requisitos para las notificaciones establecidos en cada acto jurídico de la Unión respectivo. La ENISA solo permitirá la notificación de incidentes en virtud de cada acto jurídico de la Unión a que se refiere el apartado 1 después de poner a prueba el funcionamiento y después de que la Comisión haya publicado un anuncio con arreglo al apartado 6.

- 6) La Comisión, en cooperación con la ENISA, evaluará el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad del punto de entrada único. Cuando la Comisión, previa consulta a la red de CSIRT y a las autoridades competentes en virtud de los actos jurídicos de la Unión a que se refiere el apartado 1, constatare que el punto de entrada único garantiza el correcto funcionamiento, la fiabilidad, la integridad y la confidencialidad, publicará un anuncio a tal efecto en el *Diario Oficial de la Unión Europea*.
- 7) Cuando la Comisión constatare en su evaluación que el punto de entrada único no garantiza el correcto funcionamiento, la fiabilidad, la integridad o la confidencialidad, la ENISA adoptará, en cooperación con la Comisión y sin demora indebida, todas las medidas correctoras necesarias para garantizar el correcto funcionamiento, la fiabilidad, la integridad o la confidencialidad e informará a la Comisión de los resultados. Posteriormente, la Comisión volverá a evaluar el correcto funcionamiento, fiabilidad, integridad o confidencialidad del punto de entrada único y publicará un anuncio de conformidad con el apartado 6.».
2. El artículo 23 se modifica como sigue:
- a) en el apartado 1, la primera frase se sustituye por el texto siguiente:
- «Cada Estado miembro velará por que las entidades esenciales e importantes notifiquen, sin demora indebida, a su CSIRT o, en su caso, a su autoridad competente, de conformidad con el apartado 4 del presente artículo, cualquier incidente que tenga un impacto significativo en la prestación de sus servicios a que se refiere el apartado 3 del presente artículo (incidente significativo) a través del punto de entrada único establecido con arreglo al artículo 23 *bis*.»;
- b) se añade el apartado 12 siguiente:
- «Cuando un fabricante notifique un incidente grave con arreglo al artículo 14, apartado 3, del Reglamento (UE) 2024/2847 y la notificación del incidente con arreglo a dicho artículo contenga la información pertinente exigida en el apartado 4 del presente artículo, la notificación del fabricante con arreglo al artículo 14, apartado 3, del Reglamento (UE) 2024/2847 constituirá una notificación de información con arreglo al apartado 4 del presente artículo.».
3. En el artículo 30, el apartado 1 se sustituye por el texto siguiente:
- «1. Los Estados miembros velarán por que, además de la obligación de notificación prevista en el artículo 23, las notificaciones puedan presentarse a los CSIRT o, en su caso, a las autoridades competentes, con carácter voluntario a través del punto de entrada único establecido con arreglo al artículo 23 *bis*, por parte de:
- a) las entidades esenciales e importantes en el caso de incidentes, ciberamenazas y cuasiincidentes;
- b) las entidades distintas de las mencionadas en la letra a), independientemente de si están o no comprendidas en el ámbito de aplicación de la presente Directiva, en el caso de incidentes, ciberamenazas o cuasiincidentes significativos.».

Artículo 7

Modificación del Reglamento (UE) n.º 910/2014

El Reglamento (UE) 910/2014 se modifica como sigue:

1. En el artículo 19 *bis* se inserta el apartado 1 *bis* siguiente:

«1 *bis*. Las notificaciones con arreglo al apartado 1, letra b), del presente artículo al organismo de supervisión y, en su caso, a otras autoridades competentes pertinentes, se efectuarán a través del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555.».
2. En el artículo 24, se inserta el apartado 2 *bis* siguiente:

«2 *bis*. Las notificaciones con arreglo al apartado 2, letra f *bis*), del presente artículo al organismo de supervisión y, en su caso, a otros organismos competentes pertinentes, se efectuarán a través del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555.».
3. En el artículo 45 *bis* se inserta el apartado 3 *bis* siguiente:

«3 *bis*. Las notificaciones con arreglo al apartado 3 a la Comisión y al organismo de supervisión competente se efectuarán a través del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555.».

Artículo 8

Modificaciones del Reglamento (UE) 2022/2554

El artículo 19 del Reglamento (UE) 2022/2554 se modifica como sigue:

1. en el apartado 1, el párrafo primero se modifica como sigue:

«Las entidades financieras notificarán los incidentes graves relacionados con las TIC a la autoridad competente pertinente a que se refiere el artículo 46 a través del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555, de conformidad con el apartado 4 del presente artículo.».
2. en el apartado 2, el párrafo primero se sustituye por el texto siguiente:

«Las entidades financieras podrán notificar, de manera voluntaria, ciberamenazas importantes a la autoridad competente pertinente a través del punto de entrada único con arreglo al artículo 23 *bis* de la Directiva (UE) 2022/2555 cuando consideren que la amenaza es pertinente para el sistema financiero, los usuarios del servicio o los clientes. La autoridad competente pertinente podrá transmitir esta información a otras autoridades pertinentes mencionadas en el apartado 6.».

Artículo 9

Modificaciones de la Directiva (UE) 2022/2557

El artículo 15 de la Directiva (UE) 2022/2557 se modifica como sigue:

1. en el apartado 1, la primera frase se sustituye por la frase siguiente:

«Los Estados miembros se asegurarán de que las entidades críticas notifiquen a la autoridad competente sin demora indebida, a través del punto de entrada

único establecido en virtud del artículo 23 *bis* de la Directiva (UE) 2022/2555, los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales.».

2. en el apartado 2 se añade el párrafo siguiente:

«La Comisión podrá adoptar actos de ejecución que especifiquen en mayor medida el tipo y el formato de la información notificada con arreglo al artículo 15, apartado 1. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 24, apartado 2.».

Artículo 10

Derogaciones y disposiciones transitorias

1. Queda derogado el Reglamento (UE) 2019/1150/UE con efectos a partir de [fecha = la entrada en aplicación del presente Reglamento].
2. No obstante lo dispuesto en el apartado 1, las siguientes disposiciones seguirán aplicándose hasta el 31 de diciembre de 2032:
 - a) artículo 2, punto 1;
 - b) artículo 2, punto 2;
 - c) artículo 2, punto 5;
 - d) artículo 4;
 - e) artículo 11;
 - f) artículo 15.
3. Quedan derogados los siguientes actos, con efecto a partir del [fecha, en consonancia con la entrada en vigor de las modificaciones]:
 - a) Reglamento (UE) 2022/868;
 - b) Reglamento (UE) 2018/1807;
 - c) Directiva (UE) 2019/1024.
4. Las referencias al Reglamento (UE) 2022/868, al Reglamento (UE) 2018/1807 y a la Directiva 2019/1024 se leerán con arreglo a la tabla de correspondencias que figura en el anexo I del presente Reglamento.

Artículo 11

DISPOSICIONES FINALES

El presente Reglamento entrará en vigor a los tres días de su publicación en el *Diario Oficial de la Unión Europea*.

No obstante lo dispuesto en el apartado 3, el artículo 5, apartado 2, entrará en vigor seis meses después de su publicación en el *Diario Oficial de la Unión Europea*.

El artículo 3, apartado 8, letras a) a c), el artículo 6, apartados 2 y 3, y 7 a 9, entrarán en vigor dieciocho meses después de la entrada en vigor del presente Reglamento. No obstante lo dispuesto en la primera frase, cuando la Comisión considere en su evaluación con arreglo al artículo 23 *bis*, apartado 7, de la Directiva (UE) 2022/2555 que el punto de entrada único no garantiza el correcto funcionamiento, la fiabilidad, la integridad o la confidencialidad, las obligaciones de notificación a través del punto de entrada único establecidas en el artículo 23, apartado 4, de la Directiva (UE) 2022/2555, el artículo 19 *bis*, apartado 1 *bis*, el artículo 24, apartado 2 *bis*, y el artículo 45 *bis*, apartado 3 *bis*, del Reglamento (UE) n.º 910/2014, el artículo 33, apartado 1, del Reglamento (UE) 2016/679, el artículo 19, apartados 1 y 2, del Reglamento (UE) 2022/2554, y el artículo 15, apartado 1, de la Directiva (UE) 2022/2557 entrarán en vigor veinticuatro meses después de la entrada en vigor del presente Reglamento.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo
La Presidenta / El Presidente

Por el Consejo
La Presidenta / El Presidente

FICHA LEGISLATIVA DE FINANCIACIÓN Y DIGITAL

1. MARCO DE LA PROPUESTA/INICIATIVA.....	3
1.1. Denominación de la propuesta/iniciativa	3
1.2. Ámbito(s) afectado(s).....	3
1.3. Objetivo(s).....	3
1.3.1. Objetivo(s) general(es).....	3
1.3.2. Objetivo(s) específico(s)	3
1.3.3. Resultado(s) e incidencia esperados.....	3
1.3.4. Indicadores de rendimiento	3
1.4. La propuesta/iniciativa se refiere a:	4
1.5. Justificación de la propuesta/iniciativa	4
1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la ejecución de la iniciativa.....	4
1.5.2. Valor añadido de la intervención de la UE (puede derivarse de distintos factores, como una mejor coordinación, seguridad jurídica, una mayor eficacia o complementariedades). A efectos de la presente sección, se entenderá por «valor añadido de la intervención de la UE» el valor resultante de una intervención de la UE que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.....	4
1.5.3. Principales conclusiones extraídas de experiencias similares anteriores.....	4
1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados.....	5
1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de redistribución.....	5
1.6. Duración de la propuesta/iniciativa y de su incidencia financiera	6
1.7. Método(s) de ejecución presupuestaria previsto(s).....	6
2. MEDIDAS DE GESTIÓN	8
2.1. Disposiciones en materia de seguimiento e informes	8
2.2. Sistema(s) de gestión y de control.....	8
2.2.1. Justificación del / de los método(s) de ejecución presupuestaria, del / de los mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos.....	8
2.2.2. Información relativa a los riesgos detectados y al / a los sistema(s) de control interno establecidos para atenuarlos.....	8
2.2.3. Estimación y justificación de la eficiencia en términos de costes de los controles (ratio entre los gastos de control y el valor de los correspondientes fondos gestionados), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)	8
2.3. Medidas de prevención del fraude y de las irregularidades	9
3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA	10
3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)	10

3.2. Incidencia financiera estimada de la propuesta en los créditos.....	12
3.2.1. Resumen de la incidencia estimada en los créditos operativos.....	12
3.2.1.1. Créditos procedentes del presupuesto aprobado	12
3.2.1.2. Créditos procedentes de ingresos afectados externos	17
3.2.2. Resultados estimados financiados con créditos operativos.....	22
3.2.3. Resumen de la incidencia estimada en los créditos administrativos	24
3.2.3.1. Créditos procedentes del presupuesto aprobado	24
3.2.3.2. Créditos procedentes de ingresos afectados externos	24
3.2.3.3. Total de los créditos	24
3.2.4. Necesidades estimadas de recursos humanos.....	25
3.2.4.1. Financiadas con el presupuesto aprobado	25
3.2.4.2. Financiadas con ingresos afectados externos	26
3.2.4.3. Necesidades totales de recursos humanos	26
3.2.5. Descripción de la incidencia estimada en las inversiones relacionadas con la tecnología digital.....	28
3.2.6. Compatibilidad con el marco financiero plurianual vigente	28
3.2.7. Contribución de terceros	28
3.3. Incidencia estimada en los ingresos	29
4. Dimensiones digitales	29
4.1. Obligaciones con repercusión digital	30
4.2.Data	30
4.3. Soluciones digitales.....	31
4.4. Evaluación de la interoperabilidad	31
4.5. Medidas de apoyo a la digitalización	32

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la simplificación del acervo digital, por el que se modifican el Reglamento (UE) 2023/2854, el Reglamento (UE) 2016/679, el Reglamento (UE) 2024/1689, la Directiva 2002/58/CE y la Directiva (UE) 2022/2555 y se derogan el Reglamento (UE) 2022/868, el Reglamento (UE) 2018/1807, el Reglamento (UE) 2019/1150 y la Directiva (UE) 2019/1024 (Reglamento Ómnibus Digital para el acervo digital)

1.2. Ámbito(s) afectado(s)

Redes de comunicación, contenido y tecnologías;
Mercado Interior, Industria, Emprendimiento y Pymes

1.3. Objetivo(s)

1.3.1. Objetivo(s) general(es)

Simplificación de la aplicación del acervo digital y ahorro de costes para las empresas

1.3.2. Objetivo(s) específico(s)

Objetivo específico n.º 1

Mejorar la gobernanza y la aplicación efectiva del acervo digital mediante la reducción de la complejidad de las normas, los costes administrativos para las empresas y las administraciones, y la derogación de actos legislativos

Objetivo específico n.º 2

Proporcionar un punto de entrada único para la notificación de incidentes en varios marcos jurídicos

1.3.3. Resultado(s) e incidencia esperados

Especificar los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios/grupos destinatarios.

Reducción de los costes para las empresas como consecuencia de la disminución de la complejidad de la legislación y la racionalización de la presentación de informes

1.3.4. Indicadores de rendimiento

Especificar los indicadores para hacer un seguimiento de los avances y logros.

Indicador 1

Reducciones de costes calculadas para las empresas

Indicador 2

Ahorro de costes para la notificación de incidentes por parte de las empresas

Indicador 3

1.4. La propuesta/iniciativa se refiere a:

- una acción nueva
- una acción nueva a raíz de un proyecto piloto / una acción preparatoria³⁹
- la prolongación de una acción existente
- una fusión o reorientación de una o más acciones hacia otra / una nueva acción

1.5. Justificación de la propuesta/iniciativa

1.5.1. *Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la ejecución de la iniciativa*

La entrada en vigor está prevista en un plazo de tres días a partir de la publicación en el Diario Oficial. La entrada en vigor debe ser inmediata, con notables excepciones para las normas que requieren un período transitorio. En el caso del capítulo III, relativo a la notificación de incidentes y las normas relacionadas con las plataformas, se requiere un período suficiente para su aplicación, que se adapte a las necesidades de las empresas, los Estados miembros y los organismos de la UE.

1.5.2. *Valor añadido de la intervención de la UE (puede derivarse de distintos factores, como una mejor coordinación, seguridad jurídica, una mayor eficacia o complementariedades). A efectos de la presente sección, se entenderá por «valor añadido de la intervención de la UE» el valor resultante de una intervención de la UE que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.*

Las razones para una intervención a nivel de la UE se derivan del hecho de que las modificaciones se refieren a la legislación vigente de la UE y reducen la complejidad del Derecho de la Unión (*ex ante*)

El valor añadido de la UE que se espera generar (*ex post*) consiste en racionalizar el Derecho de la Unión y reducir la carga administrativa y los costes para las empresas.

Para la creación del punto de entrada único para la notificación de incidentes, el valor añadido concreto reside en proporcionar una solución a escala de la Unión que atienda a los requisitos nacionales. Los costes para las empresas se optimizan al proporcionar un punto único, independientemente del lugar en el que esté situada la entidad notificante en la Unión y de las autoridades encargadas de recibir las notificaciones.

1.5.3. *Principales conclusiones extraídas de experiencias similares anteriores*

Las modificaciones de los reglamentos correspondientes se basan en la experiencia práctica en la aplicación de las normas, tal como se detalla en el documento de trabajo de los servicios de la Comisión adjunto. Se basan en una amplia consulta a las partes interesadas, que se centró principalmente en la aplicación cotidiana de las normas.

³⁹ Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

Las modificaciones son compatibles con el marco financiero plurianual, ya que no se prevén gastos adicionales.

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de redistribución

No procede.

1.6. Duración de la propuesta/iniciativa y de su incidencia financiera

5. Duración limitada
- en vigor desde [el DD.MM.]AAAA hasta [el DD.MM.]AAAA
- incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.
6. Duración ilimitada
- Ejecución: fase de puesta en marcha desde AAAA hasta AAAA y pleno funcionamiento a partir de la última fecha.

1.7. Método(s) de ejecución presupuestaria previsto(s)⁴⁰

7. **Gestión directa** por la Comisión
- por sus servicios, incluido su personal en las Delegaciones de la Unión;
- por las agencias ejecutivas.
8. **Gestión compartida** con los Estados miembros
9. **Gestión indirecta** mediante delegación de competencias de ejecución del presupuesto en:
- terceros países o los organismos que estos hayan designado;
- organizaciones internacionales y sus agencias (especificar);
- el Banco Europeo de Inversiones y el Fondo Europeo de Inversiones;
- los organismos a que se refieren los artículos 70 y 71 del Reglamento Financiero;
- organismos de Derecho público;
- organismos de Derecho privado investidos de una misión de servicio público, en la medida en que estén dotados de garantías financieras suficientes;
- organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;
- organismos o personas a los cuales se haya encomendado la ejecución de acciones específicas en el marco de la política exterior y de seguridad común, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificados en el acto de base pertinente;
- organismos establecidos en un Estado miembro, que se rijan por el Derecho privado de un Estado miembro o el Derecho de la Unión y reúnan las condiciones para que se les encomiende, de conformidad con las normas sectoriales

⁴⁰ En el sitio BUDGpedia puede consultarse información detallada sobre los métodos de ejecución presupuestaria y las referencias al Reglamento Financiero: <https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx>

específicas, la ejecución de fondos de la Unión o garantías presupuestarias, en la medida en que estén controlados por organismos de Derecho público o por organismos de Derecho privado investidos de una misión de servicio público y estén dotados de unas garantías financieras suficientes, en forma de responsabilidad solidaria de los organismos controladores o garantías financieras equivalentes, que podrán limitarse, para cada acción, al importe máximo de la ayuda de la Unión.

I

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

10. Las modificaciones serán objeto de seguimiento en el marco de la legislación que se modifica

2.2. Sistema(s) de gestión y de control

2.2.1. *Justificación del / de los método(s) de ejecución presupuestaria, del / de los mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos*

11. Los sistemas de gestión y control que se aplican a la legislación vigente garantizan un control eficaz también de las modificaciones

2.2.2. *Información relativa a los riesgos detectados y al / a los sistema(s) de control interno establecidos para atenuarlos*

12. No se han detectado riesgos adicionales

--

2.2.3. *Estimación y justificación de la eficiencia en términos de costes de los controles (ratio entre los gastos de control y el valor de los correspondientes fondos gestionados), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)*

13. El coste del control no diferirá del coste anterior

2.3. Medidas de prevención del fraude y de las irregularidades

14. Siguen aplicándose las mismas medidas preventivas a las modificaciones

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

Líneas presupuestarias existentes

15. En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND ⁴¹	de países de la AELC ⁴²	de países candidatos y candidatos potenciales ⁴³	de otros terceros países	otros ingresos afectados
	20 02 06. Gastos administrativos	CND	NO	NO	NO	NO

Nuevas líneas presupuestarias solicitadas

16. En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND	de países de la AELC	de países candidatos y candidatos potenciales	de otros terceros países	otros ingresos afectados

⁴¹ CD = créditos disociados / CND = créditos no disociados.

⁴² AELC: Asociación Europea de Libre Comercio.

⁴³ Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos operativos

La propuesta/iniciativa no exige la utilización de créditos operativos.

La propuesta/iniciativa exige la utilización de créditos operativos, tal como se explica a continuación

3.2.1.1. Créditos procedentes del presupuesto aprobado

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual		Número					
DG: <.....>			Año	Año	Año	Año	Total MFP 2021-2027
			2024	2025	2026	2027	
Créditos operativos							
Línea presupuestaria	Compromisos	(1a)					0,000
	Pagos	(2a)					0,000
Línea presupuestaria	Compromisos	(1b)					0,000
	Pagos	(2b)					0,000
Créditos de carácter administrativo financiados mediante la dotación de programas específicos ⁴⁴							
Línea presupuestaria		(3)					0,000
TOTAL de los créditos para la DG <.....>	Compromisos	= 1a + 1b + 3	0,000	0,000	0,000	0,000	0,000
	Pagos	= 2a + 2b + 3	0,000	0,000	0,000	0,000	0,000

⁴⁴ Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

Esta sección debe rellenarse utilizando los «datos presupuestarios de carácter administrativo» que deben introducirse en primer lugar en el anexo de la ficha legislativa de financiación y digital (anexo 5⁴⁵ de la Decisión de la Comisión sobre las normas internas de ejecución de la sección relativa a la Comisión del presupuesto general de la Unión Europea), que se carga en DECIDE a efectos de la consulta entre servicios.

DG: <.....>		Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027
• Recursos humanos		0,000	0,000	0,000	0,000	0,000
• Otros gastos administrativos		0,000	0,000	0,000	0,000	0,000
TOTAL PARA LA DG <.....>	Créditos	0,000	0,000	0,000	0,000	0,000

DG: <.....>		Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027
• Recursos humanos		0,000	0,000	0,000	0,000	0,000
• Otros gastos administrativos		0,000	0,000	0,000	0,000	0,000
TOTAL PARA LA DG <.....>	Créditos	0,000	0,000	0,000	0,000	0,000

TOTAL de los créditos de la RÚBRICA 7 del marco financiero plurianual	(Total de compromisos = Total de pagos)	0,000	0,000	0,000	0,000	0,000
--	---	--------------	--------------	--------------	--------------	--------------

En millones EUR (al tercer decimal)

	Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027

⁴⁵ Si se indica haber utilizado los créditos de la rúbrica 7, es obligatorio cumplimentar el anexo 5.

TOTAL de los créditos de las RÚBRICAS 1 a 7	Compromisos	0,000	0,000	0,000	0,000	0,000
del marco financiero plurianual	Pagos	0,000	0,000	0,000	0,000	0,000

3.2.1.2. Créditos procedentes de ingresos afectados externos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	
--	--------	--

DG: <.....>			Año	Año	Año	Año	Total MFP 2021-2027
			2024	2025	2026	2027	
Créditos operativos							
Línea presupuestaria	Compromisos	(1a)					0,000
	Pagos	(2a)					0,000
Línea presupuestaria	Compromisos	(1b)					0,000
	Pagos	(2b)					0,000
Créditos de carácter administrativo financiados mediante la dotación de programas específicos ⁴⁶							
Línea presupuestaria		(3)					0,000
TOTAL de los créditos para la DG <.....>	Compromisos	= 1a + 1b + 3	0,000	0,000	0,000	0,000	0,000
	Pagos	= 2a + 2b + 3	0,000	0,000	0,000	0,000	0,000
Rúbrica del marco financiero plurianual	7	«Gastos administrativos» ⁴⁷					

⁴⁶ Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

En millones EUR (al tercer decimal)

DG: <.....>		Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027
• Recursos humanos		0,000	0,000	0,000	0,000	0,000
• Otros gastos administrativos		0,000	0,000	0,000	0,000	0,000
TOTAL PARA LA DG <.....>	Créditos	0,000	0,000	0,000	0,000	0,000

DG: <.....>		Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027
• Recursos humanos		0,000	0,000	0,000	0,000	0,000
• Otros gastos administrativos		0,000	0,000	0,000	0,000	0,000
TOTAL PARA LA DG <.....>	Créditos	0,000	0,000	0,000	0,000	0,000

TOTAL de los créditos de la RÚBRICA 7 del marco financiero plurianual	(Total de compromisos = Total de pagos)	0,000	0,000	0,000	0,000	0,000
--	---	--------------	--------------	--------------	--------------	--------------

En millones EUR (al tercer decimal)

		Año 2024	Año 2025	Año 2026	Año 2027	Total MFP 2021-2027
TOTAL de los créditos de las RÚBRICAS 1 a 7	Compromisos	0,000	0,000	0,000	0,000	0,000

⁴⁷ Los créditos necesarios deben determinarse utilizando las cifras de costes medios anuales que figuran en la página web correspondiente de BUDGpedia.

del marco financiero plurianual	Pagos	0,000	0,000	0,000	0,000	0,000
---------------------------------	-------	-------	-------	-------	-------	-------

3.2.2. Resultados estimados financiados con créditos operativos

Créditos de compromiso en millones EUR (al tercer decimal)

Indicar los objetivos y los resultados ↓			Año 2024	Año 2025	Año 2026	Año 2027	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase la sección 1.6)										TOTAL			
	RESULTADOS																			
	Tipo ⁴⁸	Coste medio	° Z	Coste	° Z	Coste	° Z	Coste	° Z	Coste	° Z	Coste	° Z	Coste	° Z	Coste	° Z	Coste	Númer o total	Coste total
OBJETIVO ESPECÍFICO N.º 1 ⁴⁹ ...																				
— Resultado																				
— Resultado																				
— Resultado																				
Subtotal del objetivo específico n.º 1																				
OBJETIVO ESPECÍFICO N.º 2 ...																				
— Resultado																				

⁴⁸ Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, kilómetros de carreteras construidos, etc.).

⁴⁹ Tal como se describe en la sección 1.3.2. «Objetivo(s) específico(s)».

Subtotal del objetivo específico n.º 2																
TOTALES																

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

- La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo
- La propuesta/iniciativa exige la utilización de créditos de carácter administrativo, tal como se explica a continuación

3.2.3.1. Créditos procedentes del presupuesto aprobado

CRÉDITOS APROBADOS	Año	Año	Año	Año	TOTAL 2021-2027
	2024	2025	2026	2027	
RÚBRICA 7					
Recursos humanos	0,000	0,000	0,000	0,000	0,000
Otros gastos administrativos	0,000	0,000	0,000	0,000	0,000
Subtotal de la RÚBRICA 7	0,000	0,000	0,000	0,000	0,000
Al margen de la RÚBRICA 7					
Recursos humanos	0,000	0,000	0,000	0,000	0,000
Otros gastos de carácter administrativo	0,000	0,000	0,000	0,000	0,000
Subtotal al margen de la RÚBRICA 7	0,000	0,000	0,000	0,000	0,000
TOTAL	0,000	0,000	0,000	0,000	0,000

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

3.2.4. Necesidades estimadas de recursos humanos

- La propuesta/iniciativa no exige la utilización de recursos humanos
- La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación

3.2.4.1. Financiadas con el presupuesto aprobado

Estimación que debe expresarse en equivalentes a jornada completa (EJC)⁵⁰

17.

CRÉDITOS APROBADOS	Año	Año	Año	Año
	2024	2025	2026	2027
• Empleos de plantilla (funcionarios y personal temporal)				
20 01 02 01 (Sede y oficinas de representación de la Comisión)	0	0	0	0
20 01 02 03 (Delegaciones de la Unión)	0	0	0	0

⁵⁰ Especifique a continuación del cuadro cuántos EJC del número indicado ya se han asignado a la gestión de la acción o pueden reasignarse dentro de su DG y cuáles son sus necesidades netas.

01 01 01 01 (Investigación indirecta)	0	0	0	0
01 01 01 11 (Investigación directa)	0	0	0	0
Otras líneas presupuestarias (especificar)	0	0	0	0
• Personal externo (en EJC)				
20 02 01 (AC, ENCS de la «dotación global»)	0	0	0	0
20 02 03 (AC, AL, ENCS y JPD en las Delegaciones de la Unión)	0	0	0	0
Línea de apoyo administrativo [XX.01.YY.YY]	— en la sede	0	0	0
	— en las Delegaciones de la Unión	0	0	0
01 01 01 02 (AC, ENCS: Investigación indirecta)	0	0	0	0
01 01 01 12 (AC, ENCS: Investigación directa)	0	0	0	0
Otras líneas presupuestarias (especificar) de la rúbrica 7	0	0	0	0
Otras líneas presupuestarias (especificar) al margen de la rúbrica 7	0	0	0	0
TOTAL	0	0	0	0

3.2.5. Descripción de la incidencia estimada en las inversiones relacionadas con la tecnología digital

18. Obligatorio: en el cuadro que figura a continuación debe anotarse la mejor estimación de las inversiones relacionadas con la tecnología digital que conlleva la propuesta/iniciativa.
19. Con carácter excepcional, cuando sea necesario para la ejecución de la propuesta/iniciativa, deben presentarse los créditos de la rúbrica 7 en la fila correspondiente.
20. Los créditos de las rúbricas 1 a 6 deben reflejarse como «Gasto informático en programas operativos». Este gasto se refiere al presupuesto operativo que se utilizará para reutilizar, adquirir o desarrollar plataformas o herramientas informáticas directamente relacionadas con la ejecución de la iniciativa y las inversiones conexas (por ejemplo, licencias, estudios, almacenamiento de datos, etc.). La información proporcionada en este cuadro debe ser congruente con los datos consignados en la sección 4, «Dimensiones digitales».

TOTAL Créditos para fines digitales e informáticos	Año 2024	Año 2025	Año 2026	Año 2027	TOTAL MFP 2021- 2027
RÚBRICA 7					
Gasto informático (institucional)	0,000	0,000	0,000	0,000	0,000
Subtotal de la RÚBRICA 7	0,000	0,000	0,000	0,000	0,000
Al margen de la RÚBRICA 7					
Gasto informático en programas operativos	0,000	0,000	0,000	0,000	0,000
Subtotal al margen de la RÚBRICA 7	0,000	0,000	0,000	0,000	0,000
TOTAL	0,000	0,000	0,000	0,000	0,000

3.2.6. Compatibilidad con el marco financiero plurianual vigente

21. La propuesta/iniciativa:

- puede ser financiada en su totalidad mediante una redistribución dentro de la rúbrica correspondiente del marco financiero plurianual (MFP).
- requiere el uso de los márgenes no asignados con cargo a la rúbrica correspondiente del MFP o el uso de instrumentos especiales tal como se definen en el Reglamento del MFP.
- requiere una revisión del MFP.

3.2.7. *Contribución de terceros*

22. La propuesta/iniciativa:

- no prevé la cofinanciación por terceros
- prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año 2024	Año 2025	Año 2026	Año 2027	Total
Especificar el organismo de cofinanciación					
TOTAL de los créditos cofinanciados					

3.3. Incidencia estimada en los ingresos

- La propuesta/iniciativa no tiene incidencia financiera en los ingresos.
 - La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:
 - en los recursos propios
 - en otros ingresos
 - indicar si los ingresos se asignan a líneas de gasto

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa ⁵¹			
		Año 2024	Año 2025	Año 2026	Año 2027
Artículo					

23. En el caso de los ingresos afectados, especificar la línea o líneas presupuestarias de gasto en la(s) que repercutan.

⁵¹ Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos menos la deducción del 20 % de los gastos de recaudación.

24. [...]
25. Otras observaciones (por ejemplo, método o fórmula utilizada para calcular la incidencia en los ingresos o cualquier otra información).

26. [...]

27. 4. DIMENSIONES DIGITALES

4.1. Obligaciones con repercusión digital

Descripción general de las obligaciones con repercusión digital y de las categorías correspondientes (datos, digitalización y automatización de los procesos, soluciones digitales o servicios públicos digitales)

Referencia a la obligación	Descripción de la obligación	Agentes afectados por la obligación	Procesos generales	Categorías
Artículo 1	Modificación del artículo 1, apartado 1, del Reglamento de Datos para ampliar su ámbito de aplicación al establecimiento de lo siguiente: <ul style="list-style-type: none">• un marco para el registro de los servicios de intermediación de datos;• un marco para la inscripción voluntaria en un registro de las entidades que recojan y traten datos facilitados con fines altruistas;• un marco para la creación de un Comité Europeo de Innovación en materia de Datos.	Comisión Europea Servicios de intermediación de datos Entidades de recogida y tratamiento de datos	Ampliación del ámbito de aplicación del Reglamento de Datos	Servicio público digital
Artículo 1	Modificación del artículo 4, apartado 8, y el artículo 5, apartado 11, del Reglamento de Datos. Los tenedores de datos que se nieguen a compartir datos en virtud de la excepción relativa a los secretos comerciales deberán notificar debidamente	Tenedores de datos (poseedores de un secreto comercial) Originadores de solicitudes de acceso	Notificación	Datos

	dicha decisión.			
Artículo 1	Inclusión del artículo 15 <i>bis</i> en el Reglamento de Datos. Obligación de poner datos a disposición en razón de una emergencia pública.	Organismo del sector público Comisión Europea Banco Central Europeo Organismo de la Unión Tenedores de datos	Puesta a disposición de los datos	Datos
Artículo 1	Modificación del artículo 21, apartado 5, del Reglamento de Datos. Requisitos relativos al intercambio de datos con organizaciones de investigación u organismos estadísticos, obtenidos en el contexto de alguna emergencia pública. Inclusión del artículo 22 <i>bis</i> en el Reglamento de Datos, que permite presentar reclamaciones en relación con el capítulo V («Poner datos a disposición de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión en razón de necesidades excepcionales»).	Organismo del sector público Comisión Europea Banco Central Europeo Organismo de la Unión Tenedor de datos Autoridad nacional competente	Intercambio de datos Denuncias	Datos

Artículo 1	Modificaciones del artículo 32, apartados 1 a 5, del Reglamento de Datos sobre el acceso de terceros países a datos no personales.	Proveedores de servicios de tratamiento de datos Prestadores de servicios de intermediación Organizaciones de gestión de datos con fines altruistas Organismos o autoridades nacionales	Acceso y transferencia internacionales de datos por parte de las administraciones públicas	Datos Servicio público digital
Artículo 1	Modificación del artículo 35, apartado 5, del Reglamento de Datos, que permite a la Comisión adoptar especificaciones comunes relativas a la interoperabilidad de los servicios de tratamiento de datos.	Proveedores de servicios de tratamiento de datos Comisión Europea	Adopción de especificaciones comunes	Servicio público digital
Artículo 1	Modificaciones del artículo 32 <i>bis</i> al artículo 32 <i>sexies</i> del Reglamento de Datos para incluir el capítulo VII <i>bis</i> sobre el marco regulador de una etiqueta europea para los servicios de intermediación de datos, que incluya la notificación, la creación de un registro público, las condiciones para la prestación de servicios, la designación de las autoridades competentes y la supervisión del cumplimiento Modificaciones del artículo 32 <i>nonies</i> del Reglamento de Datos para incluir el	Prestadores de servicios de intermediación Interesados, tenedores de datos y usuarios de datos Estados miembros Autoridades competentes Comisión Europea	Creación de la etiqueta europea para los servicios de intermediación de datos Instauración de la libre circulación de datos en la UE	Datos Soluciones digitales Digitalización de procesos Servicio público digital

	capítulo VII <i>ter</i> sobre la libre circulación de datos dentro de la Unión, que incluya la prohibición de los requisitos de localización de datos, las obligaciones de notificación a la Comisión y la publicación de una lista consolidada.			
Artículo 1	Modificaciones del artículo 32 <i>nonies</i> del Reglamento de Datos para incluir el capítulo VII <i>ter</i> sobre la libre circulación de datos dentro de la Unión, que incluya la prohibición de los requisitos de localización de datos, las obligaciones de notificación a la Comisión y la publicación de una lista consolidada.	Estados miembros Comisión Europea	Instauración de la libre circulación de datos en la UE	Datos Digitalización de procesos Servicio público digital
Artículo 1	Inclusión del artículo 32 <i>decies</i> en el Reglamento de Datos, que define el ámbito de aplicación del capítulo VII <i>quater</i> . El artículo establece un conjunto de normas mínimas que rigen la reutilización y las disposiciones prácticas para facilitar la reutilización de los datos.	Estados miembros Tenedores de datos Usuarios de datos	Definición del objeto y el ámbito de aplicación No discriminación	Servicio público digital

	Inclusión del artículo 32 <i>undecies</i> en el Reglamento de Datos; disposición sobre la no discriminación en lo que respecta a la reutilización de datos y documentos.			
Artículo 1	Inclusión del artículo 32 <i>duodecies</i> en el Reglamento de Datos. Normas relativas a los acuerdos exclusivos para la reutilización de datos. Incluye la obligación de poner a disposición del público las condiciones finales de los acuerdos.	Posibles agentes del mercado Organismos del sector público Partes en tales acuerdos		Servicio público digital Datos
Artículo 1	Modificaciones del Reglamento de Datos: <ul style="list-style-type: none"> • 41): inclusión del artículo 32 <i>quindecies</i> sobre el principio general para la reutilización de datos públicos abiertos. • 42): inserción del artículo 32 <i>sexdecies</i> sobre el tratamiento de las solicitudes de reutilización de datos. • 43): inserción del artículo 32 <i>septdecies</i> sobre los formatos para la reutilización de los datos. • 46): inserción del artículo 32 <i>vicies</i> sobre disposiciones prácticas para facilitar la búsqueda de datos o documentos disponibles para su reutilización. 	Tenedores de datos Usuarios de datos Estados miembros (organismos del sector público) Comisión Europea	Normas de reutilización de datos	Servicio público digital Datos Digitalización de procesos

Artículo 1	Inclusión del artículo 32 <i>unvicies</i> en el Reglamento de Datos; obligación de apoyar la disponibilidad de datos de investigación.	Estados miembros Organismos de investigación Usuarios de datos	Normas de reutilización de datos	Servicio público digital Datos
Artículo 1	Inclusión del artículo 32 <i>duovicies</i> en el Reglamento de Datos. Establecimiento de las disposiciones para la publicación y reutilización de conjuntos de datos específicos de alto valor.	Comisión Europea Organismos del sector público, empresas públicas	Normas de reutilización de datos	Servicio público digital Datos
Artículo 1	Inclusión del artículo 32 <i>quatervicies</i> en el Reglamento de Datos. Establecimiento de las condiciones para la reutilización de determinadas categorías de datos. Los procedimientos para solicitar y las condiciones para permitir dicha reutilización se pondrán a disposición del público a través del punto único de información.	Organismos del sector público Usuarios de datos	Normas de reutilización de datos	Servicio público digital Datos
Artículo 1	Inclusión del artículo 32 <i>quinvicies</i> en el Reglamento de Datos; requisitos para las transferencias de datos no personales a terceros países por parte de los reutilizadores.	Reutilizadores de datos Organismos del sector público Personas físicas/jurídicas cuyos derechos pueden verse afectados	Transferencias de datos a los terceros países	Servicio público digital Datos

Artículo 1	<p>Modificaciones del Reglamento de Datos:</p> <ul style="list-style-type: none"> • 55): inclusión del artículo 32 <i>septvicies</i>; medidas organizativas relativas a los organismos competentes. • 57): inclusión del artículo 32 <i>bis ter</i> sobre los procedimientos para las solicitudes de reutilización de datos. • 58): sustitución del artículo 38, apartados 1 y 2, sobre el derecho a presentar una reclamación. 	<p>Organismos competentes</p> <p>Estados miembros</p> <p>Organismos del sector público</p>	<p>Creación de organismos competentes</p> <p>Procedimientos para las solicitudes</p> <p>Reclamaciones</p>	<p>Servicio público digital</p> <p>Datos</p>
Artículo 1	<p>Inclusión del artículo 32 <i>bis bis</i> en el Reglamento de Datos. Exigencia del uso de un punto único de información para facilitar la reutilización de los datos.</p>	<p>Estados miembros</p> <p>Tenedores de datos</p> <p>Usuarios de datos</p> <p>Comisión Europea</p>	<p>Creación de un punto único de acceso</p>	<p>Soluciones digitales</p> <p>Servicio público digital</p> <p>Digitalización de procesos</p> <p>Datos</p>
Artículo 1	<p>Modificaciones de los artículos 41 <i>bis</i>, 42, 45, 46, 48 <i>bis</i>, 49 y 49 <i>bis</i> del Reglamento de Datos para introducir el capítulo IX <i>bis</i>, por el que se crea el Comité Europeo de Innovación en materia de Datos como grupo de expertos para coordinar el cumplimiento y facilitar el desarrollo de una economía de los datos europea, y que incluyen los requisitos de composición, las</p>	<p>Comisión Europea, Comité Europeo de Innovación en materia de Datos</p> <p>Representantes de los Estados miembros competentes en materia de política de economía de los datos</p>	<p>Establecimiento del Comité Europeo de Innovación en materia de Datos</p>	<p>Servicio público digital</p> <p>Datos</p>

	<p>tareas, la facilitación de la cooperación entre las autoridades competentes y el apoyo a la aplicación coherente de los requisitos legales.</p>	<p>Autoridades competentes para la aplicación de los capítulos II, III y V</p> <p>Autoridades competentes para la reutilización de la información del sector público (Directiva sobre datos abiertos)</p> <p>Autoridades competentes en materia de servicios de intermediación de datos</p> <p>Autoridades competentes para la inscripción en el registro de organizaciones de gestión de datos con fines altruistas</p> <p>Comité Europeo de Protección de Datos (CEPD), Supervisor Europeo de Protección de Datos (SEPD)</p> <p>Agencia de la Unión Europea para la Ciberseguridad (ENISA)</p> <p>Representante de la UE para las pymes o representante de la red de</p>		
--	--	--	--	--

		<p>representantes de la UE para las pymes</p> <p>Otros representantes de organismos pertinentes en sectores específicos</p> <p>Organismos con conocimientos específicos</p> <p>Organismos de normalización</p> <p>Parlamento Europeo, Consejo de la Unión Europea, Comité Económico y Social Europeo</p> <p>Prestadores de servicios de intermediación</p> <p>Organizaciones reconocidas de gestión de datos con fines altruistas</p>		
--	--	---	--	--

Artículo 3	Modificación del artículo 33 del Reglamento (UE) 2016/679 (RGPD) en lo que respecta a las notificaciones de violaciones de la seguridad de los datos personales. Entre otras cosas, exige el uso del punto de entrada único establecido de conformidad con el artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555, y prevé el uso de modelos de notificación.	Asuntos de los datos Responsables del tratamiento de datos Autoridades de control Comité Europeo de Protección de Datos Comisión Europea	Notificación	Datos
Artículo 3	Modificación del artículo 35 y el artículo 70, apartado 1, del Reglamento (UE) 2016/679 (RGPD). Obligación de que el Comité Europeo de Protección de Datos transmita a la Comisión propuestas para seguir poniendo en práctica determinados aspectos de la evaluación de impacto relativa a la protección de datos. Entre ellas, se incluye un modelo común para dichas evaluaciones.	Comité Europeo de Protección de Datos Comisión Europea	Propuestas del CEPD transmitidas a la Comisión	Datos
Artículo 3	Inclusión del artículo 88 <i>ter</i> en el Reglamento (UE) 2016/679 (RGPD); los interesados podrán dar su consentimiento o ejercer el derecho de oposición por medios automatizados y legibles por máquina. Está previsto que una o varias organizaciones europeas de normalización elaboren las normas.	Asuntos de los datos Responsables del tratamiento de datos Organizaciones europeas de normalización Comisión Europea	Indicaciones automatizadas y legibles por máquina de las preferencias del interesado	Soluciones digitales Automatización de procesos

Artículo 6	<p>Modificación de la Directiva (UE) 2022/2555 (SRI 2):</p> <ul style="list-style-type: none"> • (1): inclusión del artículo 23 <i>bis</i> sobre el desarrollo y el mantenimiento de un punto de entrada único para la notificación de incidentes; • (3): modificación del artículo 23, apartado 4, para exigir el uso del punto de entrada único para las notificaciones de incidentes graves; • (4): inclusión del artículo 23, apartado 12, que garantiza que los incidentes graves solo se notifiquen una vez (ya sea en virtud de la Directiva SRI 2 o del Reglamento de Ciberresiliencia); • (5): modificación del artículo 30, apartado 1, que garantiza que el punto de entrada único pueda utilizarse, con carácter voluntario, para las notificaciones de diferentes entidades. 	<p>Notificantes (entidades esenciales e importantes)</p> <p>CSIRT/autoridades competentes (según proceda)</p> <p>Comisión Europea</p> <p>ENISA.</p>	Notificación	<p>Datos</p> <p>Soluciones digitales</p> <p>Servicio público digital</p>
Artículo 7	<p>Modificación del Reglamento (UE) n.º 910/2014 que exige el uso del punto de entrada único, de conformidad con el artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555, para:</p> <ul style="list-style-type: none"> • artículo 19 <i>bis</i>, apartado 1 <i>bis</i>: las 	<p>Notificantes (prestadores no cualificados de servicios de confianza; prestadores cualificados de servicios de confianza; proveedores</p>	Notificación	Datos

	<p>notificaciones a que se refiere el apartado 1, letra b);</p> <ul style="list-style-type: none"> • artículo 24, apartado 2 <i>bis</i>: las notificaciones a que se refiere el apartado 2, letra <i>f ter</i>); artículo 45 <i>bis</i>, apartado 3 <i>bis</i>: las notificaciones a que se refiere el apartado 3. 	<p>de navegadores web)</p> <p>Organismos de supervisión</p> <p>Otros organismos/autoridades competentes pertinentes</p> <p>Comisión Europea</p>		
Artículo 8	<p>Modificación del Reglamento (UE) 2022/2554 (Reglamento sobre Resiliencia Operativa Digital) que exige el uso del punto de entrada único, de conformidad con el artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555, para:</p> <ul style="list-style-type: none"> • artículo 19, apartado 1: incidentes graves relacionados con las TIC; • artículo 19, apartado 2: notificaciones voluntarias de ciberamenazas importantes. 	<p>Notificantes (entidades financieras)</p> <p>Organismos de supervisión</p> <p>Otros organismos/autoridades competentes pertinentes</p> <p>Comisión Europea</p> <p>ENISA.</p>	Notificación	Datos
Artículo 9	<p>Modificación de la Directiva (UE) 2022/2557 (Directiva REC) que exige el uso del punto de entrada único, de conformidad con el artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555, para:</p> <ul style="list-style-type: none"> • artículo 15, apartado 1: incidentes que perturben o puedan perturbar significativamente la prestación de servicios esenciales. 	<p>Notificantes (entidades críticas)</p> <p>Organismos de supervisión</p> <p>Otros organismos/autoridades competentes pertinentes</p> <p>Comisión Europea</p>	Notificación	Datos

		ENISA.		
--	--	--------	--	--

4.2. Datos

Descripción general de los datos incluidos en el ámbito de aplicación

Tipo de datos	Referencia a las obligaciones	Norma o especificación (si procede)
Denegación de una solicitud de acceso a datos sobre la base de la excepción relativa al secreto comercial (y notificación de dicha solicitud a la autoridad competente)	Artículo 1	Deberá justificarse debidamente sobre la base de elementos objetivos.
Los datos deben ponerse a disposición en el contexto de una emergencia pública	Artículo 1	Se incluyen los metadatos necesarios para interpretar y utilizar los datos. En el caso de datos personales, deben estar seudonimizados cuando sea posible.
Notificación de la intención de poner datos a disposición en el contexto de una emergencia pública	Artículo 1	Informar de la identidad y los datos de contacto de la organización o persona que recibe los datos, la finalidad de la transmisión o puesta a disposición de los datos, el período durante el cual deben utilizarse los datos y las medidas técnicas de protección y organizativas adoptadas.
Reclamaciones en virtud del capítulo V («Poner datos a disposición de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión en razón de necesidades excepcionales»).	Artículo 1	//
Datos no personales conservados en la Unión Europea	Artículo 1	//

Datos que deben facilitarse en respuesta a una solicitud de reutilización de datos	Artículo 1	Proporcionar la cantidad mínima de datos admisible
Notificación de la solicitud de reutilización de datos que va a concederse	Artículo 1	//
Datos para los que se prestan servicios de intermediación (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	Formato recibido del interesado / tenedor de datos; conversiones únicamente para mejorar la interoperabilidad o cumplir las normas internacionales/europeas en materia de datos
Información sobre los usos y las condiciones de los datos (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	Debe facilitarse de manera concisa, transparente, inteligible y fácilmente accesible
Solicitudes de inscripción en el registro público de la UE y cambios en la información notificada (etiqueta europea para los servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas)	Artículo 1	Las autoridades competentes establecerán los formularios de solicitud necesarios.
Solicitudes de inscripción en el registro público de la UE aceptadas (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Notificación de cambios posteriores en la información facilitada durante el proceso de solicitud (etiqueta europea para los servicios de intermediación de datos y organizaciones de gestión	Artículo 1	//

de datos con fines altruistas)		
Recepción de la notificación de cambios posteriores (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Información facilitada a los interesados/tenedores de los datos antes del tratamiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Consentimiento (o retirada del consentimiento) para el tratamiento de datos por parte de una organización reconocida de gestión de datos con fines altruistas (etiqueta europea para los servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas)	Artículo 1	Se obtendrá por medios electrónicos
Información sobre la jurisdicción de un tercer país en la que está previsto que se utilicen los datos	Artículo 1	//
Notificación de transferencias, acceso o uso no autorizados de datos no personales (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Información para el seguimiento del cumplimiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de	Artículo 1	Las solicitudes deben ser proporcionadas y estar motivadas

gestión de datos con fines altruistas)		
Notificación de no cumplimiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Decisión de revocar el derecho al uso de la etiqueta (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1	//
Proyectos de actos legislativos sobre los requisitos de localización de datos	Artículo 1	//
Condiciones finales de los acuerdos exclusivos	Artículo 1	//
Datos (o notificaciones) relativos a una solicitud de reutilización	Artículo 1	En cualquier formato o lengua preexistente y, cuando sea posible y apropiado, por medios electrónicos, en formatos abiertos, legibles por máquina, accesibles, localizables y reutilizables, junto con sus metadatos.
Datos de investigaciones públicamente financiadas	Artículo 1	Plenamente disponibles, siguiendo el principio de «abiertos por defecto» y compatibles con los principios FAIR.
Conjuntos de datos específicos de alto valor	Artículo 1	Disponible gratuitamente; serán legibles por máquina; se proporcionarán vía API y en forma de descarga masiva (cuando proceda). Actos de ejecución que deben seguirse; estos pueden incluir

		formatos de datos y metadatos.
Condiciones para permitir la reutilización de los datos o documentos a que se refiere el artículo 2, apartado 54	Artículo 1	Accesible al público.
Notificación de reutilización no autorizada de datos no personales	Artículo 1	//
Notificación de la intención de transferir datos no personales a un tercer país y la finalidad de dicha transferencia (al organismo del sector público)	Artículo 1	//
Notificación de la intención de transferir datos no personales a un tercer país, la finalidad de dicha transferencia y las garantías adecuadas (a la persona física o jurídica cuyos derechos e intereses puedan verse afectados)	Artículo 1	//
Toda la información pertinente relativa a la aplicación de los artículos 32 septvicies (condiciones de reutilización), 32 <i>bis bis</i> (terceros países) y 32 <i>bis ter</i> (tasas) del Reglamento de Datos.	Artículo 1	Disponible y fácilmente accesible a través de un punto único de información.
Reclamación presentada por personas físicas o jurídicas si se han vulnerado sus derechos en virtud del Reglamento de Datos o en relación con otras cuestiones pertinentes	Artículo 1	//
Información sobre el estado de los procedimientos / recursos judiciales en relación con una reclamación	Artículo 1	//

presentada en virtud del Reglamento de Datos		
Datos sobre experiencias y buenas prácticas (Comité Europeo de Innovación en materia de Datos)	Artículo 1	//
Evaluación de los capítulos II, III, IV, V, VI, VII y VIII del Reglamento de Datos Evaluación de los capítulos VII <i>bis</i> , VII <i>ter</i> y VII <i>quater</i> del Reglamento de Datos	Artículo 1 Artículo 1	Se establecen requisitos mínimos de contenido para los informes.
Notificación de violaciones de la seguridad de los datos personales	Artículo 3	A través del punto de entrada único establecido con arreglo al artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555 (y, por tanto, respetando las especificaciones de dicho punto). El Consejo Europeo de Protección de Datos elaborará una propuesta de modelo común (véase la entrada siguiente).
Propuesta del CEPD de un modelo común de notificación de violación de la seguridad de los datos	Artículo 3	//
Propuestas del CEPD sobre la evaluación de impacto relativa a la protección de datos	Artículo 3	//
Informes sobre incidentes significativos con arreglo a la Directiva SRI 2	Artículo 6	A través del punto de entrada único establecido con arreglo al artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555 (y, por tanto, respetando las especificaciones de dicho punto).

Notificación de violaciones de la seguridad de los datos personales	Artículo 3	A través del punto de entrada único establecido con arreglo al artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555 (y, por tanto, respetando las especificaciones de dicho punto)
Notificaciones de incidentes graves relacionados con las TIC con arreglo al Reglamento sobre Resiliencia Operativa Digital; notificaciones voluntarias de ciberamenazas significativas con arreglo al Reglamento sobre Resiliencia Operativa Digital	Artículo 8	A través del punto de entrada único establecido con arreglo al artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555 (y, por tanto, respetando las especificaciones de dicho punto)
Notificaciones de incidentes que perturben o puedan perturbar significativamente la prestación de servicios esenciales, de conformidad con la Directiva REC	Artículo 9	A través del punto de entrada único establecido con arreglo al artículo 23 <i>bis</i> de la Directiva (UE) 2022/2555 (y, por tanto, respetando las especificaciones de dicho punto)

Armonización con la Estrategia Europea de Datos

Explíquese cómo se armonizan las obligaciones con la Estrategia Europea de Datos

Estas modificaciones del Reglamento de Datos establecen el Comité Europeo de Innovación en materia de Datos (capítulo IX *bis*), que coordina la aplicación de las normas y elabora directrices para los espacios comunes europeos de datos sectoriales; las etiquetas europeas para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas (capítulo VII *bis*), que crean un ecosistema confiable para el intercambio de datos y la protección de los derechos; el capítulo VII *ter* aplica la libre circulación de datos no personales al prohibir requisitos de localización de datos injustificados; el capítulo VII *quater* racionaliza las normas sobre la reutilización de los datos del sector público mediante la unificación de las disposiciones de la Directiva sobre datos abiertos y el Reglamento relativo a la gobernanza europea de datos; las normas sobre transferencias internacionales de datos refuerzan la soberanía digital europea al proteger los datos del acceso no autorizado por parte de terceros países; por último, las excepciones para las pymes y la presencia del representante de la UE para las pymes en el Comité Europeo de Innovación en materia de Datos garantizan que la economía de los datos también sea más accesible para las pequeñas empresas.

Armonización con el principio de «solo una vez»

Explíquese cómo se ha tomado en consideración el principio de «solo una vez» y cómo se ha estudiado la posibilidad de reutilizar los datos existentes

Estas modificaciones apoyan el principio de «solo una vez» al crear infraestructuras para la reutilización eficiente de los datos: el Comité Europeo de Innovación en materia de Datos desarrolla normas de interoperabilidad en todos los espacios comunes europeos de datos para reducir la duplicación del suministro de datos; los servicios de intermediación de datos actúan como intermediarios de confianza que permiten el intercambio seguro de los datos existentes y eliminan la recogida redundante; las organizaciones de gestión de datos con fines altruistas facilitan el intercambio voluntario de datos en beneficio público, a fin de que los datos puedan reutilizarse con fines de investigación y para los servicios públicos; las disposiciones sobre la libre circulación evitan las barreras que exigen un almacenamiento de datos en distintas ubicaciones; y, por último, las salvaguardias aplicables a las transferencias internacionales garantizan la accesibilidad transfronteriza de los datos, al tiempo que mantienen la protección, lo que permite que, en conjunto, las personas y las empresas proporcionen sus datos una sola vez y que las necesidades posteriores se atiendan mediante mecanismos de intercambio seguros y respetuosos con sus derechos. Por su parte, las disposiciones relativas al punto de entrada único refuerzan aún más el principio de «solo una vez» en lo que respecta a la notificación de incidentes.

Explíquese en qué medida los datos de nueva creación son localizables, accesibles, interoperables y reutilizables, y cumplen normas de alta calidad

Estas modificaciones garantizan que los datos de nueva creación cumplan los principios FAIR y las normas de calidad a través de mecanismos coordinados: el Comité Europeo de Innovación en materia de Datos desarrolla especificaciones técnicas comunes y protocolos de interoperabilidad accesibles en todos los espacios de datos sectoriales; las disposiciones relativas a la libre circulación evitan la fragmentación que socava la calidad de los datos; la función de coordinación del Comité puede permitir una aplicación armonizada de las normas sobre metadatos, los requisitos técnicos y los parámetros de referencia de calidad en todos los Estados miembros.

Flujos de datos

Descripción general de los flujos de datos

NOTA: La mayoría de los flujos de datos que se detallan a continuación son flujos preexistentes que se trasladan de un Reglamento a otro. En concreto, las disposiciones del Reglamento relativo a la gobernanza europea de datos se transfieren al Reglamento de Datos.

Tipo de datos	Referencia a las obligaciones	Agentes que proporcionan los datos	Agentes que reciben los datos	Desencadenante del intercambio de datos	Frecuencia (si procede)
Denegación de una solicitud de acceso a datos sobre la base de la excepción relativa al secreto comercial (y notificación de dicha solicitud a la autoridad competente)	Artículo 1 Modificación del artículo 4, apartado 8, y el artículo 5, apartado 11, del Reglamento de Datos	Tenedor de datos	Usuario de datos (que realiza la solicitud); autoridad competente designada con arreglo al artículo 37	Denegación de una solicitud de acceso a los datos sobre la base de la excepción del secreto comercial	Carácter <i>ad hoc</i>
Los datos deben ponerse a disposición en el contexto de una emergencia pública	Artículo 1 Inclusión del artículo 15 <i>bis</i> en el Reglamento de Datos	Tenedor de datos	Organismo del sector público; Comisión Europea; Banco Central Europeo; Organismo de la Unión	Emergencia pública + solicitud de acceso a los datos que cumplen las condiciones necesarias	Carácter <i>ad hoc</i>
Notificación de la intención de poner datos a disposición en el contexto de una emergencia pública	Artículo 1 Modificación del artículo 21, apartado 5, del Reglamento de Datos	Organismo del sector público; Comisión Europea; Banco Central Europeo; Organismo de la Unión	Tenedor de datos del que se recibieron los datos	Emergencia pública + intención de transmitir o poner datos a disposición	Carácter <i>ad hoc</i>
Reclamaciones en virtud del capítulo V («Poner datos a disposición de los organismos	Artículo 1 Inclusión del artículo	Tenedor de datos; entidad del sector público;	Autoridad competente del Estado miembro en	Cuando surja un litigio en relación con una solicitud de datos	Carácter <i>ad hoc</i>

del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión en razón de necesidades excepcionales»)	22 bis en el Reglamento de Datos	Comisión Europea: Banco Central Europeo; Organismo de la Unión	el que esté establecido el tenedor de datos	con arreglo al artículo 15 bis del Reglamento de Datos	
Datos no personales conservados en la Unión Europea	Artículo 1 Modificación de los siguientes artículos del Reglamento de Datos: <i>Artículo 32, apartados 1, 3 y 4</i>	Proveedores de servicios de tratamiento de datos, proveedores de servicios de intermediación de datos, organizaciones de gestión de datos con fines altruistas	Órganos jurisdiccionales de terceros países, autoridades administrativas de terceros países, clientes (tenedores de datos / interesados)	Solicitud de un tercer país sobre la base de un acuerdo internacional; solicitud de un tercer país que cumpla las condiciones del artículo 32, apartado 3; solicitud de acceso de un cliente a sus propios datos	Carácter <i>ad hoc</i>
Datos que deben facilitarse en respuesta a una solicitud de reutilización de datos	Artículo 1 Modificación del artículo 32, apartados 4 y 5, del Reglamento de Datos	Proveedor de servicios de intermediación de datos u organización reconocida de gestión de datos con fines altruistas	El originador de la solicitud de reutilización de datos (autoridad de un tercer país)	Fecha de concesión de la solicitud de reutilización	Carácter <i>ad hoc</i>
Notificación de la solicitud de reutilización de datos que va a	Artículo 1	Proveedor de servicios de	Cliente	Solicitud de reutilización de datos	Carácter <i>ad hoc</i>

concederse	Modificación del artículo 32, apartados 4 y 5, del Reglamento de Datos	intermediación de datos u organización reconocida de gestión de datos con fines altruistas		por parte de una autoridad de un tercer país concedida (excepto cuando la solicitud tenga fines de aplicación de la ley)	
Información que debe publicarse en los registros públicos (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>bis</i> en el Reglamento de Datos	Comisión Europea	El público	La información sobre los servicios reconocidos de intermediación de datos o las organizaciones reconocidas de gestión de datos con fines altruistas está disponible o necesita cambios	En curso (registro actualizado periódicamente)
Datos para los que se prestan servicios de intermediación (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>quater</i> en el Reglamento de Datos	Asuntos de los datos Tenedores de datos	Usuarios de datos (a través del proveedor de servicios de intermediación de datos)	Consentimiento del interesado Permiso del tenedor de datos Solicitud del usuario de datos	Según el acuerdo/contrato entre las partes

Información sobre los usos y las condiciones de los datos (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>quater</i> en el Reglamento de Datos	Prestador de servicios de intermediación	Asuntos de los datos	Antes de que el interesado dé su consentimiento para el uso de los datos	Cada vez que se solicite el consentimiento
Solicitudes de inscripción en el registro público de la UE y cambios en la información notificada (etiqueta europea para los servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>sexies</i> en el Reglamento de Datos	Prestadores de servicios de intermediación Organizaciones de gestión de datos con fines altruistas	Autoridad competente del Estado miembro de establecimiento principal	Presentación de la candidatura	Carácter <i>ad hoc</i>
Solicitudes de inscripción en el registro público de la UE aceptadas (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>sexies</i> en el Reglamento de Datos	Autoridad competente	Comisión Europea	Solicitud aprobada	Carácter <i>ad hoc</i> (en un plazo de doce semanas a partir de la recepción de una solicitud, siempre que la decisión sea positiva)
Notificación de cambios posteriores en la información facilitada durante el proceso de solicitud (etiqueta europea para los servicios de intermediación)	Artículo 1 Inclusión del artículo 32 <i>sexies</i> en el Reglamento de	Entidades registradas	Autoridad competente	Cambios en la información facilitada o cuando las entidades cesen sus actividades en la Unión	Carácter <i>ad hoc</i>

de datos y organizaciones de gestión de datos con fines altruistas)	Datos				
Recepción de la notificación de cambios posteriores (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>sexies</i> en el Reglamento de Datos	Autoridad competente	Comisión Europea	Las entidades registradas notifican el cambio (véase la entrada anterior)	<i>Ad hoc</i> , sin demora
Información facilitada a los interesados/tenedores de los datos antes del tratamiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>septies</i> en el Reglamento de Datos	Organización reconocida de gestión de datos con fines altruistas	Asuntos de los datos Tenedores de datos	Antes de cualquier tratamiento de sus datos	Antes de cada actividad de tratamiento (debe ser clara y fácilmente comprensible)
Consentimiento (o retirada del consentimiento) para el tratamiento de datos por parte de una organización reconocida de gestión de datos con fines altruistas (etiqueta europea para los servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>septies</i> en el Reglamento de Datos	Asuntos de los datos Tenedores de datos (si se trata de datos no personales)	Organización de gestión de datos con fines altruistas	Consentimiento del interesado / permiso del tenedor de datos necesario para las actividades de tratamiento	Según el consentimiento/permiso concedido, con posibilidad de retirada en cualquier momento

Información sobre la jurisdicción de un tercer país en la que está previsto que se utilicen los datos	Artículo 1 Inclusión del artículo 32 <i>septies</i> en el Reglamento de Datos	Organización de gestión de datos con fines altruistas	Tenedores de datos	Cuando la organización de gestión de datos con fines altruistas facilite el tratamiento de datos por terceros	Carácter <i>ad hoc</i>
Notificación de transferencias, acceso o uso no autorizados de datos no personales (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>septies</i> en el Reglamento de Datos	Organización de gestión de datos con fines altruistas	Tenedores de datos	Acción no autorizada	<i>Ad hoc</i> , sin demora
Información para el seguimiento del cumplimiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>octies</i> en el Reglamento de Datos	Prestadores de servicios de intermediación Organizaciones de gestión de datos con fines altruistas	Autoridades competentes	Solicitud de una autoridad competente Solicitud de una persona física o jurídica	Carácter <i>ad hoc</i> (previa solicitud, que debe ser proporcionada y motivada)
Notificación de no cumplimiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>octies</i> en el Reglamento de Datos	Autoridad competente	Entidad que se considera no conforme	La autoridad competente considera que un proveedor reconocido de servicios de intermediación de	Carácter <i>ad hoc</i> (seguida de la oportunidad de que la entidad exponga sus observaciones en un plazo de treinta días)

				datos o una organización reconocida de gestión de datos con fines altruistas no es conforme	
Decisión de revocar el derecho al uso de la etiqueta (etiqueta europea para los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas)	Artículo 1 Inclusión del artículo 32 <i>octies</i> en el Reglamento de Datos	Autoridad competente	El público	Tras la decisión de revocación de la etiqueta	Carácter <i>ad hoc</i>
Proyectos de actos legislativos sobre los requisitos de localización de datos	Artículo 1	Estados miembros	Comisión Europea	Creación de un proyecto de acto legislativo que introduce un nuevo requisito de localización de datos o introduce cambios en un requisito de localización de datos existente	Carácter <i>ad hoc</i> , inmediatamente
Condiciones finales de los acuerdos exclusivos	Artículo 1	Partes en el acuerdo	El público	Acuerdos exclusivos establecidos a partir del 16 de julio de 2019	Carácter <i>ad hoc</i> , al menos dos meses antes de la entrada en vigor de un acuerdo

Datos (o notificaciones) relativos a una solicitud de reutilización	Artículo 1 Inclusión del artículo 32 <i>septdecies</i> en el Reglamento de Datos	Organismos del sector público	Originadores de solicitudes de reutilización de datos	Si debe presentarse alguno de los documentos siguientes: datos/documentos solicitados; oferta de licencia; notificaciones de retraso; notificación de una decisión negativa.	Carácter <i>ad hoc</i>
Condiciones finales de los acuerdos exclusivos	Artículo 1 Inclusión del artículo 32 <i>duodecies</i> en el Reglamento de Datos	Partes en un acuerdo exclusivo	Público general	Alcance de las condiciones finales de un acuerdo exclusivo	Carácter <i>ad hoc</i>
Condiciones para permitir la reutilización de los datos o documentos a que se refiere el artículo 2, apartado 54	Artículo 1 Inclusión del artículo 32 <i>septvicies</i> en el Reglamento de Datos	Organismos del sector público (competentes para conceder o denegar solicitudes de acceso)	Público general	Cuando concedan la reutilización de datos o documentos	Carácter <i>ad hoc</i>
Notificación de reutilización no autorizada de datos no personales	Artículo 1 Inclusión del artículo 32 <i>septvicies</i> en el	Reutilizador (posiblemente con la ayuda del	Personas físicas o jurídicas cuyos derechos e	Reutilización no autorizada realizada	Carácter <i>ad hoc</i>

	Reglamento de Datos	organismo del sector público)	intereses puedan verse afectados		
Notificación de la intención de transferir datos no personales a un tercer país y la finalidad de dicha transferencia (al organismo del sector público)	Artículo 1 Inclusión del artículo 32 <i>bis bis</i> en el Reglamento de Datos	Reutilizador	Organismo del sector público	Intención de transferir datos a un tercer país	Carácter <i>ad hoc</i>
Notificación de la intención de transferir datos no personales a un tercer país, la finalidad de dicha transferencia y las garantías adecuadas (a la persona física o jurídica cuyos derechos e intereses puedan verse afectados)	Artículo 1 <i>Inclusión del artículo 32 bis bis en el Reglamento de Datos</i>	Reutilizador (posiblemente con la ayuda del organismo del sector público)	Personas físicas o jurídicas cuyos derechos e intereses puedan verse afectados	Intención de transferir datos a un tercer país	Carácter <i>ad hoc</i>
Toda la información pertinente relativa a la aplicación de los artículos 32 <i>septvicies</i> (condiciones de reutilización), 32 <i>bis bis</i> (terceros países) y 32 <i>bis ter</i> (tasas) del Reglamento de Datos.	Artículo 1 <i>Inclusión del artículo 32 bis quinquies en el Reglamento de Datos</i>	Estados miembros	A disposición de los usuarios del punto único de información	Debe facilitarse la información pertinente	Carácter <i>ad hoc</i>
Reclamación presentada por personas físicas o jurídicas si se han vulnerado sus derechos en virtud del Reglamento de Datos o en relación con otras	Artículo 1 Modificación del artículo 38, apartados 1 y 2, del Reglamento de	Personas físicas o jurídicas	Autoridad competente pertinente del Estado miembro de que se trate	Denuncia que debe presentarse	Carácter <i>ad hoc</i>

cuestiones pertinentes	Datos				
Información sobre el estado de los procedimientos / recursos judiciales en relación con una reclamación presentada en virtud del Reglamento de Datos	Artículo 1 Modificación del artículo 38, apartados 1 y 2, del Reglamento de Datos	Autoridad competente pertinente	Personas físicas o jurídicas que formularon la reclamación	Reclamación presentada	Carácter <i>ad hoc</i>
Datos sobre experiencias y buenas prácticas (Comité Europeo de Innovación en materia de Datos)	Artículo 1 Inclusión del capítulo IX <i>bis</i> en el Reglamento de Datos	Comité Europeo de Innovación en materia de Datos	Comisión; Autoridades competentes	Insumo que debe facilitarse	Carácter <i>ad hoc</i>
Evaluación de los capítulos II, III, IV, V, VI, VII y VIII del Reglamento de Datos Evaluación de los capítulos VII <i>bis</i> , VII <i>ter</i> y VII <i>quater</i> del Reglamento de Datos	Artículo 1 Modificación del artículo 49, apartado 1, del Reglamento de Datos Artículo 1 Modificación del artículo 49, apartado 2, del Reglamento de Datos	Comisión Europea	Parlamento Europeo; Consejo; Comité Económico y Social Europeo	Evaluación del Reglamento de Datos realizada	Plazo: 12 de septiembre de 2028 A más tardar el [fecha de entrada en vigor más cinco años]
Notificación de violaciones de la seguridad de los datos personales	Artículo 3 Modificación del artículo 33, apartado	Responsables del tratamiento de datos	Autoridad de control	Existencia de una violación de la seguridad de los datos	Carácter <i>ad hoc</i>

	1, del RGPD				
Propuesta del CEPD de un modelo común de notificación de violación de la seguridad de los datos	Artículo 3 Modificación del artículo 33, apartado 1, del RGPD	Comité Europeo de Protección de Datos	Comisión	Propuesta que debe presentarse	En un plazo de [meses] a partir de la entrada en vigor del presente Reglamento Cada tres años
Propuestas del CEPD sobre la evaluación de impacto relativa a la protección de datos	Artículo 3 Modificación del artículo 70, apartado 1, del RGPD	Comité Europeo de Protección de Datos	Comisión	Propuesta que debe presentarse	Carácter <i>ad hoc</i>
Informes sobre incidentes significativos con arreglo a la Directiva SRI 2	Artículo 6 Inclusión de los artículos 23 <i>bis</i> y 23 <i>ter</i> , modificación del artículo 23 y el artículo 30, apartado 1, de la Directiva SRI 2	Entidades esenciales e importantes	CSIRT/autoridades competentes (según proceda)	Circunstancias descritas en el artículo 23, apartado 3, de la Directiva SRI 2	Carácter <i>ad hoc</i>
Notificación de violaciones de la seguridad de los datos personales	Artículo 3 Modificación del artículo 33 del RGPD	Responsables del tratamiento de datos	Autoridad de control	Violación de la seguridad de los datos personales	Carácter <i>ad hoc</i>
Notificaciones de incidentes graves relacionados con las TIC con arreglo al Reglamento	Artículo 8 Modificación del	Entes del sector financiero	Autoridad competente	Incidentes graves relacionados con las TIC; ciberamenazas	Carácter <i>ad hoc</i>

sobre Resiliencia Operativa Digital; notificaciones voluntarias de ciberamenazas significativas con arreglo al Reglamento sobre Resiliencia Operativa Digital	artículo 19 del Reglamento sobre Resiliencia Operativa Digital		pertinente	importantes	
Notificaciones de incidentes que perturben o puedan perturbar significativamente la prestación de servicios esenciales, de conformidad con la Directiva REC	Artículo 9 Modificación del artículo 15 de la Directiva REC	Entidades críticas	Autoridad competente	Incidentes que perturben o puedan perturbar significativamente la prestación de servicios esenciales	Carácter <i>ad hoc</i>

4.3. Soluciones digitales

Descripción general de las soluciones digitales

NOTA: Todas las soluciones digitales que se detallan a continuación son soluciones preexistentes cuya base jurídica se traslada de un Reglamento a otro. En concreto, las disposiciones del Reglamento relativo a la gobernanza europea de datos se transfieren al Reglamento de Datos.

Soluciones digitales	Referencia a las obligaciones	Principales funcionalidades asignadas	Organismo responsable	¿Cómo se garantiza la accesibilidad?	¿Cómo se tiene en cuenta la reusabilidad?	Uso de tecnologías de IA (si procede)
Registro público de la Unión de servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas	Inclusión del artículo 32 <i>bis</i> en el Reglamento de Datos	Almacenamiento y publicación de la información obligatoria	Comisión Europea	//	//	No procede
Punto único de información (en virtud del Reglamento de Datos)	Artículo 1 <i>Inclusión del artículo 32 bis quinquies en el Reglamento de Datos</i>	Información que debe estar disponible y accesible; competente para recibir consultas o solicitudes de reutilización de las categorías de datos protegidos; transmitir las solicitudes, cuando	Comisión Europea	Punto único de acceso que ofrece un registro electrónico de datos consultable disponible en los puntos únicos de información nacionales e información adicional sobre	Disponibilidad por medios electrónicos de una lista de activos consultable que contenga una visión general de todos los recursos de datos disponibles [...] y las condiciones para su	No procede

		<p>sea posible y apropiado por medios automatizados, a los organismos competentes del sector público;</p> <p>poner a disposición por medios electrónicos una lista de activos consultable que contenga una visión general de todos los recursos documentales disponibles</p>		<p>cómo solicitar datos a través de dichos puntos únicos de información nacionales</p>	reutilización	
<p>Punto único de acceso para notificaciones de incidentes</p>	<p>Artículo 6</p> <p>Inclusión del artículo 23 <i>bis</i> en la Directiva SRI 2</p>	<p>Permitir la notificación de incidentes con arreglo a los actos pertinentes a nivel de la Unión</p> <p>Garantizar la interoperabilidad y la compatibilidad con las carteras europeas para</p>	<p>Comisión Europea: ENISA.</p>	<p>Interoperabilidad y compatibilidad con las carteras europeas para empresas y sus propios medios de accesibilidad</p>	<p>Posibilidad de atender a la notificación de incidentes en virtud de diferentes actos jurídicos; posibilidad de incorporar en el futuro nuevas bases jurídicas a</p>	<p>No procede</p>

		empresas			la solución de punto de entrada único	
--	--	----------	--	--	---------------------------------------	--

Explíquese en qué medida se ajusta cada solución digital a las políticas digitales y los textos legislativos aplicables

Registro público de la Unión de servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas

Política digital o sectorial (cuando proceda)	Explicación de cómo se armoniza con ella
<i>Reglamento de Inteligencia Artificial</i>	No procede
<i>Marco de ciberseguridad de la UE</i>	No procede
<i>Reglamento eIDAS</i>	No procede
<i>Pasarela digital única e IMI</i>	Modificación del Reglamento (UE) 2018/1724 para añadir «Inscripción como proveedor de servicios de intermediación de datos» e «Inscripción como organización de gestión de datos con fines altruistas reconocida en la Unión» en el anexo II.
<i>Otras</i>	No procede

Punto único de información (en virtud del Reglamento de Datos)

Política digital o sectorial (cuando proceda)	Explicación de cómo se armoniza con ella
<i>Reglamento de Inteligencia Artificial</i>	No procede

<i>Marco de ciberseguridad de la UE</i>	Los organismos del sector público podrán establecer el requisito de acceso y reutilización a distancia de los datos o documentos en un entorno de tratamiento seguro facilitado o controlado por el organismo del sector público. En estos casos, los organismos del sector público impondrán condiciones que preserven la integridad del funcionamiento de los sistemas técnicos del entorno de tratamiento seguro usado.
<i>Reglamento eIDAS</i>	No procede
<i>Pasarela digital única e IMI</i>	No procede
<i>Otras</i>	El punto único de información se ajustará a lo dispuesto en el Reglamento (UE) 2016/679 (RGPD). Los organismos del sector público podrán establecer requisitos para conceder acceso a la reutilización de datos o documentos únicamente cuando estos se hayan anonimizado o estén sujetos a otra forma de preparación pertinente. Además, en caso de reutilización no autorizada de datos no personales, el reutilizador deberá informar a las personas físicas cuyos derechos e intereses puedan verse afectados.

Punto único de acceso para notificaciones de incidentes

Política digital o sectorial (cuando proceda)	Explicación de cómo se armoniza con ella
<i>Reglamento de Inteligencia Artificial</i>	No procede
<i>Marco de ciberseguridad de la UE</i>	Como modificación de la Directiva SRI 2, incorpora un énfasis inherente en la ciberseguridad. En términos más generales, el punto de entrada único tiene por objeto servir de pasarela y canalizar todas las notificaciones de incidentes relacionados con la ciberseguridad a las correspondientes autoridades competentes, en virtud de varios actos jurídicos de la Unión.
<i>Reglamento eIDAS</i>	El punto de entrada único también es obligatorio para la notificación de incidentes con arreglo al

	<p>Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).</p> <p>La ENISA velará por que el punto de entrada único sea interoperable y compatible con las carteras europeas para empresas y por que estas últimas puedan utilizarse al menos para identificar y autenticar a las entidades que utilicen el punto de entrada único. La iniciativa estratégica relativa a la cartera europea para empresas se basará en el marco eIDAS.</p>
<i>Pasarela digital única e IMI</i>	No procede
<i>Otras</i>	La propuesta tuvo en cuenta todo el acervo digital, en particular las políticas relativas a los datos, la ciberseguridad y las telecomunicaciones.

4.4. Evaluación de la interoperabilidad

Descripción general de los servicios públicos digitales afectados por las obligaciones

Servicio público digital o categoría de servicios públicos digitales	Descripción	Referencia a las obligaciones	Solución(es) de la Europa Interoperable (NO PROCEDE)	Otras soluciones de interoperabilidad
Infraestructura europea de transparencia y gobernanza de datos	<p>Servicio público digital que permite establecer una infraestructura de gobernanza y transparencia de los datos y que aprovecha, entre otras cosas, un registro público de la UE de servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas, así como un punto único de información que ayude a los reutilizadores a encontrar información sobre la reutilización de determinadas categorías de datos protegidos.</p> <p>Categoría de servicios públicos digitales con arreglo a la COFOG 04.9.0 - Asuntos económicos n.c.o.p. (CS)</p>	Artículo 1	//	//
Notificación de incidentes	Servicio público digital que permite la notificación de incidentes a través del punto de	Artículo 6	//	Carteras europeas de empresas

	<p>entrada único.</p> <p>Categoría de servicios públicos digitales según la COFOG 03.6.0</p> <p>- Orden público y seguridad n.e.p.</p>			
--	--	--	--	--

Repercusión de las obligaciones sobre la interoperabilidad transfronteriza por cada servicio público digital

NOTA: *En el siguiente análisis, los números de los artículos que se proporcionan a lo largo de la sección «Medida(s)» se refieren al acto o actos legislativos que se modifican. La correspondencia con los requisitos del Omnibus Digital se realiza una vez, en la parte superior de cada celda.*

Servicio público digital n.º 1 - Infraestructura europea de gobernanza de datos y transparencia

Evaluación	Medidas	Posibles obstáculos restantes (si procede)
<p>Armonización con las políticas digitales y sectoriales existentes.</p> <p>Enumérense las políticas digitales y sectoriales aplicables que se hayan establecido</p>	<p>Artículo 1</p> <p>La armonización con las políticas digitales y sectoriales vigentes se refleja en los considerandos del Reglamento relativo a la gobernanza europea de datos:</p> <p>Pasarela digital única [Reglamento (UE) 2018/1724] (considerando 56): los procedimientos de notificación para los servicios de intermediación de datos y los procedimientos de inscripción para las organizaciones de gestión de datos con fines altruistas deben estar disponibles a través de la pasarela digital única y garantizar el acceso transfronterizo en línea.</p> <p>Marco Europeo de Interoperabilidad (considerando 54): la infraestructura digital debe ajustarse a los principios del Marco Europeo de Interoperabilidad para garantizar el uso transfronterizo e intersectorial de los datos.</p> <p>Bloques constitutivos del MCE (infraestructuras de servicios digitales del Mecanismo «Conectar Europa») (considerando 54): referencias «los vocabularios básicos y los módulos del Mecanismo “Conectar Europa”». El servicio digital debe aprovechar los bloques constitutivos del MCE (como la entrega electrónica, la identificación electrónica o</p>	

	<p>la firma electrónica) para la ejecución técnica.</p> <p>Requisitos de accesibilidad [Directivas (UE) 2016/2102 y (UE) 2019/882] (considerando 62). Directiva (UE) 2016/2102 (Directiva sobre accesibilidad de los sitios web): los registros públicos y los servicios digitales deben ser accesibles para las personas con discapacidad; Directiva (UE) 2019/882 (Directiva Europea de Accesibilidad): los servicios digitales deben cumplir los requisitos de accesibilidad.</p> <p>RGPD [Reglamento (UE) 2016/679] (considerandos 4 y 35): todos los servicios digitales que traten datos personales deben cumplir los requisitos del RGPD en materia de protección de datos, privacidad y seguridad.</p> <p>Reglamento (UE) 2018/1725 (considerando 4): cuando las instituciones de la UE traten datos a través de estos registros, deben ajustarse al presente Reglamento.</p> <p>Directiva sobre datos abiertos [Directiva (UE) 2019/1024] (considerandos 6 y 10): “La Directiva (UE) 2019/1024 y la normativa sectorial de la Unión garantizan que los organismos del sector público hagan que una mayor cantidad de los datos que generan estén fácilmente disponibles para su utilización y reutilización”: El servicio digital completa la Directiva sobre datos abiertos al abordar categorías de datos protegidos que quedan fuera de su ámbito de aplicación, al tiempo que garantiza que los organismos del sector público sigan el principio de «abiertos desde el diseño y por defecto» cuando proceda.</p> <p>Políticas sectoriales sobre espacios de datos europeos y datos sectoriales, en particular el Espacio Europeo de Datos de Salud, el espacio común europeo de datos relativos a la movilidad, los datos relativos al Pacto Verde Europeo y al clima y la energía, los datos relativos a la industria y de fabricación, los datos de servicios financieros, los datos agrícolas, el espacio de datos relativos a las administraciones públicas y el espacio de datos en materia de cualificaciones.</p>	
--	---	--

<p>Medidas organizativas para la prestación sencilla de servicios públicos digitales transfronterizos.</p> <p>Enumérense las medidas de gobernanza previstas</p>	<p>Artículo 1</p> <p>Designación y coordinación de la autoridad competente</p> <ul style="list-style-type: none"> - Artículo 32 <i>bis</i>: Cada Estado miembro designará una o varias autoridades competentes responsables de la inscripción en el registro de los proveedores de servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas. Estas autoridades competentes mantendrán su independencia respecto de cualquier proveedor reconocido de servicios de intermediación de datos u organización reconocida de gestión de datos con fines altruistas. <p>Artículo 32 <i>bis quater</i>: Cada Estado miembro designará uno o varios organismos competentes para asistir a los organismos del sector público que concedan o denieguen el acceso para la reutilización de categorías de datos protegidos.</p> <p>Artículo 32 <i>octies</i>: Las autoridades competentes supervisarán el cumplimiento de las disposiciones del Reglamento de Datos por parte de los proveedores reconocidos de servicios de intermediación de datos y las organizaciones reconocidas de gestión de datos con fines altruistas.</p> <p>Mecanismo de competencia transfronteriza</p> <p>Artículo 32 <i>sexies</i>: Los servicios de intermediación de datos son competencia de la autoridad competente del Estado miembro de establecimiento principal. El mismo principio se aplica a las organizaciones de gestión de datos con fines altruistas.</p> <p>Reconocimiento mutuo y registro único</p> <p>Artículo 32 <i>sexies</i>: La inscripción en el registro como servicio de intermediación de datos / organización de gestión de datos con fines altruistas será válida en todos los Estados miembros.</p> <p>Artículo 32 <i>bis</i>: uso de un logotipo común.</p> <p>Registros centralizados a nivel de la UE para la recogida de datos y la transparencia</p>	
--	---	--

	<p>Artículo 32, letra a): Registros públicos de la Unión de todos los proveedores de servicios de intermediación de datos y organizaciones de gestión de datos con fines altruistas</p> <p>Artículo 32, letra e): Las autoridades competentes informarán sin demora a la Comisión por vía electrónica acerca de las nuevas inscripciones, modificaciones y supresiones en el registro, y la Comisión actualizará los registros de la UE en consecuencia.</p> <p>Supervisión y coordinación de la aplicación</p> <p>Autoridades nacionales competentes</p> <p>Comité Europeo de Innovación en materia de Datos</p> <p>Gobernanza de la transferencia de datos de terceros países</p> <p>Artículo 32 <i>bis bis</i>: Requisitos para las transferencias de datos no personales a terceros países por parte de los reutilizadores.</p> <p>Acuerdos exclusivos</p> <p>Artículo 32 <i>duodecies</i>: Define la permisibilidad de los acuerdos exclusivos relativos a la reutilización de los datos y documentos en poder de los organismos del sector público. Exige transparencia de las condiciones finales.</p>	
<p>Medidas adoptadas para garantizar el consenso en cuanto a los datos.</p> <p>Enumérense dichas medidas</p>	<p>Artículo 1</p> <p>Normas comunes y marcos interoperables</p> <ul style="list-style-type: none"> - El Comité Europeo de Innovación en materia de Datos asesora a la Comisión Europea sobre las actividades de normalización que deben emprenderse en relación con los aspectos intersectoriales del intercambio de datos, en particular en relación con la aparición de espacios comunes europeos de datos, teniendo en cuenta las actividades de normalización sectoriales. <ul style="list-style-type: none"> o Artículo 42: El Comité Europeo de Innovación en materia de Datos ayuda a «adoptar directrices que establezcan marcos interoperables y prácticas comunes para el funcionamiento de los espacios comunes europeos de 	

	<p>datos».</p> <ul style="list-style-type: none"> - Logotipo común para identificar a los servicios de intermediación de datos y las organizaciones de gestión de datos con fines altruistas. - Artículo 32 <i>octodecies</i>: Los organismos del sector público y las empresas públicas pondrán sus datos y documentos a disposición, siempre que sea posible y apropiado, por medios electrónicos, en formatos que sean abiertos, legibles por máquina, accesibles, fáciles de localizar y reutilizables, junto con sus metadatos. Tanto el formato como los metadatos cumplirán, cuando sea posible, normas formales abiertas. <p>Otras medidas pertinentes:</p> <ul style="list-style-type: none"> - Artículo 32 <i>unvicies</i>: Los Estados miembros, en cooperación con la Comisión, continuarán los esfuerzos de simplificación del acceso a conjuntos de datos y pondrán a disposición conjuntos de datos adecuados en formatos que sean accesibles, fáciles de localizar y reutilizables por medios electrónicos. - Artículo 32 <i>duovicies</i>: Los Estados miembros apoyarán la disponibilidad de los datos de investigación de una manera compatible con los principios FAIR. 	
<p>Uso de especificaciones y normas técnicas abiertas acordadas en común.</p> <p>Enumérense dichas medidas</p>	<p>Artículo 1</p> <p>Medidas relativas a los datos legibles por máquina:</p> <ul style="list-style-type: none"> - Artículo 32 <i>bis</i>: Registro de la UE, legible por máquina, de proveedores de servicios de intermediación de datos. - Artículo 32 <i>bis</i>: Registro de la UE, legible por máquina, de organizaciones de gestión de datos con fines altruistas. - Artículo 32 <i>octodecies</i>: Los organismos del sector público pondrán sus datos y documentos a disposición, siempre que sea posible, en formatos que sean abiertos, legibles por máquina, accesibles, fáciles de localizar y reutilizables, conjuntamente con sus metadatos. Tanto el formato como los metadatos cumplirán, cuando sea 	

	<p>posible, normas formales abiertas.</p> <ul style="list-style-type: none"> - Artículo 32 <i>octodecies</i>: Los conjuntos de datos de alto valor se pondrán a disposición para su reutilización en un formato legible por máquina, a través de API adecuadas y, cuando proceda, en forma de descarga masiva. - Artículo 32 <i>unvicies</i>: Los Estados miembros crearán dispositivos prácticos que faciliten la búsqueda de los datos o documentos disponibles para su reutilización, tales como listados de datos o documentos principales con los metadatos correspondientes, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina, y portales conectados a los listados. En la medida de lo posible, los Estados miembros facilitarán la búsqueda lingüística de los datos o documentos en varios idiomas. - Artículo 32 <i>tervicies</i>: Los conjuntos de datos específicos de alto valor deben ser legibles por máquina. Los actos de ejecución podrán establecer acuerdos relativos a los formatos de los datos y los metadatos, así como acuerdos técnicos para la difusión. <p>Medidas relativas a la interacción de máquina a máquina:</p> <ul style="list-style-type: none"> - Artículo 32 <i>bis quinquies</i>: Exigencia del uso del punto único de información. El punto único de información será competente para recibir las consultas o solicitudes y las transmitirá, cuando resulte posible y adecuado, a través de medios automatizados, a los organismos del sector público competentes o a los organismos competentes. <p>Otras medidas pertinentes:</p> <ul style="list-style-type: none"> - Artículo 48 <i>bis</i>: Modificación del anexo II del Reglamento (UE) 2018/1724 (pasarela digital única). Sinergias exploradas. - Considerando 52 del Reglamento Ómnibus Digital: en la medida de lo posible, la ENISA debe tener en cuenta las soluciones técnicas nacionales existentes que facilitan la notificación de incidentes, como las plataformas nacionales, cuando 	
--	---	--

	<p>elaboren las especificaciones sobre las medidas técnicas, operativas y organizativas relativas a la creación, el mantenimiento y el funcionamiento seguro del punto de entrada único. La ENISA también debe tener en cuenta protocolos y herramientas técnicas, como interfaces de programación de aplicaciones y normas legibles por máquina, que permitan a las entidades facilitar la integración de las obligaciones de notificación de incidentes en los procesos empresariales y a las autoridades conectar el punto de entrada único con sus sistemas nacionales de notificación.</p>	
--	---	--

Servicio público digital n.º 2 — Notificación de incidentes

Evaluación	Medidas	Posibles obstáculos restantes (si procede)
<p>Armonización con las políticas digitales y sectoriales existentes.</p> <p>Enumérense las políticas digitales y sectoriales aplicables que se hayan establecido</p>	<p>Artículo 6</p> <p>La armonización general con las políticas digitales y sectoriales existentes se ofrece a través de la Directiva (UE) 2022/2555 (SRI 2), que el Reglamento Ómnibus Digital está modificando actualmente. Además, el Reglamento Ómnibus prevé sinergias con la cartera europea para empresas y el Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia). En particular:</p> <ul style="list-style-type: none"> • el artículo 23, apartado 4, exige el uso del punto de entrada único para la notificación en virtud de la Directiva SRI 2; • el artículo 23, apartado 1, establece que una notificación de incidente grave con arreglo al artículo 14, apartado 3, del Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia) también constituirá una notificación de información en virtud de la Directiva (UE) 2022/2555 (SRI 2). Esto se ajusta al principio de «solo una vez»; • el artículo 23 <i>bis</i>, apartado 3, letra d), establece el nexo con las carteras europeas para empresas. 	

<p>Medidas organizativas para la prestación sencilla de servicios públicos digitales transfronterizos.</p> <p>Enumérense las medidas de gobernanza previstas</p>	<p>Artículo 6</p> <p>El artículo 23 <i>bis</i> define las funciones y responsabilidades. A saber, la ENISA:</p> <ul style="list-style-type: none"> • desarrollará y mantendrá un punto de entrada único para apoyar la obligación de notificar incidentes y acontecimientos conexos en virtud de los actos jurídicos de la Unión; • adoptará medidas técnicas, operativas y organizativas para gestionar los riesgos para la seguridad que planteen el punto de entrada único y la información presentada o difundida. Al hacerlo, consultará a la Comisión, a la red de CSIRT y a las autoridades competentes pertinentes. 	
<p>Medidas adoptadas para garantizar el consenso en cuanto a los datos.</p> <p>Enumérense dichas medidas</p>	<p>Artículo 6</p> <p>El artículo 23 <i>bis</i> encarga a la ENISA la elaboración de especificaciones que garanticen la capacidad necesaria para la interoperabilidad con respecto a otras obligaciones de notificación pertinentes.</p> <p><i>NOTA:</i> Los requisitos de contenido para la notificación de incidentes se establecen con más detalle en los actos jurídicos pertinentes de la Unión, incluida la Directiva (UE) 2022/2555 (SRI 2). El artículo 23 <i>bis</i>, apartado 3, letra c), del Reglamento Ómnibus aclara que la ENISA velará por que estos requisitos se tengan debidamente en cuenta.</p>	
<p>Uso de especificaciones y normas técnicas abiertas acordadas en común.</p> <p>Enumérense dichas medidas</p>	<p>Artículo 6</p> <p>El artículo 23 <i>bis</i> exige que se elaboren especificaciones:</p> <ul style="list-style-type: none"> • la ENISA proporcionará y aplicará las especificaciones sobre las medidas técnicas relativas a la creación, el mantenimiento y el funcionamiento seguro del punto de entrada único. Estas especificaciones incluirán, entre otras cosas: <ul style="list-style-type: none"> ○ la capacidad necesaria para la interoperabilidad con respecto a otras 	

	<p>obligaciones de notificación;</p> <ul style="list-style-type: none"> ○ disposiciones técnicas para que las entidades y autoridades pertinentes accedan, presenten, recuperen, transmitan o traten por otro medio la información procedente del punto de entrada único, así como protocolos y herramientas técnicas que permitan a las entidades y autoridades un tratamiento ulterior de la información recibida en sus sistemas. ● Cuando esté disponible, el punto de entrada único será interoperable y compatible con las carteras europeas para empresas. 	
--	---	--

4.5. Medidas de apoyo a la digitalización

Descripción general de las medidas de apoyo a la digitalización

Descripción de la medida	Referencia a las obligaciones	Función de la Comisión (Si procede)	Agentes que deben participar (Si procede)	Calendario previsto (Si procede)
Acto de ejecución: diseño del logotipo común para los proveedores de servicios de intermediación de datos	Artículo 1	Establecer las características del logotipo común, incluidas sus modalidades de diseño y uso.	Comité del procedimiento de examen	//
Acto de ejecución: diseño del logotipo común para las organizaciones reconocidas de gestión de datos con fines	Artículo 1	Establecer las características del logotipo común, incluidas sus modalidades de	Comité del procedimiento de examen	//

altruistas		diseño y uso.		
Supervisión y cumplimiento: las autoridades competentes podrán supervisar el cumplimiento por iniciativa propia o a petición de personas físicas o jurídicas	Artículo 1	//	Autoridades competentes, servicios de intermediación de datos, organizaciones de gestión de datos con fines altruistas	//
Acto de ejecución: Conjuntos de datos específicos de alto valor	Artículo 1	Establecer una lista de conjuntos de datos específicos de alto valor. Podrán especificar los acuerdos para la publicación y reutilización de los tipos de conjuntos de datos de alto valor.	Comité del procedimiento de examen	//
Directrices: <ul style="list-style-type: none"> • el Comité Europeo de Innovación en materia de Datos debe ofrecer asesoramiento sobre las directrices relativas a los espacios comunes europeos de datos; • el Comité Europeo de Innovación en materia de Datos debe adoptar directrices sobre marcos interoperables 	Artículo 1	Ayuda del Comité Europeo de Innovación en materia de Datos	Comité Europeo de Innovación en materia de Datos	//

Acto de ejecución: modelo común para notificar una violación de la seguridad de los datos personales	Artículo 3	Adoptar un modelo común sobre la base de la propuesta del CEPD.	Comité del procedimiento de examen	//
Acto delegado: Indicaciones automatizadas y legibles por máquina de las preferencias del interesado	Artículo 3	Establecer la obligación para los navegadores web y los proveedores de equipos terminales	Comité del procedimiento de examen	//
Acto de ejecución: Notificaciones de incidentes de resiliencia de las entidades críticas	Artículo 9	Especificar en mayor medida el tipo y el formato de la información notificada con arreglo al artículo 15, apartado 1, de la Directiva (UE) 2022/2557 (REC).	//	//