COMISIÓN EUROPEA

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) 2016/1679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854, (UE) 2024/1689 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 por el que se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Omnibus Digital)**

{SWD(2025) 836 final}

# EXPOSICIÓN DE MOTIVOS

## 1. CONTEXTO DE LA PROPUESTA

### • Motivos 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: un nuevo impulso para simplificar, clarificar y mejorar el acervo de la UE, como medida clave para apoyar la competitividad de la Unión.

Esta visión refleja el plan más amplio expuesto por la presidenta de la Comisión, Ursula von der Leyen, en sus orientaciones políticas para el mandato 2024-2029[2]. Como también se destaca en los informes Draghi[3] y Letta[4], la acumulación de normas ha tenido en ocasiones un efecto adverso sobre la competitividad. Se necesitan mejoras rápidas y visibles para los ciudadanos y las empresas, mediante una aplicación más rentable y favorable a la innovación de nuestras normas, manteniendo al mismo tiempo unos niveles elevados y los objetivos acordados.

Las Conclusiones del Consejo Europeo de 20 de marzo de 2025 instaban además a la Comisión a «seguir revisando y sometiendo a pruebas de resistencia el acervo de la UE, con el fin de determinar formas de simplificar y consolidar aún más la legislación»[5]. También subrayaban la necesidad de dar seguimiento con nuevos conjuntos de iniciativas de simplificación. En sus Conclusiones de 26 de junio, el Consejo Europeo subrayó la importancia de una legislación «sencilla por diseño», «sin menoscabar la previsibilidad, los objetivos políticos y los altos niveles de exigencia»(6) .Las Conclusiones del Consejo Europeo de 23 de octubre de 2025 reafirmaron «la urgente necesidad de impulsar un programa ambicioso y horizontal de simplificación y mejora de la legislación a todos los niveles —europeo, nacional y regional— y en todos los ámbitos, a fin de garantizar la competitividad de Europa». También instaron a la Comisión a «presentar rápidamente nuevos paquetes ambiciosos de simplificación, entre otros […] en el ámbito digital»(7) .

En su resolución sobre «la aplicación y racionalización de las normas del mercado interior de la UE para reforzar el mercado único», votada el 11 de septiembre en sesión plenaria [8], el Parlamento Europeo hizo hincapié en la necesidad de simplificar para facilitar el cumplimiento de las normas por parte de las empresas sin comprometer los objetivos políticos fundamentales de la UE.

En las actividades de consulta y participación de la Comisión en torno al programa de simplificación, las partes interesadas que representan diferentes intereses han pedido modificaciones específicas de determinados

---

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

[2] Von der Leyen, U. (2024) *La elección de Europa: Orientaciones políticas para la próxima Comisión Europea 2024-2029*. Disponible en: e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

[3] Draghi, M. (2024) *El futuro de la competitividad europea*. Disponible en: Informe Draghi sobre la competitividad de la UE

[4] Letta, E. (2024) *Mucho más que un mercado*. Disponible en: Enrico Letta - Mucho más que un mercado (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 UE para reforzar el mercado único, 11 de septiembre de 2025 (2025/2009/INI)

normas digitales, con el fin de racionalizar los costes de cumplimiento y aclarar las interacciones entre las normas de su sector.

Con un valor añadido de 791 000 millones de euros en toda la Unión Europea en 2022[9], el sector de las TIC desempeña un papel crucial en el impulso de la competitividad de la UE en todos los sectores de la economía, tanto a través del crecimiento de las empresas digitales como de la oferta de soluciones digitales clave en todos los ámbitos. Las normas digitales han sido fundamentales para configurar un entorno empresarial justo en la UE. Han establecido un verdadero mercado único para los servicios digitales. La UE ha sido pionera en la regulación digital y ha establecido el estándar de referencia para el más alto 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 realizar una «prueba de resistencia» exhaustiva del conjunto de normas digitales a lo largo de todo el mandato legislativo. El objetivo es muy claro: garantizar que las normas sigan siendo adecuadas para apoyar la innovación y el crecimiento, cumplan sus objetivos y sean un motor de la competitividad. A lo largo de este proceso, la Comisión tratará de aportar soluciones convincentes para simplificar, aclarar y consolidar la eficacia de las normas y su aplicación mediante todos los instrumentos disponibles, ya sean ajustes normativos, una mayor cooperación entre las autoridades, la promoción de soluciones digitales que simplifiquen «por diseño» el cumplimiento normativo u otras medidas complementarias.

**La propuesta del Omnibus Digital es un primer paso** para optimizar la aplicación del código normativo digital. Incluye un conjunto de modificaciones técnicas a un amplio corpus de legislación digital, seleccionadas para aliviar de forma inmediata a las empresas, las administraciones públicas y los ciudadanos, con el fin de estimular la competitividad. El objetivo inmediato es garantizar que el cumplimiento de las normas tenga un coste menor, cumpla los mismos objetivos y aporte en 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 realizados por la vicepresidenta ejecutiva Henna Virkkunen y el comisario Michael McGrath.

Por estas razones, las modificaciones se centran en aprovechar las oportunidades que ofrece el uso de los datos, como recurso fundamental de la economía de la UE, sobre todo con vistas a apoyar el desarrollo y el uso de soluciones de inteligencia artificial fiables en el mercado de la UE. Las modificaciones específicas de las normas de protección de datos y privacidad respaldan este objetivo y proporcionan medidas de simplificación inmediatas para las empresas y los particulares, reforzando su capacidad para ejercer sus derechos.

Además, las modificaciones del Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial[10]), 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 el desarrollo y el uso seguros y fiables de la IA.

El Omnibus Digital también propone una solución muy clara para agilizar la notificación de incidentes de ciberseguridad, reuniendo en un único mecanismo de notificación todas las obligaciones de notificación relacionadas.

---

[9] Eurostat (2025) *Estadísticas explicadas: Sector de las TIC: valor añadido, empleo e I+D*. Disponible en: Sector de las TIC: valor añadido, empleo e I+D - Estadísticas explicadas - Eurostat

[10] Según propuesta legislativa separada

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

Las modificaciones tienen por objeto racionalizar las normas, reduciendo el número de leyes y armonizando las disposiciones. Reducen los costes administrativos al simplificar las disposiciones y los procedimientos. Eximen a las pequeñas empresas de mediana capitalización de determinadas obligaciones en toda la legislación sobre datos y el Reglamento (UE) 2024/1689 (la Ley de Inteligencia Artificial[11]), además de las pequeñas y microempresas que ya están cubiertas por un régimen especial. También estimulan las oportunidades para un entorno empresarial dinámico, creando más seguridad jurídica y oportunidades, en particular en lo que se refiere al intercambio y la reutilización de datos, al tratamiento de datos personales o a la formación de sistemas y modelos de inteligencia artificial.

Al mismo tiempo, las modificaciones propuestas siguen siendo de carácter técnico, ya que pretenden ajustar el marco regulador, pero no modificar sus objetivos fundamentales. Las medidas están calibradas para mantener el mismo nivel de protección de los derechos fundamentales.

Junto con el Digital Omnibus, la Comisión también presenta su propuesta de **Reglamento sobre carteras empresariales europeas**, una iniciativa fundamental para simplificar el cumplimiento normativo y reducir las cargas administrativas de las empresas. Las carteras empresariales se diseñarán como herramientas digitales seguras para las empresas, que actuarán como una plataforma única para simplificar sus interacciones en toda la UE. Mediante la implementación de un identificador único y persistente, las empresas podrán verificar digitalmente identidades, firmar documentos, sellar con fecha y hora e intercambiar información digital verificada sin problemas a través de las fronteras mediante el uso de una única solución. Con la adopción de las carteras empresariales europeas, las empresas, especialmente las pymes, podrán cumplir fácilmente con la normativa, liberando recursos vitales que podrán redirigirse hacia el crecimiento y la innovación.

Como segundo paso en el compromiso de someter a «pruebas de resistencia» el reglamento digital, **la Comisión también está llevando a cabo una evaluación de la adecuación digital.** Mientras que las propuestas del paquete «Omnibus» son inmediatas y específicas, el análisis que realizará la Comisión en la evaluación de la adecuación digital se centrará en el impacto acumulativo de las normas digitales, con el fin de comprobar cómo contribuyen a la competitividad de la UE y en qué aspectos será necesario proponer nuevos ajustes en la segunda mitad del mandato legislativo.

La evaluación de la adecuación digital se pone en marcha al mismo tiempo que la propuesta Ómnibus, con una amplia consulta pública. La Comisión pretende involucrar a todas las partes interesadas y realizar una consulta amplia. El objetivo es realizar un seguimiento con una visión general y un amplio mapeo de cómo el conjunto de normas digitales cubre los sectores estratégicos de la industria de la UE, y abordar cómo 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.

La «prueba de resistencia» del acervo digital también continuará 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 prevé publicar en 2026 una revisión de la

[11] Según la propuesta separada

Ley de Mercados Digitales, del Programa Político de la Década Digital, la Ley de Chips, la Directiva sobre Servicios de Comunicación Audiovisual y una evaluación de la Directiva sobre Derechos de Autor. Para 2027, entre los actos que se prevé evaluar figuran, entre otros, la Ley de Ciber-Solidaridad, el Reglamento sobre Internet Abierto, la NIS2 y la Ley de Servicios Digitales. En 2028, la Comisión debería evaluar, por ejemplo, la Ley Europea de Libertad de los Medios de Comunicación y la Ley de Datos, seguida de una evaluación de la Ley de IA en 2029 y una evaluación de la cláusula de caducidad del Reglamento por el que se establece el Centro Europeo de Competencia en Ciberseguridad y la Red Europea de Ciberseguridad.

Las partes interesadas han subrayado en repetidas ocasiones que, en muchos casos, el esfuerzo de simplificación no consiste tanto en modificar las normas como en aclarar su aplicación. **La Comisión está dando prioridad a una serie de directrices** destinadas a apoyar la aplicación uniforme de las normas, sin perjuicio de las interpretaciones del Tribunal de Justicia.

En lo que respecta al marco regulador de los datos, la Comisión anunció su prioridad en la Estrategia de la Unión de Datos, centrándose en particular en las directrices sobre la compensación razonable para aclarar lo que se puede cobrar por el intercambio de datos, proporcionando seguridad jurídica tanto a los titulares de los datos como a los destinatarios de los mismos, y en las directrices para aclarar las definiciones.

Para apoyar la aplicación de la Ley de Inteligencia Artificial, la Comisión sigue dando prioridad a la publicación de directrices sobre varios aspectos, tal y como se detalla en la exposición de motivos de la propuesta de Directiva Ómnibus Digital que modifica la Ley de Inteligencia Artificial.

***Propuestas en la Directiva Ómnibus Digital***

**El «acervo legislativo en materia de datos»** se ha ampliado en los últimos años a una serie de reglamentos, lo que ha creado complejidad jurídica, incluyendo algunos solapamientos, definiciones que no están perfectamente alineadas y cuestiones sobre la interacción de los instrumentos. En particular, se adoptó el Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), diseñado para crear un mercado único de servicios en la nube. Ha sido sustituido parcialmente por el capítulo VI del Reglamento (UE) 2023/2854 (Ley de Datos), que establece obligaciones en materia de cambio entre servicios de tratamiento de datos.

Otro ejemplo es el capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), que complementa las normas sobre la reutilización de la información del sector público de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) para los datos que no pueden reutilizarse sin restricciones. Además, otros capítulos del Reglamento (UE) 2022/868 (Ley de gobernanza de datos) establecieron normas sobre los servicios de intermediación de datos, el altruismo de datos, 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 (Ley de Datos) estableció la obligación material de los fabricantes de dispositivos conectados y los proveedores de servicios relacionados de compartir datos con sus usuarios, o de las empresas de compartir datos con organismos gubernamentales, así como normas sobre contratos de intercambio justo de datos.

Para abordar esta cuestión, la Ley Ómnibus propone derogar las normas obsoletas, en particular las normas actuales del Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales, FFDR), 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 (Ley de Gobernanza de Datos, DGA), como las normas sobre altruismo de datos y servicios de intermediación de datos, con el fin de aumentar el atractivo de esos mecanismos de intercambio de datos. Al mismo tiempo, las normas de la Ley de gobernanza de datos sobre la reutilización de datos protegidos 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 reflejado en el Reglamento ( UE) 2023/2854 ( Reglamento sobre datos). Esta solución presenta

Numerosos beneficios para las administraciones públicas que poseen datos del sector público, así como para los reutilizadores, ya que pueden agilizar 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, de empresas designadas como guardianas, tal como se definen en el artículo 3 del Reglamento (UE) 2022/1925 (Ley de Mercados Digitales), que tienen un poder y una influencia significativos en el mercado interior. Para evitar que estas entidades 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 dichas entidades.

La propuesta incluye las normas consolidadas y simplificadas del Reglamento (UE) 2024/1689 (Reglamento sobre la libre circulación de datos), el Reglamento (UE) 2022/868 (Ley de gobernanza de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) en el Reglamento (UE) 2023/2854 (Ley de datos), creando un único instrumento consolidado para la economía de datos de Europa. Se derogan el Reglamento ( UE) 2024/1689 (Reglamento sobre la libre circulación de datos), la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) y el Reglamento (UE) 2022/868 (Ley de gobernanza de datos). Las normas de los cuatro instrumentos se armonizan y simplifican para mejorar la claridad y la coherencia, lo que aumenta su eficacia y ayuda a las empresas a impulsar la innovación. Esta iniciativa se ajusta a la Estrategia de la Unión de Datos, cuyo objetivo fundamental es impulsar la simplificación del marco legislativo.

Además, para ayudar aún más a las pequeñas empresas, las normas que facilitan el cumplimiento de la legislación de la UE en materia de datos para las pequeñas y medianas empresas (pymes) se amplían para incluir a las pequeñas empresas de mediana capitalización (PEMC). El Reglamento (UE) 2023/2854 (Ley de Datos), que entró en vigor el 12 de septiembre de 2025, supone un paso importante hacia una economía de datos justa y competitiva en la UE. Los cambios propuestos en esta propuesta no pretenden introducir modificaciones en los logros del Reglamento (UE) 2023/2854 (Ley 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 titulares de los datos, es necesario calibrar cuatro elementos clave. En concreto, es fundamental garantizar que el Reglamento (UE) 2023/2854 (Ley 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 salvaguardias contra el riesgo de fuga de secretos comerciales a terceros países en el contexto de las disposiciones obligatorias sobre intercambio de datos del IoT. En segundo lugar, el amplio alcance del marco entre empresas y gobiernos 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 dar lugar a incertidumbre jurídica. Por último, las disposiciones del Reglamento (UE) 2023/2854 (Ley de Datos) sobre el cambio entre servicios de tratamiento de datos siguen siendo pertinentes como contribución fundamental a un mercado de la nube más abierto y competitivo. No obstante, estas disposiciones no tenían suficientemente en cuenta la situación específica de los servicios que, para ser utilizables, están significativamente adaptados a las necesidades de un cliente o son prestados por pymes y microempresas. Las modificaciones contenidas en la presente propuesta mantendrán el objetivo de eliminar la dependencia de un proveedor, en particular los gastos de cambio y de salida, al tiempo que se reduce la carga administrativa de los proveedores de los servicios mencionados. Por lo tanto, la propuesta presenta modificaciones que mejoran la claridad jurídica y se ajustan en gran medida a los objetivos generales del Reglamento (UE) 2023/2854 (la Ley de Datos).

Además, con el fin de ayudar aún más a las pequeñas empresas, las normas que facilitan el cumplimiento del acervo de la UE en materia de datos para las pequeñas y medianas empresas (pymes) se amplían para incluir a las pequeñas empresas de mediana capitalización (PEMC).

**En lo que respecta 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, RGPD) entró en vigor el 25 de mayo de 2018, creando 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 quienes tratan datos personales. Si bien las partes interesadas consideran en general que el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) es equilibrado y sólido y sigue siendo adecuado para su finalidad, algunas entidades, especialmente las empresas más pequeñas y las asociaciones con un número reducido de operaciones de tratamiento de datos no intensivas y, a menudo, de bajo riesgo, han expresado su preocupación por 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 contenidas en la presente propuesta tienen por objeto abordar esas preocupaciones, en particular aclarando determinadas definiciones clave, como la noción de datos personales; facilitando el cumplimiento, por ejemplo, prestando apoyo a los responsables del tratamiento en lo que respecta a los criterios y 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 datos a las autoridades de control; y aclarando determinados aspectos del tratamiento de datos para la formación y el desarrollo de la inteligencia artificial. Las modificaciones propuestas también abordan la falta de claridad sobre las condiciones de la investigación científica, proporcionando una definición de investigación científica, aclarando además que el tratamiento posterior con fines científicos es compatible con la finalidad inicial del tratamiento y aclarando que la investigación científica constituye un interés legítimo. También se propone ampliar las excepciones a la obligación de informar sobre el tratamiento. Cuando procede, esta propuesta refleja los cambios introducidos en el Reglamento general de protección de datos por 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.

Además, hace tiempo que se necesita una solución normativa sobre la fatiga del consentimiento y la proliferación de los banners de cookies. La Directiva (UE) 2002/58/CE sobre la privacidad y las comunicaciones electrónicas («Directiva sobre la privacidad electrónica»), revisada por última vez en 2009, establece un marco para la protección de la confidencialidad de las comunicaciones y especifica el Reglamento (UE) 2016/679 («Reglamento general de protección de datos, RGPD») cuando el tratamiento de datos personales se produce 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 relacionada con ellos. Una parte esencial del uso de los equipos terminales, como los teléfonos y los ordenadores personales, es consumir contenidos y utilizar servicios en línea. Muchos de estos servicios en línea dependen de los ingresos procedentes de la publicidad, incluida la publicidad personalizada. Este es también el caso de los servicios de medios de comunicación. Los proveedores de servicios en línea dependen de las denominadas «cookies» o tecnologías similares que utilizan las capacidades de tratamiento y almacenamiento de los equipos terminales, accediendo así, por ejemplo, a la información almacenada en los equipos terminales o emitida por ellos. Esto se utiliza para diversos fines, como optimizar la prestación del servicio para un equipo terminal concreto, garantizar la seguridad del equipo terminal y del servicio en general, pero también para realizar un seguimiento del comportamiento de las personas y su interacción con diferentes servicios en línea con el fin de ofrecer publicidad personalizada.

Cuando el uso de estas tecnologías no sea necesario para el almacenamiento técnico o el acceso con el único fin de llevar a cabo o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o cuando sea estrictamente necesario para proporcionar una información

servicio social solicitado explícitamente por el suscriptor o usuario, la Directiva (UE) 2002/58/CE (la Directiva sobre privacidad electrónica) exige el consentimiento. Dicho consentimiento se solicita normalmente a través de banners emergentes que se muestran en el sitio web o en la aplicación móvil. Estos banners contienen información sobre los fines del tratamiento, a menudo vinculada a los tipos de cookies y a los destinatarios de los datos, y no siempre son fáciles de entender para las personas. Por estas razones, es posible que no logren su objetivo, que es informar a las personas y darles control sobre la protección de su privacidad y el tratamiento de sus datos personales, sino que, por el contrario, se perciban como una molestia para los usuarios de Internet. Al mismo tiempo, los proveedores de servicios en línea incurren en costes considerables para diseñar banners que cumplan con la normativa.

Aumentando la complejidad, el artículo 5, apartado 3, de la Directiva (UE) 2002/58/CE (Directiva sobre la privacidad electrónica) se aplica a la instalación de cookies o tecnologías similares para obtener información del equipo terminal de un usuario, mientras que el tratamiento posterior de los datos personales está sujeto al Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Si bien se requiere el consentimiento para garantizar el control 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 incertidumbre 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 privacidad electrónica y el Reglamento general de protección de datos ha dado lugar a que diferentes autoridades nacionales sean competentes para supervisar las normas de los dos marcos jurídicos.

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

Por último, la propuesta allana el camino para que las indicaciones de las elecciones individuales sean automáticas y legibles por máquina, y para que los proveedores de sitios web y aplicaciones móviles y los proveedores de aplicaciones para teléfonos móviles respeten dichas indicaciones una vez que se disponga de las normas. Esto se basa en la modificación de 2009 de la Directiva (UE) 2002/58/CE (Directiva sobre la privacidad electrónica) (véase el considerando 66 de la Directiva 2009/136/CE), que ya fomentaba la posibilidad de expresar el consentimiento del usuario mediante la configuración adecuada de un navegador u otra aplicación cuando fuera técnicamente posible y eficaz, y el artículo 21, apartado 5, del Reglamento (UE) 2016/679 (Reglamento general de protección de datos), así como la propuesta de la Comisión de 2017 sobre un Reglamento relativo a la privacidad y las comunicaciones electrónicas (COM(2017)10), que proponía la gestión de las opciones del usuario mediante la configuración del navegador web. Esto otorga a la Comisión el mandato de solicitar a los organismos de normalización que desarrollen un conjunto de normas para codificar las indicaciones automatizadas y legibles por máquina de las opciones de los interesados, así como la comunicación de dichas opciones desde los navegadores a los sitios web y desde las aplicaciones de telefonía móvil a los servicios web. Una vez que estas normas estén disponibles, y tras un período de gracia de seis meses, los responsables del tratamiento que utilicen sitios web y aplicaciones móviles para prestar sus servicios 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, se les aplicará una presunción de cumplimiento. Sobre esta base, se espera que los navegadores también desarrollen la configuración pertinente. Las disposiciones se formulan de manera tecnológicamente neutra, de modo que otras herramientas, como la IA agencial, también puedan ayudar a los usuarios a tomar decisiones de consentimiento, siempre que sean adecuadas para garantizar el cumplimiento de los requisitos del RGPD. Teniendo en cuenta la importancia de las fuentes de ingresos en línea

para el periodismo independiente como pilar indispensable de una sociedad democrática, los proveedores de servicios de medios de comunicación, tal como se definen en el Reglamento (UE) 2024/1083 (Ley Europea de Libertad de los Medios de Comunicación), no deberían estar obligados a respetar dichas señales, lo que les permitiría interactuar directamente con los usuarios para informarles y permitirles tomar sus decisiones 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 múltiples actos jurídicos.** Al fomentar el principio de «notificar una vez, compartir muchas veces», el punto de entrada único reducirá la carga administrativa de las entidades, al tiempo que garantizará un flujo eficaz y seguro de información sobre los incidentes de seguridad a los destinatarios definidos en la legislación correspondiente.

La propuesta establece la obligación de la ENISA de desarrollar el punto de entrada único, teniendo en cuenta la plataforma única de notificación de vulnerabilidades explotadas activamente e incidentes graves en virtud del Reglamento (UE) 2024/2847 (Ley de Ciberresiliencia (CRA)). Establece requisitos específicos para la herramienta, como conducto seguro de la información notificada por las entidades y enviada a las autoridades competentes. No modifica los requisitos jurídicos subyacentes para la notificación de incidentes, pero optimiza significativamente el flujo de trabajo y los recursos que se exigen a las entidades.

La propuesta también exige el uso del punto de entrada único para una serie de obligaciones de notificación de incidentes estrechamente interrelacionadas establecidas en la Directiva (UE) 2022/2555 (Directiva NIS2), el Reglamento (UE) 2016/679 (RGPD), el Reglamento (UE) 2022/2554 (DORA), el Reglamento (UE) 910/2014 (Reglamento eIDAS) y la Directiva (UE) 2022/2557 (Directiva CER). Otras obligaciones de notificación sectoriales, como las establecidas en el marco del código de red sobre aspectos de ciberseguridad de los flujos transfronterizos de electricidad (NCCS) y los instrumentos pertinentes para el sector de la aviación, también se incluirán en el punto de entrada único mediante modificaciones de los respectivos 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 comunicada mediante la introducción de habilitaciones para varios actos jurídicos, cuando estas no existan. La propuesta aclara que, al elaborar plantillas comunes de información para la Directiva (UE) 2022/2555, la Directiva (UE) 2022/2557 o el Reglamento (UE) 2016/679, con el fin de garantizar la coherencia, promover las sinergias y reducir la carga administrativa de las entidades minimizando el número de campos de datos que estas deben completar, la Comisión debe tener debidamente en cuenta la experiencia adquirida y las plantillas comunes elaboradas en virtud del Reglamento (UE) 2022/2554 (DORA).

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 la promoción de la equidad y la transparencia para los usuarios empresariales de servicios de intermediación en línea (el Reglamento sobre las relaciones entre plataformas y empresas o «Reglamento P2B»). El Reglamento está en vigor desde el 12 de julio de 2020 y supuso el primer paso hacia la creación de un marco jurídico completo para la economía de las plataformas. Desde su entrada en vigor, otros actos legislativos de la UE han regulado los servicios de intermediación en línea y las plataformas en línea. Entre ellos figuran el Reglamento (UE) 2022/1925 (la Ley de Mercados Digitales, DMA) y el Reglamento (UE) 2022/2065 (la Ley de Servicios Digitales, DSA), que en gran medida superan las disposiciones del Reglamento P2B. Se mantendrán determinadas disposiciones del Reglamento P2B con el fin de garantizar la seguridad jurídica de los actos que contienen referencias cruzadas a dichas disposiciones, por ejemplo, la Directiva (UE) 2023/2831 sobre la mejora de las condiciones de trabajo 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 superposición y el solapamiento de normas, tal y como han solicitado las partes interesadas. Los proveedores de servicios de intermediación en línea se beneficiarán de una mayor claridad de las disposiciones legales. La aplicación de la normativa será más específica.

- **Coherencia con las disposiciones políticas existentes en el ámbito político**

La propuesta va acompañada de una segunda propuesta por la que se modifica el Reglamento (UE) 2024/1689 (Ley de IA), que junto con la primera conforman el «Omnibus Digital» y marcan el primer paso inmediato hacia la simplificación del reglamento digital. Además del «Omnibus Digital», la propuesta de revisión del Reglamento (UE) 2019/881 (Ley de Ciberseguridad) incluirá, entre otras cosas, la actualización del mandato de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), así como medidas destinadas a simplificar el cumplimiento de los requisitos de ciberseguridad.

El «Digital Omnibus» forma parte de una estrategia más amplia de simplificación normativa anunciada a través del paquete digital, que se presenta con más detalle en la sección introductoria de la presente exposición de motivos.

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

La propuesta forma parte del programa 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 diferentes normas, incluso cuando se refieren a diferentes ámbitos políticos. Este es el caso, por ejemplo, de la solución de simplificación digital desarrollada en el marco del punto único de entrada para la notificación de incidentes, que no modifica las obligaciones reglamentarias subyacentes, pero reúne en una misma interfaz las normas de ciberseguridad que se aplican 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 114 y 16 del Tratado de Funcionamiento de la Unión Europea, que reflejan el fundamento jurídico de los actos modificados. El fundamento jurídico adecuado para las disposiciones que modifican el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el Reglamento (UE) 2018/1725 es el artículo 16 del Tratado. Dado que todos los demás actos modificados se basan en el artículo 114 del Tratado, la misma base jurídica también es adecuada para las disposiciones modificadoras correspondientes del presente Reglamento.

- **Subsidiariedad (para competencias no exclusivas)**

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 preservan la lógica de subsidiariedad que sustenta los actos modificados.

Por lo que se refiere al Reglamento (UE) 2023/2854 (Ley de Datos), las modificaciones refuerzan el objetivo del Reglamento de eliminar las barreras en el mercado único para la economía basada en datos. Lo hacen añadiendo al Reglamento las normas 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 en las competencias de los Estados miembros ni de las instituciones de la UE.

Lo mismo ocurre con 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 (Ley de Datos) sin modificar sustancialmente las competencias otorgadas a los Estados miembros. Una parte significativa de los datos del sector público ya está sujeta al Reglamento de Ejecución (UE) 2023/138 sobre conjuntos de datos de alto valor([12]) , que es directamente aplicable. La transformación en un reglamento facilitará la aplicación uniforme de los cambios propuestos en todos los Estados miembros. Apoyará en particular a las administraciones públicas que poseen datos del sector público, pero también a los reutilizadores de dichos datos, al racionalizar los procesos y reducir la carga administrativa asociada a la interpretación y aplicación de las diversas legislaciones nacionales. 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 proporcionar suficiente flexibilidad para las soluciones nacionales, una prerrogativa subrayada por los Estados miembros.

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 a la aplicación de las normas vigentes y reducir la carga administrativa, en la medida de lo posible, sin menoscabar el alto nivel de protección de datos previsto en el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el Reglamento (UE) 2018/1725. Del mismo modo, no modifican las competencias de los Estados miembros ni de los organismos e instituciones de la UE.

Con la introducción del punto único de entrada para la notificación de incidentes, se propone una solución a escala europea que permita canalizar las múltiples obligaciones legales impuestas a las empresas para notificar esencialmente el mismo incidente. La solución no altera en modo alguno los derechos y competencias de las autoridades nacionales para recibir dichas notificaciones. Por el contrario, incentiva la notificación al proporcionar un punto de entrada único en una interfaz fácil de usar para presentar aparentemente una sola notificación, al tiempo que se responde a múltiples obligaciones legales al mismo tiempo. Dado que muchos de los servicios en cuestión se prestan a nivel transfronterizo y los proveedores están presentes en varios Estados miembros, es necesaria una solución europea.

- **Proporcionalidad**

La propuesta incluye modificaciones técnicas necesarias para alcanzar los objetivos de reducir las cargas administrativas y proporcionar claridad normativa, al tiempo que se preservan y optimizan los objetivos subyacentes de la legislación modificada. Son proporcionadas, ya que imponen costes de transición y adaptación insignificantes, si es que los hay, a las empresas y las autoridades, pero facilitan un elevado ahorro de costes en los próximos años.

Varias de las modificaciones presentadas en el presente Reglamento persiguen el objetivo de simplificación, principalmente proporcionando seguridad jurídica y aclarando la aplicación de las normas, por ejemplo, en lo que se refiere a las aclaraciones para los titulares de datos sobre la protección de los secretos comerciales en el Reglamento (UE) 2023/2854 (Ley de Datos), o aclaraciones sobre el entrenamiento de modelos y sistemas 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 el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el Reglamento (UE) 2018/1725. Algunas de las disposiciones pretenden codificar las interpretaciones del Tribunal de Justicia de la Unión Europea, por ejemplo, en lo que respecta a

[12] Reglamento de Ejecución (UE) 2013/138.

La seudonimización de los datos personales se aclara aún más en el Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Como tal, incluye modificaciones muy específicas de las normas, al tiempo que se espera que tenga un gran impacto a la hora de proporcionar 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, observando que los mismos objetivos reglamentarios pueden alcanzarse con menores 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 (Ley de gobernanza de datos) se transforma en un régimen voluntario que fomenta la confianza en el Reglamento (UE) 2023/2854 (Ley de datos).

Con la ampliación a las pequeñas empresas de mediana capitalización de determinadas disposiciones aplicables a las pequeñas y medianas empresas, las medidas de simplificación son específicas y introducen cambios mínimos en el alcance de esas obligaciones, al tiempo que proporcionan seguridad jurídica a un abanico más amplio de empresas con un alto potencial para apoyar la competitividad de la UE. Las propuestas se limitan a los cambios necesarios para garantizar que las PYME se beneficien del mismo marco jurídico que las PYME.

El punto único de entrada para la notificación de incidentes y violaciones de datos supone un importante ahorro de costes para las empresas, al tiempo que aborda el problema generalizado de la falta de notificación. No solo es una solución proporcionada, sino que aporta una simplificación clave mediante una herramienta digital y refuerza la eficacia de las obligaciones de notificación cubiertas por el punto de entrada.

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

- **Elección del instrumento**

Las modificaciones se proponen mediante un Reglamento, dada la naturaleza de las normas modificadas. Cuando se modifican las Directivas, las disposiciones se dirigen a los organismos europeos o introducen modificaciones específicas, en particular para excluir disposiciones desarrolladas con mayor detalle en los Reglamentos.

## 3. RESULTADOS DE EVALUACIONES EVALUACIONES, CONSULTAS A LAS PARTES INTERESADAS Y EVALUACIONES DE IMPACTO

- **Evaluaciones a posteriori/controles de idoneidad de la legislación vigente**

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

Una excepción a esto es la revisión preliminar de 2023 del Reglamento (UE) 2019/1150 (el Reglamento sobre las relaciones entre plataformas y empresas (P2B)[13]. El informe observó efectos positivos iniciales cuando

[13] Documento de trabajo de los servicios de la Comisión, Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la primera

en materia de transparencia contractual para los usuarios empresariales y de garantías procesales en la tramitación de reclamaciones, por ejemplo. Sin embargo, el informe también puso de manifiesto que tanto los usuarios empresariales como los proveedores de servicios de intermediación en línea y los motores de búsqueda en línea desconocían sus respectivos derechos y obligaciones en virtud del Reglamento (UE) 2019/1150 (Reglamento P2B). A ello se sumó un cumplimiento insuficiente del Reglamento (UE) 2019/1150 (Reglamento P2B), lo que dio lugar a una falta de aplicación. Hasta 2023 se recibieron muy pocas reclamaciones en virtud del Reglamento (UE) 2019/1150 (Reglamento P2B). El informe concluía que «en la actualidad no se ha alcanzado todo el potencial del Reglamento (UE) 2019/1150 (Reglamento P2B)». Mientras tanto, el Reglamento (UE) 2022/2065 (DSA) y el Reglamento (UE) 2022/1925 (DMA) comenzaron a aplicarse plenamente y han superado en gran medida las disposiciones del Reglamento (UE) 2019/1150 (Reglamento P2B).

- **Consultas a las partes interesadas**

Se llevaron a cabo varias consultas durante la preparación de la propuesta. Cada una de ellas se concibió como complementaria a las demás, abordando diferentes aspectos temáticos o diferentes grupos de partes interesadas.

En la primavera de 2025 se publicaron tres consultas públicas y convocatorias de presentación de pruebas sobre los pilares fundamentales de la propuesta. Se llevó a cabo una consulta sobre la estrategia «Apply AI» del 9 de abril al 4 de junio[14] otra sobre la revisión del Reglamento (UE) 2019/881 (Ley de Ciberseguridad) del 11 de abril al 20 de junio[15] y, por último, otra sobre la estrategia de la Unión Europea de Datos del 23 de mayo al 20 de julio[16] . Cada cuestionario tenía una sección específica (o, en ocasiones, varias) dedicada a las preocupaciones sobre la aplicación y la simplificación, directamente relacionada con las reflexiones sobre el Omnibus Digital. En total, se obtuvieron 718 respuestas únicas como parte de esta primera ronda de consultas.

Entre el 16 de septiembre y el 14 de octubre de 2025[17] se publicó una convocatoria de presentación de pruebas sobre el Omnibus Digital. Su objetivo era dar a las partes interesadas la oportunidad de comentar una propuesta consolidada sobre el alcance del Omnibus Digital. Se recibieron 513 respuestas, presentadas por diversos grupos de interesados, entre los que destacaban empresas y asociaciones empresariales, la sociedad civil, el mundo académico y las autoridades, así como contribuciones individuales de ciudadanos.

La vicepresidenta ejecutiva Henna Virkkunen organizó dos diálogos de aplicación sobre los temas clave abordados en el paquete de medidas digitales: el primero sobre la política de datos [18] (1 de julio de 2025) y el segundo sobre la política de ciberseguridad [19] (15 de septiembre).

---

Revisión preliminar sobre 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 {SWD(2023) 300 final}

14 Comisión Europea (2025) *Convocatoria de presentación de pruebas sobre la estrategia «Apply AI»*. Disponible en: Estrategia «Apply AI»: reforzar el continente de la IA

15 Comisión Europea (2025) *Convocatoria de presentación de pruebas sobre la revisión de la Ley de Ciberseguridad.* Disponible en: La Ley de Ciberseguridad de la UE

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

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

18 Comisión Europea (2025) *Diálogo sobre la aplicación: política de datos*. Disponible en: Diálogo sobre la aplicación: política de datos - Comisión Europea

El comisario McGrath organizó un diálogo sobre la aplicación del RGPD (16 de julio de 2025).

Los servicios de la Comisión también llevaron a cabo varias «comprobaciones de la realidad»: grupos de discusión 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 los retos prácticos de aplicación que se plantean en el día a día y estimar los costes de cumplimiento.

Con el fin de consultar específicamente a las pequeñas y medianas empresas (pymes) y recabar sus opiniones, se organizó un panel específico para pymes a través de la Red Europea de Empresas (EEN)[20] entre el 4 de septiembre y el 16 de octubre de 2025.

Por último, los servicios de la Comisión recibieron numerosos documentos de posición 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 opiniones de las partes interesadas coincidieron en la necesidad de simplificar la aplicación de algunas de las normas digitales. Las partes interesadas acogieron con satisfacción el énfasis en la coherencia y la consolidación de las normas, así como en la optimización de los costes de cumplimiento.

Hubo una clara petición de racionalizar el acervo en materia de datos y consolidar las normas. Esto se aborda en la propuesta, junto con modificaciones específicas respaldadas por las partes interesadas, entre otras cosas en lo que respecta al Reglamento general de protección de datos y la fatiga generada por los banners de cookies. Además, las empresas han señalado la necesidad de realizar nuevas evaluaciones de la interacción entre las normas sobre datos que merecen un análisis más profundo mediante las herramientas de mejora de la reglamentación, en particular la próxima evaluación de la 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. Esta petición de actuación se aborda mediante la propuesta de un punto único de entrada para la notificación de incidentes.

En lo que respecta a la Ley de Inteligencia Artificial, las partes interesadas han señalado la necesidad de seguridad jurídica en la aplicación de las normas y han destacado, en particular, la necesidad de disponer de normas y orientaciones antes de aplicar las normas. La propuesta reglamentaria separada en el marco del Omnibus Digital responde a sus preocupaciones.

Por último, las partes interesadas no se han pronunciado sobre el impacto 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 muy 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 normas más recientes.

En el documento de trabajo de los servicios de la Comisión que acompaña al paquete Digital Omnibus se ofrece una descripción detallada de estas consultas a las partes interesadas y de cómo se han reflejado en la propuesta.

---

[19] Comisión Europea (2025) *Diálogo sobre la aplicación de la política de ciberseguridad con la vicepresidenta ejecutiva Henna Virkkunen*. Disponible en: Diálogo sobre la aplicación de la política de ciberseguridad con la vicepresidenta ejecutiva Henna Virkkunen - Comisión Europea

[20] La EEN es la mayor red de apoyo a las pequeñas y medianas empresas del mundo, y está gestionada por el Consejo Europeo de Innovación y la Agencia Ejecutiva para las Pymes (EISMEA) de la Comisión Europea.

- **Recopilación y uso de conocimientos especializados**

Además de las consultas mencionadas anteriormente, la Comisión se basó principalmente en análisis internos para elaborar la presente propuesta. También se encargaron dos estudios para respaldar el análisis de los capítulos de la propuesta relativos a los datos. El primero 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 (Ley de gobernanza de datos). El segundo estudio, más estrechamente vinculado a la Comunicación sobre la estrategia de la Unión de Datos (adoptada como parte del mismo paquete de simplificación junto con la Directiva Ómnibus Digital), se centró en la evolución de las políticas de datos relacionadas con la IA generativa, el cumplimiento normativo y las dimensiones internacionales. Ambos estudios se están ultimando y se publicarán en una fase posterior.

Los servicios de la Comisión también han realizado un estudio sobre la interacción entre el Reglamento (UE) 2022/2065 (Ley de Servicios Digitales) y otros actos legislativos, incluido 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 (Ley de Servicios Digitales) y otras normas relacionadas, de conformidad con el requisito del artículo 91 del Reglamento (UE) 2022/2065 (Ley de Servicios Digitales).

- **Evaluación de impacto**

Las modificaciones propuestas en el presente Reglamento son específicas y de carácter técnico. Su objetivo es garantizar una aplicación más eficaz de las normas. No se prestan a múltiples opciones políticas que puedan someterse a pruebas y comparaciones significativas y, de conformidad con las directrices para la mejora de la reglamentación, no se basan en un informe completo de evaluación de impacto.

El documento de trabajo adjunto profundiza en la lógica de intervención de las modificaciones, las opiniones de las partes interesadas sobre las diferentes medidas y presenta el análisis de la relación coste-beneficio de las propuestas, incluidos los ahorros de costes generados y otros tipos de repercusiones. En muchos casos, se basa en las respectivas evaluaciones de impacto que se realizaron originalmente para los diferentes actos.

- **Adecuación y simplificación normativa**

El Reglamento propuesto supone una reducción muy importante de la carga para las empresas, así como para las administraciones públicas y los ciudadanos. Las estimaciones iniciales prevén un ahorro posible de al menos 1 000 millones de euros anuales, desde el momento de su entrada en vigor, con un ahorro adicional de 1 000 millones de euros en costes puntuales, lo que supone un total de al menos 5 000 millones de euros en tres años hasta 2029. También se esperan en gran medida beneficios no cuantificables, en particular gracias a un conjunto de normas simplificadas que facilitarán su aplicación y cumplimiento. Los cálculos tampoco incluyen las oportunidades comerciales creadas por el enfoque normativo propuesto.

Si bien las pymes ya están exentas en virtud de determinadas disposiciones de los actos jurídicos modificados en la Directiva Digital Omnibus, se proponen nuevas medidas de apoyo en el ámbito del cambio de nube. En el capítulo sobre normas armonizadas de intercambio de datos, algunas exenciones ya previstas para las pymes se amplían a las pequeñas empresas de mediana capitalización (SMC).

La propuesta también es plenamente coherente con la «verificación digital» de la Comisión, cuyo objetivo es garantizar la adecuada adaptación de las propuestas políticas a los entornos digitales. Para más detalles al respecto, véase el capítulo 4 de la Declaración Legislativa y Financiera Digital adjunta.

- **Derechos fundamentales**

Las modificaciones propuestas apoyan las oportunidades de innovación para las empresas en el mercado único y, por lo tanto, promueven el derecho a ejercer una actividad empresarial 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 a la protección de los datos personales, y se han calibrado para preservar el más alto nivel de protección y ayudar a las personas a ejercer eficazmente sus derechos, al tiempo que se optimizan los costes y se crean nuevas oportunidades de innovación. De este modo, la propuesta sigue estrictamente el principio de proporcionalidad consagrado en el artículo 52 de la Carta.

En el caso concreto de las modificaciones específicas del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y del Reglamento (UE) 2018/1725, las modificaciones propuestas simplificarían los requisitos para el tratamiento de bajo riesgo, armonizarían determinadas normas y aclararían algunos conceptos clave del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el 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 datos personales son más críticas.

En lo que respecta a la privacidad de las comunicaciones, la propuesta mantiene el nivel más alto de protección, incluido el acceso basado en el consentimiento a los equipos terminales. La modificación de la Directiva (UE) 2002/58/CE (Directiva sobre la privacidad electrónica) no altera las protecciones sustantivas. Armoniza las normas para el tratamiento de datos personales en y desde equipos terminales con las del Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Se mantienen las normas sobre la integridad de los equipos terminales en virtud de la Directiva cuando se tratan datos no personales.

## 4. REPERCUSIONES PRESUPUESTARIAS

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

## 5. OTROS ELEMENTOS

- **Planes de aplicación y disposiciones de seguimiento, evaluación y presentación de informes**

N.A.

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

***Modificaciones del Reglamento (UE) 2023/2854 — Ley de Datos***

Las modificaciones del marco jurídico en materia de datos consolidan en el Reglamento (UE) 2023/2854 (Ley de Datos) de manera sólida y racionalizada las disposiciones del Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos), el Reglamento (UE) 2022/868 (Ley de gobernanza 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 (Ley de Datos).

El artículo 1 recoge las modificaciones del Reglamento (UE) 2023/2854 (Ley de Datos) sobre normas armonizadas en materia de acceso y uso equitativos de los datos 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 (Ley de Datos), en el que se insertarán nuevos capítulos, tal y como se explica más adelante.

El apartado 2 modifica las definiciones e inserta otras nuevas.

El apartado 3 crea una nueva norma en virtud del artículo 4, apartado 8, del Reglamento (UE) 2023/2854 (Ley de Datos) que permite a los titulares de datos negarse a revelar secretos comerciales a un usuario cuando exista un alto riesgo de adquisición, uso o divulgación ilícitos a terceros países, o a entidades bajo su control, que estén sujetos 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 (Ley de Datos), relativo a la divulgación de secretos comerciales a terceros por parte de los titulares de datos.

Los apartados 5 a 19 reducen el ámbito de aplicación del capítulo V de «necesidades excepcionales» a «emergencias públicas». Se suprimen los artículos 14 y 15 y se crea un nuevo artículo 15 bis, que se convierte en el único artículo para solicitar durante emergencias públicas en el marco del régimen B2G del Reglamento (UE) 2023/2854 (Ley 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 de una emergencia pública (artículo 15 bis, apartado 3). Las referencias cruzadas se ajustan en consecuencia y se simplifica y aclara el lenguaje. El artículo 1, apartado 21, crea un nuevo artículo 22 bis que enmarca el régimen de reclamaciones en virtud del capítulo V, fusionando disposiciones que antes se repetían.

Los apartados 20 a 22 incluyen determinadas exenciones al capítulo VI del Reglamento (UE) 2023/2854 (Ley de Datos) (cambio entre servicios de tratamiento de datos): En el artículo 31 se introduce un régimen específico más flexible para los servicios de tratamiento de datos personalizados, es decir, los servicios de tratamiento de datos que no son estándar y que no funcionarían sin una adaptación previa a las necesidades y al ecosistema del usuario, cuando se presten en virtud de contratos celebrados antes del 12 de septiembre de 2025. Del mismo modo, en el artículo 31 se introduce un nuevo régimen específico más flexible para los servicios de tratamiento de datos prestados por pymes y microempresas sobre la base de contratos celebrados antes del 12 de septiembre de 2025, acompañado de una aclaración de que estos proveedores pueden incluir penalizaciones por rescisión anticipada en los contratos de duración determinada.

Los apartados 23 a 25 incluyen modificaciones del artículo 32 del Reglamento (UE) 2023/2854 (Ley de Datos) como consecuencia de la integración de los organismos que actualmente se rigen por el Reglamento (UE) 2022/868 (Ley de Gobernanza de Datos) en el Reglamento (UE) 2023/2854 (Ley de Datos).

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

El apartado 27 integra dos regímenes jurídicos que figuran actualmente en el Reglamento (UE) 2022/868 (Ley de gobernanza de datos), que quedará derogado una vez que entre en vigor la Ley Ómnibus. Este punto reforma las normas actuales de los capítulos III y IV de la Ley de gobernanza de datos, que establecen un régimen de notificación obligatoria para los proveedores de servicios de intermediación de datos y un régimen de registro voluntario para las organizaciones de altruismo de datos. Los dos regímenes se insertarán como nuevo capítulo VII bis en el Reglamento (UE) 2023/2854 (Ley de Datos). A la luz del carácter emergente del mercado de los servicios de intermediación de datos, las obligaciones del Reglamento (UE) 2022/868 (Ley de Gobernanza de Datos) se flexibilizarán para que este mercado pueda crecer: 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 importante, la de mantener los servicios de intermediación de datos legalmente separados de cualquier otro servicio que una empresa pueda querer ofrecer, se sustituirá por la obligación de

mantener los servicios funcionalmente separados, junto con un conjunto adicional de condiciones. Por último, se reduce drásticamente la lista de obligaciones. En lo que respecta al altruismo de datos, se suprimen las obligaciones de información y transparencia para las organizaciones de altruismo de datos, así como la idea de complementar las normas del Reglamento (UE) 2022/868 (Ley de gobernanza de datos) con un «código de altruismo de datos» con normas aún más detalladas.

Se introduce un nuevo capítulo VIIb en virtud del cual la prohibición de los requisitos de localización de los datos no personales dentro de la Unión, que figuraba anteriormente en el Reglamento (UE) 2018/1807 (Reglamento sobre la libre circulación de datos no personales), que va a ser derogado, se inserta en el Reglamento (UE) 2023/2854 (Ley de Datos). Se mantiene la obligación de notificar a la Comisión, pero se suprime el punto único de información en línea nacional 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 fusionadas sobre la reutilización de datos y documentos en poder de organismos del sector público en virtud del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos):

- El punto 4 introduce las definiciones de las disposiciones insertadas en el Reglamento (UE) 2023/2854 (Ley de Datos), armonizando la definición de datos y documentos mediante una delimitación estricta entre contenido digital (datos) y no digital (documentos).
- Introduce el nuevo capítulo VIIc sobre la reutilización de datos y documentos en poder de organismos del sector público.
- Introduce una nueva sección 1, en la que se establecen los principios generales aplicables al capítulo recién insertado.
- Introduce el objeto y el ámbito de aplicación del capítulo fusionado, combinando las normas comunes del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Establece el principio común de no discriminación aplicable al intercambio de datos gubernamentales abiertos y determinadas categorías de datos protegidos.
- Establece la prohibición de acuerdos exclusivos, común al régimen de datos abiertos del gobierno y a determinadas categorías de datos protegidos.
- Establece los principios generales relativos a la tarificación por la reutilización de datos abiertos del gobierno o de determinadas categorías de datos protegidos. Como nueva norma, los organismos del sector público deberán garantizar que cualquier tasa pueda pagarse también en línea a través de servicios de pago transfronterizos ampliamente disponibles, sin discriminación por la reutilización de datos abiertos del gobierno. Esto supone una ampliación de esta norma, que anteriormente solo se aplicaba a la reutilización de determinadas categorías de datos protegidos en virtud del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos).
- Establece el derecho de los reutilizadores de datos abiertos del gobierno y de determinadas categorías de datos protegidos a ser informados de los medios de recurso disponibles en relación con las decisiones o prácticas que les afecten.
- Inserta la sección sobre las normas para la reutilización de datos abiertos del gobierno, anteriormente las normas de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).

- Determina el ámbito de aplicación de la sección, incluida la no aplicación a determinadas categorías de datos protegidos en el ámbito 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 datos abiertos del sector público.
- Establece las normas para la tramitación de las solicitudes de reutilización de datos abiertos del sector público, insertando la antigua disposición de la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Introduce las normas sobre los formatos disponibles para la reutilización de datos abiertos del sector público, anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos).
- Introduce las normas que regulan la tarificación de los datos públicos abiertos, anteriormente regulados por la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos). Como nueva norma, los organismos del sector público podrán aplicar tarifas más elevadas por la reutilización por parte de grandes empresas. Dichas tarifas deberán ser proporcionadas y su importe deberá basarse en criterios objetivos.
- Introduce las normas sobre licencias estándar para la reutilización de datos abiertos del sector público, anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos). Como nueva norma, los organismos del sector público pueden prever condiciones especiales para las empresas de gran tamaño. Dichas condiciones deben ser proporcionadas y basarse en criterios objetivos.
- Introduce las normas sobre disposiciones prácticas anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos), con el fin de facilitar la búsqueda de datos o documentos disponibles para su reutilización en el Reglamento (UE) 2023/2854 (Ley de Datos).
- Introduce las normas sobre datos de investigación que figuraban anteriormente en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) en el Reglamento (UE) 2023/2854 (Ley de Datos).
- Introduce las normas sobre conjuntos de datos de alto valor, anteriormente incluidas en la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos), en el Reglamento (UE) 2023/2854 (Ley de Datos).
- Crea una nueva sección para la reutilización de determinadas categorías de datos protegidos con el fin de incluir en el capítulo las antiguas normas del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos). El punto describe el ámbito de aplicación de esta tercera sección, que excluye del ámbito de aplicación los datos y documentos incluidos en el ámbito de aplicación de la sección dos, que regula el régimen de reutilización de los datos abiertos del gobierno. 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. Se trata del principio establecido en el capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza 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, anteriormente incluidas en el capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), de forma simplificada y racionalizada. Incluye una aclaración sobre las normas aplicables en los casos en que los datos personales hayan sido anonimizados. Se mantienen los requisitos relativos a las transferencias de datos no personales a terceros países, pero se dividen en un nuevo artículo en el punto 54.
- Introduce las normas sobre el cobro de tasas, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), en el Reglamento (UE) 2023/2854 (Ley de datos). Como nueva norma, los organismos del sector público pueden prever tasas más elevadas para la reutilización por parte de grandes empresas.

grandes empresas. Dichas tasas deben ser proporcionadas y basarse en criterios objetivos. La consideración especial para incentivar la reutilización por parte de las pymes se amplía a las PYME.

- Se introducen las normas sobre organismos competentes, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), en el Reglamento (UE) 2023/2854 (Ley de datos). Los organismos competentes tienen por objeto ayudar a los organismos del sector público a responder a las solicitudes de reutilización de los datos y documentos contemplados en la sección 3.

- Introduce las normas sobre el punto único de información, que anteriormente formaban parte del capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), en el Reglamento (UE) 2023/2854 (Ley 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.

- Introduce las normas sobre el procedimiento de solicitud de reutilización de determinadas categorías de datos protegidos, anteriormente reguladas en el capítulo II del Reglamento (UE) 2022/868 (Ley de gobernanza de datos), en el Reglamento (UE) 2023/2854 (Ley de datos).

El apartado 57 integra las normas básicas sobre el Comité Europeo de Innovación en materia de Datos (EDIB), un grupo que asesora a la Comisión sobre la aplicación coherente de la Ley de Datos y que sirve de foro de coordinación para la elaboración de políticas en el ámbito de la economía de los datos. Integrará las normas básicas en la Ley de Datos. Los cambios permitirán a la Comisión modificar los documentos fundamentales pertinentes del EDIB (Decisión de la Comisión de 20 de febrero de 2023 - C(2023)1074 final) y ampliar la composición del mismo a representantes de la elaboración de políticas nacionales, además de las autoridades competentes.

Los apartados 61 a 65 contienen modificaciones de las disposiciones del Reglamento (UE) 2023/2854 (Ley de Datos) sobre el procedimiento del Comité y la facultad de delegación, y el apartado 66 sobre el Reglamento (UE) 2022/868 (Ley de gobernanza de datos) necesarias para introducir las normas del Reglamento (UE) 2022/868 (Ley de gobernanza de datos) y la Directiva (UE) 2019/1024 (Directiva sobre datos abiertos) en el Reglamento (UE) 2023/2854 (Ley de datos).

El apartado 68 amplía la atención especial prestada a las pymes en el contexto de la evaluación a las microempresas y el punto 69 introduce la evaluación de las normas recién incorporadas al Reglamento (UE) 2023/2854 (Ley de Datos).

**El artículo 2** introduce en el Reglamento (UE) 2018/174 las referencias pertinentes a los servicios de intermediación de datos y al altruismo de datos en el anexo relativo a «la creación, renovación y cierre de una empresa».

***Modificaciones del Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 y la Directiva 2002/58/CE***

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

**En el artículo 3:**

El apartado 1 aclararía la definición de datos personales del artículo 4 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) al establecer que la información no se considerará datos personales para una entidad determinada cuando esta no disponga de medios razonablemente susceptibles de utilizarse 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 exención a la prohibición general del tratamiento de datos biométricos, cuando sea necesario para confirmar la identidad del interesado y cuando los datos y los medios para dicha verificación estén bajo el control exclusivo de dicho interesado. También establecería una exención para el tratamiento residual de categorías especiales de datos personales para el desarrollo y funcionamiento de un sistema de IA o un modelo de IA, con sujeción a determinadas condiciones, entre ellas la adopción de medidas organizativas y técnicas adecuadas para evitar la recogida de categorías especiales de datos personales y la supresión de dichos datos.

El apartado 3 aclararía la situación prevista en el artículo 12 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) en la que los interesados abusan del derecho de acceso con fines distintos de la protección de sus datos personales. En consecuencia, el responsable del tratamiento podría negarse a atender la solicitud o cobrar una tarifa 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 (Reglamento general de protección de datos), suprimiendo esta obligación en situaciones en las que existan motivos razonables para suponer que el interesado ya dispone de la información, a menos que el responsable del tratamiento transmita los datos a otros destinatarios o categorías de destinatarios, transfiera los datos a un tercer país, lleve a cabo una toma de decisiones automatizada o el tratamiento pueda suponer un alto riesgo para los derechos del interesado.

El apartado 5 aclararía los requisitos para la toma de decisiones individuales automatizadas con arreglo al artículo 22 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos), en el contexto de la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, en particular que el requisito de «necesidad» es independiente de si la decisión podría tomarse por medios distintos de los exclusivamente automatizados.

El apartado 6 armonizaría la obligación del responsable del tratamiento de notificar las violaciones de datos a la autoridad de control competente con arreglo al artículo 33 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos) con su obligación de notificar dichas violaciones a los interesados, al estipular que la notificación solo es necesaria si la violación de datos puede suponer un alto riesgo para los derechos del interesado. También ampliaría el plazo de notificación a 96 horas. Se propone asimismo que los responsables del tratamiento utilicen el punto de entrada único cuando notifiquen las violaciones de datos a la autoridad de control. Además, el Comité Europeo de Protección de Datos estaría obligado a elaborar y presentar a la Comisión una propuesta de modelo común para las notificaciones de violaciones de datos, que la Comisión estaría facultada para adoptar mediante un acto de ejecución, tras examinarlo, según sea 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, al disponer que se facilite a escala de la UE una lista única de operaciones de tratamiento que requieren y no requieren una evaluación de impacto relativa a la protección de datos, contribuyendo así a la armonización del concepto de alto riesgo. El Comité Europeo de Protección de Datos estaría obligado a elaborar propuestas para dichas listas. También estaría obligado a elaborar una propuesta de modelo común y una metodología común para realizar evaluaciones de impacto relativas a la protección de datos, que la Comisión estaría facultada para adoptar mediante un acto de ejecución, tras revisarlas, según sea necesario.

El apartado 8 establece que la Comisión, junto con el Comité Europeo de Protección de Datos, puede ayudar a los responsables del tratamiento a evaluar si los datos resultantes de la seudonimización no constituyen datos personales, especificando los medios y criterios pertinentes para dicha evaluación, incluido el estado actual de las técnicas disponibles y los criterios para evaluar el riesgo de reidentificación...

El apartado 12 reforma el régimen jurídico relativo al tratamiento de datos personales en o desde equipos terminales («dispositivos conectados»), que actualmente forma parte de la Directiva 2002/58/CE (Directiva sobre privacidad electrónica). Se inserta un nuevo artículo 88 bis en el Reglamento (UE) 2016/679 (Reglamento general de protección de datos), que establece el requisito del consentimiento para el almacenamiento o el acceso a datos personales en los equipos terminales de personas físicas y que incluye el tratamiento de datos personales en y desde equipos terminales en el ámbito de aplicación del Reglamento (UE) 2016/679 (Reglamento general de protección de datos). Se ha añadido un nuevo artículo 88 ter al Reglamento (UE) 2016/679 (Reglamento general de protección de datos), relativo a las indicaciones automatizadas y legibles por máquina de las elecciones individuales y al respeto de dichas indicaciones por parte de los proveedores de sitios web una vez que se disponga de normas.

**En el artículo 4:**

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

**En el artículo 5:**

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

***Punto único de entrada para la notificación de incidentes***

**En el artículo 6**:

En los apartados 1 y 2, se establece el punto único de entrada para la notificación de incidentes, incluyendo requisitos específicos para la ENISA. Además, se establece que la notificación de incidentes exigida por la Directiva NIS2 debe realizarse a través del nuevo punto único de entrada.

**En el artículo 7**: el punto de entrada único también es obligatorio para la notificación de incidentes en virtud del Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).

**En el artículo 8:** el punto de entrada único también es obligatorio para el Reglamento (UE) 2022/2554 (DORA).

**En el artículo 9**: el punto de entrada único también es obligatorio para la Directiva (UE) 2022/2557 (CER).

Además, en el artículo 3, apartado 6, se establece que la notificación de incidentes de violación de datos también es obligatoria para el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y debe canalizarse a través del punto de entrada único. En el artículo 5, apartado 1, se derogan los requisitos de notificación previstos en la Directiva 2002/58/CE (Directiva sobre la privacidad electrónica), ya que han quedado obsoletos a la luz de las disposiciones del Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

***Derogaciones de actos y disposiciones finales***

**En el artículo 10**:

El apartado 1 deroga el Reglamento (UE) 2019/1150 (Reglamento P2B), considerado de relevancia residual a la luz de las recientes normas que cubren en gran medida las mismas cuestiones. No obstante, el apartado 2 aborda las referencias cruzadas al Reglamento (UE) 2019/1150 (Reglamento P2B)

en otros instrumentos jurídicos: estas seguirán aplicándose hasta que se modifiquen en sus actos originales, a más tardar el 31 de diciembre de 2032, con el fin de evitar cualquier incertidumbre jurídica.

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

**El artículo 11** establece las disposiciones finales del Reglamento modificativo.

2025/0360 (COD)

Propuesta de

**REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

**por el que se modifican los Reglamentos (UE) 2016/1679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854, (UE) 2024/1689 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 por el que se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 y la Directiva (UE) 2019/1024 (Omnibus 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,

Tras la transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[21] , Visto el dictamen del Banco Central Europeo[22] ,

Visto el dictamen del Comité de las Regiones[23] , De conformidad con el procedimiento legislativo ordinario, Considerando lo siguiente:

(1) En su Comunicación titulada «Una Europa más simple y más rápida»[24] , la Comisión anunció su compromiso con un ambicioso programa destinado a promover políticas innovadoras y con visión de futuro que refuercen la competitividad de la Unión y aligeren radicalmente la carga normativa para los ciudadanos, las empresas y las administraciones, manteniendo al mismo tiempo el más alto nivel en la promoción de los valores de la Unión. En consecuencia, la Comisión dio prioridad a la propuesta de ajustes inmediatos de la legislación, incluida la legislación digital, para hacer frente al reto de la competitividad de la Unión.

(2) La legislación digital de la Unión establece un alto nivel en la Unión y puede ser una poderosa fuente de ventaja competitiva para las empresas que cumplen las normas, mostrando al mundo

---

[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, «Una Europa más sencilla y rápida: Comunicación sobre la aplicación y la simplificación», COM(2025)47 final, de 11 de febrero de 2025

marca líder de calidad, seguridad y fiabilidad. La normativa digital ha establecido unas reglas de juego claras en la Unión para las empresas responsables, garantizando la equidad y la transparencia en las relaciones entre empresas, estimulando modelos de negocio innovadores, estableciendo un alto nivel de protección y seguridad de los consumidores y protegiendo 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 a la rápida expansión de las tecnologías digitales en la economía y la dinámica social de la Unión, y con el fin de abordar los nuevos retos y promover las oportunidades empresariales en la UE. A pesar del compromiso de la Comisión de realizar 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 la próxima verificación de la adecuación digital, así como otras evaluaciones específicas de las normas digitales, es necesario introducir cambios normativos inmediatos. Por consiguiente, el presente Reglamento propone una primera serie de modificaciones del marco legislativo digital, con el fin de aportar aclaraciones normativas inmediatas que estimulen la innovación en el mercado de la Unión y reduzcan los costes administrativos de cumplimiento, en particular para las empresas, al tiempo que se racionalizan los costes administrativos y de supervisión para las autoridades de supervisión y los órganos consultivos. Las modificaciones también pretenden aportar claridad a los particulares.

(4) Dado el papel fundamental que desempeñan los datos en la creación de valor en la economía digital, y de conformidad con los objetivos de la Comunicación sobre una estrategia para una Unión Europea de los Datos, las modificaciones presentadas en el presente Reglamento al marco legislativo relativo a los datos tienen por objeto crear un marco regulador coherente y cohesionado para la disponibilidad y el uso de los datos, racionalizando y consolidando el marco regulador de los datos en solo dos actos jurídicos, a saber, los Reglamentos (UE) 2016/679[25]y (UE) 2023/2854(26)del Parlamento Europeo y del Consejo, frente a los cinco actos aplicables actualmente. Las modificaciones tienen por objeto reducir los costes administrativos innecesarios y estimular la disponibilidad de datos como requisito previo para apoyar a las empresas digitales competitivas en la Unión, manteniendo al mismo tiempo el más alto nivel de protección de la privacidad, la protección de los datos personales y las prácticas comerciales leales, y garantizando los objetivos reglamentarios fundamentales, incluido el cumplimiento de la legislación de la Unión y nacional en materia de competencia.

(5) Reconociendo la evolución iterativa de las normas horizontales y sectoriales, es indispensable abordar también los solapamientos en disposiciones específicas que dan lugar a duplicaciones innecesarias de las cargas administrativas. Este es el caso de los requisitos establecidos en varias normas para la notificación de incidentes de ciberseguridad y otros incidentes relacionados, en los que las soluciones digitales, tal como se proponen en el presente Reglamento, pueden suponer un alivio inmediato para 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

---

[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 Diciembre de 2023 sobre normas armonizadas relativas al acceso y uso equitativos de los datos y por el que se modifica el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Ley de Datos)

anteriores, que quedan 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 Consejo[27] ha establecido normas para las funciones de intermediación en tres contextos diferentes: a) funciones que apoyan la reutilización de datos protegidos en poder de organismos del sector público en condiciones controladas; b) servicios de intermediación de datos que facilitan el intercambio de datos entre los interesados, los titulares de los datos y los usuarios de los datos; y c) organizaciones de altruismo de datos que apoyan el uso de los datos puestos a disposición por los interesados y los titulares de los datos con fines altruistas o filantrópicos. Las funciones que apoyan 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 Consejo([28]). Su interacción ha causado confusión, especialmente entre los organismos del sector público. Por lo tanto, es necesario fusionar los dos conjuntos de normas. La evaluación de las normas sobre los servicios de intermediación de datos ha puesto de manifiesto que la definición de los proveedores de servicios de intermediación de datos adolece de deficiencias y que las normas son demasiado estrictas para que los proveedores de servicios puedan encontrar un modelo financiero sostenible. Por lo tanto, también es necesario racionalizar el régimen. En lo que respecta al altruismo en materia de datos, determinadas normas del Reglamento (UE) 2022/868, en particular la obligación de los Estados miembros de disponer de políticas nacionales sobre altruismo en materia de datos, el establecimiento de un «código normativo» y la elaboración de un formulario europeo de consentimiento para el altruismo en materia de datos, parecen regulaciones innecesarias, 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 Consejo([29]) sobre las directrices relativas al tratamiento de datos personales en el contexto de la investigación científica.

(8) Si bien se reconoce la importancia de los servicios de intermediación de datos en el contexto de numerosas iniciativas que apoyan el intercambio de datos y la colaboración, deben aclararse las normas del Reglamento (UE) 2022/868 sobre los proveedores de servicios de intermediación de datos. En particular, debe precisarse la definición de dichos proveedores. Deben eliminarse los elementos que servían meramente como ejemplos ilustrativos, en lugar de excepciones. Además, deben subsanarse las lagunas derivadas de formulaciones ambiguas, en particular en lo que respecta al concepto de «grupo cerrado». Los servicios no deben poder registrarse como servicios de intermediación de datos cuando sean utilizados exclusivamente por un grupo cerrado de empresas y cuando cualquier ampliación de dicho grupo de empresas solo pueda ser decidida por ese grupo y no por el proveedor de servicios. Más importante aún, 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 los demás. Además, con el fin de permitir

---

27 Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre la gobernanza de datos en la Unión Europea y por el que se modifica el Reglamento (UE) 2018/1724 (Ley 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, sobre 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 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).

modelos de negocio sostenibles, el régimen debería flexibilizarse suprimiendo el requisito de separación jurídica entre los servicios de intermediación de datos y otros servicios de valor añadido que un servicio debería poder ofrecer, sustituyéndolo por una separación funcional y manteniendo al mismo tiempo determinadas salvaguardias. El régimen de supervisión administrativa debería 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 altruismo de datos, solo debería haber registros públicos de la Unión, a saber, uno para los proveedores de servicios de intermediación de datos y otro para las organizaciones de altruismo de datos. Las autoridades competentes que supervisan la concesión de la etiqueta y el cumplimiento por parte de las entidades de los requisitos para obtenerla deberían ser independientes en esta tarea. Esto debe entenderse en el sentido de que son jurídica y funcionalmente independientes de un servicio de intermediación de datos o de una organización de altruismo de datos, incluso a nivel de su alta dirección. Las organizaciones gubernamentales deben poder apoyar financieramente a los servicios de intermediación de datos o a las organizaciones de altruismo de datos, en particular dada la naturaleza emergente de estas entidades, siempre que sean entidades jurídicamente independientes. Con el 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 altruismo de datos reconocidos en la Unión. sobre el diseño de logotipos comunes para identificar a los proveedores de servicios de intermediación de datos y a las organizaciones de altruismo de datos reconocidos en la Unión.

(9) El Reglamento (UE) 2023/2854 elimina las barreras al acceso y la utilización de los datos, 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 titulares de datos que pongan los datos a disposición de los usuarios y de los terceros seleccionados por estos, incluidos los datos protegidos como secretos comerciales, siempre que se mantengan las medidas de confidencialidad establecidas por el titular de los datos. Este requisito de mantener la confidencialidad complementa la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo ([30]) ,que establece la norma para la protección de los secretos comerciales dentro de la Unión. Sin embargo, la divulgación de secretos comerciales a entidades de terceros países puede aumentar los riesgos para su integridad y confidencialidad cuando se exponen a jurisdicciones con protecciones inadecuadas o dificultades en su aplicación efectiva, lo que puede dar lugar a un uso no autorizado, daños económicos e incertidumbre jurídica.

(11) Es necesario reforzar el Reglamento (UE) 2023/2854 introduciendo un motivo adicional para que los titulares de datos se nieguen a revelar secretos comerciales, complementando las disposiciones existentes que permiten la denegación basada en la demostración por parte del titular de los datos de una alta probabilidad de daño económico grave. En virtud de la nueva disposición, los titulares de datos podrán denegar la divulgación de secretos comerciales si demuestran que existe un alto riesgo de adquisición, utilización o divulgación ilícitas a entidades sujetas a regímenes con una protección inadecuada, no equivalente o con marcos jurídicos más débiles que las normas aplicables de la Unión. La nueva disposición también cubre los casos en que el marco jurídico del tercer país, en teoría, es

---

[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 adquisición, utilización y divulgación ilícitas (DO L 157 de 15.6.2016, p. 1).

sólido o supera las normas de la Unión, pero carece de una aplicación adecuada en la práctica. Estos riesgos ponen de relieve la posibilidad de que los secretos comerciales puedan ser adquiridos, utilizados o divulgados en violación del Derecho de la Unión, lo que amenaza la integridad y la confidencialidad de los secretos comerciales.

(12) La activación del mecanismo de denegación debe seguir siendo voluntaria, y la demostración debe realizarse únicamente tras su activación. No debe exigirse a los titulares de datos que realicen un análisis o una demostración exhaustivos 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 divulgar secretos comerciales. En su demostración, los titulares de datos pueden tener en cuenta diversos factores, como normas jurídicas insuficientes o inadecuadas, una aplicación deficiente o arbitraria, infracciones históricas, obligaciones de divulgación en el extranjero que entran en conflicto con el Derecho de la Unión, recursos jurídicos o vías de recurso limitados para las entidades de la Unión, el uso indebido estratégico de tácticas procesales para socavar a los competidores o una influencia política indebida. Dada la diversidad de entidades, terceros países y escenarios de intercambio de datos implicados, los titulares de datos deben centrar su evaluación y demostración en los riesgos pertinentes y actuar en consecuencia, entre otras cosas 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.

(13) Una protección insuficiente de los secretos comerciales y las dificultades para hacerlos valer en terceros países pueden causar un perjuicio irreparable a las empresas europeas. Por lo tanto, el objetivo es reforzar las salvaguardias de los secretos comerciales evitando su filtración a personas físicas o jurídicas establecidas en jurisdicciones que plantean tales riesgos o sujetas a ellas. Esto incluye a las entidades con sede en la Unión controladas por entidades de terceros países, que pueden actuar de mala fe o como fachada de 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 sujeto a la jurisdicción de un tercer país significa que la persona física o jurídica está legalmente regulada, controlada o vinculada de otro modo por las leyes o la autoridad reguladora de un tercer país. Las filiales o empresas asociadas de sociedades matrices de terceros países pueden aprovechar estas jurisdicciones para eludir o burlar las leyes 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 tener la propiedad mayoritaria. Los titulares de los 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 a terceros, velando al mismo tiempo por que siga siendo adecuadamente no intrusiva.

(14) Proteger los secretos comerciales frente a esas vulnerabilidades es esencial para que las industrias europeas mantengan su posición en el mercado y su ventaja competitiva. Si bien los titulares de datos pueden ejercer su discreción a la hora de proteger sus secretos comerciales, la negativa a compartir datos debe limitarse a circunstancias excepcionales y justificadas, con el fin de preservar los objetivos del Reglamento (UE) 2023/2854 de fomentar la innovación basada en datos y una economía digital próspera en la Unión. Deben mantenerse las salvaguardias contra el uso indebido del mecanismo de denegación, incluida la obligación del titular de los datos de demostrar de manera debidamente fundamentada que la divulgación supone un riesgo elevado y de notificarlo a las autoridades competentes. Esta demostración debe proporcionarse por escrito, sin demoras indebidas, al usuario o a terceros, y debe ser proporcional al caso en cuestión. Todas las partes implicadas deben tratar la decisión y la demostración que la respalda como confidenciales, a fin de

preservar la naturaleza confidencial de los secretos comerciales en cuestión. Los usuarios y terceros, según sea el caso, pueden impugnar la decisión del titular de los datos ante la autoridad competente, ante los tribunales o a través de organismos de resolución de litigios.

(15) A fin de simplificar el marco de intercambio de datos entre empresas y administraciones públicas previsto en el Reglamento (UE) 2023/2854 y aclarar las ambigüedades que anteriormente imponían obligaciones más amplias a las empresas, es necesario reducir el ámbito de aplicación del capítulo V de dicho Reglamento de «necesidad excepcional» a «emergencias públicas». El concepto de «emergencias públicas», definido en el artículo 2, apartado 29, del Reglamento (UE) 2023/2854, garantiza así que las obligaciones establecidas en dicho capítulo solo se invoquen en situaciones urgentes y bien definidas, lo que reduce los retos técnicos, administrativos y jurídicos a los que se enfrentaban las empresas en el régimen anterior. De este modo se garantizaría que las solicitudes de datos sean pertinentes y proporcionadas para responder a las emergencias públicas, mitigarlas o apoyar la recuperación de las mismas. Dado que el marco actualizado de la Unión sobre estadísticas europeas en virtud del Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo([31]) no aborda las emergencias públicas, es esencial preservar 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 estén obligadas a facilitar datos para hacer frente a una emergencia pública, en cuyo caso dichas empresas podrán solicitar una compensación.

(16) A fin de mitigar las incertidumbres jurídicas que podrían desalentar los modelos de negocio innovadores, es necesario abordar las importantes ambigüedades y cargas que se derivan del cumplimiento de las disposiciones sobre contratos inteligentes que ejecutan acuerdos de intercambio de datos en virtud del artículo 36 del Reglamento (UE) 2023/2854. La ausencia de normas armonizadas y de definiciones claras de conceptos clave como «solidez», «control de acceso» y «coherencia con las condiciones contractuales», junto con el requisito de un «mecanismo de terminación o interrupción seguro» potencialmente incompatible con las arquitecturas de cadenas de bloques descentralizadas o públicas basadas en libros de contabilidad inmutables, planteaba retos a los innovadores desde el punto de vista de los costes y las oportunidades. Además, la ambigüedad que rodea la realización de la evaluación de la conformidad en virtud del 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 promovería el desarrollo y la introducción en el mercado de nuevos modelos de negocio, fomentaría la innovación y reduciría las barreras para las tecnologías emergentes.

(17) Ciertos servicios de tratamiento de datos, que no entran en el modelo de prestación de infraestructura como servicio (IaaS), se adaptan a las necesidades o al ecosistema de un cliente. La prestación de dichos servicios de tratamiento de datos se basa en negociaciones precontractuales y contractuales que requieren mucho tiempo para determinar los requisitos específicos de

---

[31] Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, sobre las estadísticas europeas y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 del Parlamento Europeo y del Consejo relativo a la transmisión de datos sujetos a confidencialidad estadística a la Oficina Estadística de las Comunidades Europeas, el Reglamento (CE) n.º 322/97 del Consejo, relativo a la política estadística de la Comunidad Europea, 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 27.3.1989, p. 1). (CE) n.º 322/97 del Consejo, relativo a 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).

el cliente y los esfuerzos técnicos posteriores para personalizar el servicio de tratamiento de datos y ofrecer una solución a medida. Se trata de servicios que no se prestan de forma estándar y que se personalizan según las necesidades del cliente para ofrecer una solución a medida, en la que el proveedor ha adaptado la mayoría de las características y funcionalidades del servicio de tratamiento de datos a las necesidades específicas del cliente, ya que la mayoría de las características y funcionalidades no serían utilizables para un cliente sin una adaptación previa por parte del proveedor. Estos servicios difieren de los servicios de tratamiento de datos personalizados a los que se refiere el artículo 31, apartado 1, del Reglamento (UE) 2023/2854. Los servicios de tratamiento de datos personalizados son servicios cuyas características principales han sido personalizadas en su mayoría para adaptarse a las necesidades específicas de un cliente concreto o que no se ofrecen a gran escala comercial a través del catálogo de servicios del proveedor. Para evitar los costes adicionales y la carga administrativa que supone 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 excepción de la obligación de reducir y, en última instancia, eliminar los cargos por cambio de proveedor y salida, los servicios personalizados prestados en virtud de 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 motivos relacionados con la planificación financiera y la atracción de inversiones, los proveedores de servicios de tratamiento de datos, especialmente las pymes y las microempresas, pueden preferir y ofrecer contratos de duración determinada. Es necesario aclarar que los proveedores de servicios de tratamiento de datos pueden incluir en dichos contratos cláusulas sobre sanciones proporcionales por rescisión anticipada, siempre que no constituyan un obstáculo para el cambio de proveedor. Además, los proveedores de servicios de tratamiento de datos que son pymes o microempresas se ven especialmente afectados por la necesidad de adaptar 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 esos proveedores si prestan servicios de tratamiento de datos, distintos de los de IaaS, basados en 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 gastos de cambio, incluidos los gastos de salida, constituyen un grave obstáculo para el cambio, los nuevos regímenes más ligeros para los servicios de tratamiento de datos personalizados o prestados por pymes o microempresas no deben socavar la supresión gradual de dichos gastos. Las disposiciones contractuales contrarias a ese objetivo deben considerarse como si nunca hubieran existido, si se incluyen en acuerdos contractuales sobre la prestación de servicios que entran en el ámbito de aplicación de esos dos nuevos regímenes específicos.

(19) El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo[32] introdujo un principio clave para apoyar la economía basada en datos dentro de la Unión, que sustenta de manera concreta la libertad de establecimiento y la libre prestación de servicios. La «libre circulación de datos» en la Unión, aclarada mediante la prohibición de imponer la localización de datos, sigue siendo un principio fundamental que proporciona seguridad jurídica a las empresas y debe mantenerse en el Reglamento (UE) 2023/2854. La disposición no afecta al tratamiento de datos en la medida en que se lleve a cabo como parte de una actividad que

[32] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre 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).

queda fuera del 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. Al mismo tiempo, otras disposiciones del Reglamento (UE) 2018/1807 quedan sustituidas por normas más recientes. En particular, el capítulo VI del Reglamento (UE) 2023/2854 introdujo un marco jurídico horizontal moderno que aborda el cambio entre servicios de tratamiento de datos y dejó prácticamente obsoleto el artículo 6 del Reglamento (UE) 2018/1807. La coexistencia de esas disposiciones ha aumentado la complejidad jurídica para las empresas. Por lo tanto, debe derogarse el Reglamento (UE) 2018/1807.

(20) El concepto de «seguridad pública», en el sentido del artículo 52 del TFUE y tal como lo interpreta el Tribunal de Justicia, abarca tanto la seguridad interior como la exterior de un Estado miembro, así como las cuestiones de seguridad pública, con el fin, en particular, de facilitar la investigación, la detección y el enjuiciamiento de los delitos penales. Supone la existencia de una amenaza real y suficientemente grave que afecte a uno de los intereses fundamentales de la sociedad, como una amenaza al funcionamiento de las instituciones y los servicios públicos esenciales y a la supervivencia de la población, así como el riesgo de una perturbación grave de las relaciones exteriores o de 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 que se justifiquen por motivos de seguridad pública deben ser adecuados para alcanzar el objetivo perseguido y no deben ir más allá de lo 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 incertidumbre jurídica, principalmente para los organismos del sector público. Por lo tanto, es necesario armonizar las normas en un único instrumento jurídico para lograr 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 desde la perspectiva tanto de los organismos del sector público como de los reutilizadores de la información del sector público, es razonable derogar la Directiva (UE) 2019/1024 y el Reglamento (UE) 2022/868, armonizar ambos regímenes y consolidar las normas en un único capítulo 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 garantizar que, incluso cuando se designen organismos competentes específicos para cada sector, todos los sectores pertinentes queden finalmente cubiertos. Las modificaciones introducidas en el presente Reglamento deben entenderse en el sentido de que no alteran la interpretación de las diferentes definiciones y términos, salvo que se especifique claramente lo contrario.

(23) Los datos y documentos que pueden ponerse a disposición del público para su reutilización y los datos y documentos que están protegidos por motivos de confidencialidad comercial, incluidos los secretos comerciales, profesionales y empresariales, la confidencialidad estadística, la protección de los derechos de propiedad intelectual de terceros o la protección de los datos personales, suelen estar en poder de los mismos organismos del sector público. Por lo tanto, es necesario armonizar las definiciones y los principios comunes que se aplican a toda la información del sector público y abordar las cuestiones relativas a la interacción entre los dos conjuntos de normas.

(24) Las normas existentes deben racionalizarse para mejorar su claridad y coherencia. No obstante, los dos regímenes de reutilización deben seguir siendo distintos y su ámbito de aplicación respectivo 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 correspondiente a determinadas categorías de datos protegidos deben limitar su disponibilidad pública y considerar la posibilidad de ponerlos a disposición para su reutilización como datos protegidos.

(25) Las empresas emergentes, las pequeñas empresas y las empresas que se consideran medianas según el artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión[33] y las empresas de sectores con capacidades digitales menos desarrolladas tienen dificultades para reutilizar datos y documentos. Al mismo tiempo, han surgido unas pocas entidades muy grandes con un considerable poder económico en la economía digital gracias a la acumulación y agregación de grandes volúmenes de datos y a la infraestructura tecnológica para monetizarlos. Entre esas grandes empresas se incluyen las que prestan servicios de plataforma básicos y están designadas como guardianes del acceso en virtud del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo([34]) y sujetas a obligaciones especiales para corregir los desequilibrios. A fin de corregir esos 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 grandes empresas. Dichas condiciones deben ser proporcionadas, basarse en criterios objetivos y tener en cuenta el poder económico, la capacidad de la entidad para adquirir datos o su designación como guardián de acceso en virtud del Reglamento (UE) 2022/1925, así como otros criterios similares, cuando proceda. Dichas condiciones especiales pueden referirse, entre otras cosas, a los cargos 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 gama de participantes en el mercado y no refuercen inadvertidamente las posiciones dominantes existentes. Las empresas muy grandes, y en particular las designadas como guardianes del acceso en virtud del Reglamento (UE) 2022/1925, tienen un poder y una influencia significativos en el mercado interior. Para evitar que estas entidades aprovechen sus importantes medios en detrimento de la competencia leal y la innovación, los organismos del sector público deben poder fijar cargos y tasas más elevados por la reutilización de datos gubernamentales abiertos y datos protegidos. Dichos cargos 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 pequeñas empresas y los nuevos operadores del mercado para innovar y competir en la economía digital.

(27) El presente Reglamento propone una serie de modificaciones específicas del Reglamento (UE) 2016/679 con fines de clarificación y simplificación, al tiempo que se mantiene el mismo nivel de protección de datos. El artículo 4 del Reglamento (UE) 2016/679 establece que los datos personales son cualquier información relacionada con una persona física identificada o identificable. Con el fin de

---

[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 competitivos y justos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Ley de Mercados Digitales ) (DO L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que puedan utilizarse razonablemente para identificar a la persona física de forma directa o indirecta. Teniendo en cuenta la jurisprudencia del Tribunal de Justicia de la Unión Europea relativa a la definición de datos personales, es necesario aclarar en qué casos debe considerarse identificable a una persona física. La existencia de información adicional que permita identificar al interesado no significa, por sí sola, que los datos seudonimizados deban considerarse, en todos los casos y para todas las personas o entidades, datos personales a efectos de la aplicación del Reglamento (UE) 2016/679. En particular, debe aclararse que la información no debe considerarse datos personales para una entidad determinada cuando dicha entidad no disponga de medios razonablemente susceptibles de utilizarse 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 de que disponen, convierte esa información en datos personales solo para aquellos terceros que dispongan de dichos medios. Una entidad para la que la información no es, en principio, datos personales no entra en el ámbito de aplicación del Reglamento (UE) 2016/679. A este respecto, el Tribunal de Justicia de la Unión Europea ha sostenido que no es razonablemente probable que se utilicen medios para identificar al interesado cuando el riesgo de identificación parece insignificante en la realidad, en la medida en que la identificación de dicho interesado está prohibida por la ley o es imposible en la práctica, por ejemplo, porque supondría un esfuerzo desproporcionado en términos de tiempo, coste y trabajo. Un ejemplo de prohibición de reidentificación se encuentra en las obligaciones de los usuarios de datos sanitarios en el artículo 61, apartado 3, del Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo([35]). 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.

(28) A fin de evaluar si la investigación cumple las condiciones de investigación científica a efectos del presente Reglamento, pueden tenerse en cuenta elementos como el enfoque metodológico y sistemático aplicado al realizar la investigación en el ámbito específico. La investigación y el desarrollo tecnológico deben llevarse a cabo en entornos académicos, industriales y de otro tipo, incluidas las pequeñas y medianas empresas (artículo 179, apartado 2, del TFUE), y deben ser siempre de alta calidad y respetar los principios de fiabilidad, honestidad, respeto y responsabilidad (verificabilidad).

(29) Cabe reiterar que el tratamiento posterior con fines de archivo en interés público, de investigación científica o histórica o con fines estadísticos debe considerarse una operación de tratamiento lícita y compatible. En tales casos, no es necesario determinar, sobre la base del artículo 6, apartado 4, del presente Reglamento, si la finalidad del tratamiento posterior es compatible con la finalidad para la que se recabaron inicialmente los datos personales.

---

[35] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos Sanitarios y por el que se modifica 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)

(30) Una IA fiable es fundamental para impulsar el crecimiento económico y apoyar la innovación con resultados socialmente beneficiosos. El desarrollo y el uso de sistemas de IA y los modelos subyacentes, como los grandes modelos lingüísticos y los modelos de vídeo generativo, se basan en datos, incluidos datos personales, en diversas fases del ciclo de vida de la IA, como la fase de formación, prueba y validación, y en algunos casos pueden conservarse en el sistema o modelo de IA. Por lo tanto, el tratamiento de datos personales en este contexto puede llevarse a cabo con fines de 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 la utilización (despliegue) de la IA en un contexto específico o para fines específicos cumpla con otras disposiciones del Derecho de la Unión o nacional, ni a la obligación de garantizar el cumplimiento cuando su uso esté expresamente prohibido por la ley. Tampoco afecta a su obligación de garantizar que se cumplan todas las demás condiciones del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, así como 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 la escalabilidad de las obligaciones en virtud del presente Reglamento, sopesa el interés legítimo perseguido por el responsable del tratamiento o un tercero y los intereses, derechos y libertades del interesado, se debe considerar si el interés perseguido por el responsable del tratamiento es beneficioso para el interesado y la sociedad en general, lo que puede ser el caso, por ejemplo, cuando el tratamiento de datos personales es necesario para detectar y eliminar sesgos, protegiendo así a los interesados contra la discriminación, o cuando el tratamiento de datos personales tenga por objeto garantizar resultados precisos 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 en función de su relación con el responsable del tratamiento, las garantías adecuadas para minimizar el impacto en los derechos de los interesados, como proporcionar una mayor transparencia a los interesados, otorgarles un derecho incondicional a oponerse al tratamiento de sus datos personales, respetar las indicaciones técnicas incorporadas en un servicio que limite el uso de datos para el desarrollo de IA por parte de terceros, el uso de otras técnicas de vanguardia para la protección de la privacidad en el entrenamiento de la IA y medidas técnicas adecuadas para minimizar eficazmente los riesgos derivados, por ejemplo, de la regurgitación, la fuga de datos y otras acciones intencionadas 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. A tal fin, 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 científica, de conformidad con el artículo 13 de la Carta. Por lo tanto, 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 que se cumplan todas las demás condiciones del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, así como 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, incluidos datos personales y categorías especiales de los mismos. Las categorías especiales de datos personales pueden existir de forma residual en los conjuntos de datos de formación, prueba o validación, o conservarse en el sistema de IA o el modelo de IA, aunque las categorías especiales de datos personales no sean necesarias para los fines del tratamiento. A 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 las categorías especiales

de datos personales, debe permitirse una excepción a la prohibición de tratar 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 aplicado de manera eficaz las medidas técnicas y organizativas adecuadas para evitar el tratamiento de esos 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 requiriera un esfuerzo desproporcionado, en particular cuando la eliminación de categorías especiales de datos memorizados en el sistema o modelo de IA requiriera la reingeniería del sistema o modelo de IA, el responsable del tratamiento debería proteger eficazmente dichos datos para que no se utilicen para inferir resultados, se divulguen o se pongan a disposición de terceros. Esta excepción no debería aplicarse cuando el tratamiento de categorías especiales de datos personales sea necesario para la finalidad del tratamiento. En este caso, el responsable del tratamiento deberá acogerse a las excepciones previstas en el artículo 9, apartado 2, letras a) a j), del Reglamento (UE) 2016/679.

(34) Los datos biométricos, tal como se definen en el artículo 4, apartado 14, del Reglamento (UE) 2016/679, se refieren al tratamiento de determinadas características de una persona física mediante medios técnicos específicos que permiten o confirman la identificación única de dicha persona. El concepto de datos biométricos incluye dos funciones distintas, a saber, la identificación de una persona física o la verificación (también denominada autenticación) de su identidad declarada, ambas basadas en procesos técnicos diferentes. El proceso de identificación se basa en una búsqueda «uno a muchos» de los datos biométricos del interesado en una base de datos, mientras que el proceso de verificación se basa en una comparación «uno a uno» de los datos biométricos facilitados por el interesado, que de este modo afirma su identidad. También debe permitirse una excepción a la prohibición de tratar datos biométricos prevista en el artículo 9, apartado 1, del Reglamento cuando la verificación de la identidad declarada del interesado sea necesaria para un fin perseguido por el responsable del tratamiento y se apliquen las garantías adecuadas para que el interesado tenga el control exclusivo del proceso de verificación. Por ejemplo, cuando los datos biométricos se almacenan de forma segura únicamente por parte del interesado o se almacenan de forma segura por parte del responsable del tratamiento en un formato cifrado de última generación y la clave de cifrado o un medio equivalente está en poder exclusivo del interesado, es improbable que dicho tratamiento genere riesgos significativos para sus derechos y libertades fundamentales. El responsable del tratamiento no tiene conocimiento de los datos biométricos o solo lo tiene durante un tiempo muy limitado durante el proceso de verificación.

(35) El artículo 15 del Reglamento (UE) 2016/679 otorga a los interesados el derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que les conciernen y, en tal caso, el acceso a los datos personales y a determinada información adicional. El derecho de acceso debe permitir al interesado conocer y verificar la licitud del tratamiento y ejercer los demás derechos que le confiere el Reglamento (UE) 2016/679. Por el contrario, debe aclararse en el artículo 12 del Reglamento que el derecho de acceso, que es desde el principio favorable a los interesados, no debe ser objeto de abuso en el sentido de que los interesados lo utilicen con fines distintos de la protección de sus datos. Por ejemplo, se produciría un abuso del derecho de acceso cuando el interesado tuviera la intención de provocar 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 presentar una reclamación por daños y perjuicios. Otros ejemplos de abuso son las 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 algún tipo de beneficio por parte del responsable del tratamiento. Además, con el fin de mantener su carga en un nivel razonable, los responsables del tratamiento deberían tener una menor carga de

respecto al carácter excesivo de una solicitud que respecto al carácter manifiestamente infundado de una solicitud. La razón es que el carácter manifiestamente infundado de una solicitud depende de hechos que se encuentran principalmente dentro del ámbito de responsabilidad del responsable del tratamiento, mientras que el carácter excesivo de una solicitud se refiere a la posible conducta abusiva de un interesado, que se encuentra principalmente fuera del ámbito de influencia del responsable del tratamiento y, por lo tanto, este último solo puede demostrar dicho abuso hasta un nivel razonable. En cualquier caso, al solicitar el acceso en virtud del artículo 15 del Reglamento (UE) 2016/679, el interesado debe ser lo más específico posible. Las solicitudes excesivamente amplias e indiferenciadas también deben considerarse excesivas.

(36) El artículo 13 del Reglamento (UE) 2016/679 exige al responsable del tratamiento que facilite al interesado determinada información sobre el tratamiento de sus datos personales, así como otra información 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 apartado 4 del artículo 13 del Reglamento (UE) 2016/679, dicha 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 menoscabar las posibilidades del interesado de ejercer sus derechos en virtud del capítulo III del Reglamento, esta excepción debe ampliarse a las situaciones en las que el tratamiento no sea susceptible de generar un riesgo elevado, 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 refieren las letras a) y c) del apartado 1, habida cuenta 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. Se trata de situaciones en las que el contexto de la relación entre el responsable del tratamiento y el interesado es muy claro y circunscrito y la actividad del responsable del tratamiento no es intensiva en datos, como la relación entre un artesano y sus clientes, en la que el alcance del tratamiento se limita a los datos mínimos necesarios para prestar el servicio. La actividad del responsable del tratamiento no es intensiva en datos cuando recopila una cantidad reducida 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 es intensivo en datos, no es complejo y el responsable del tratamiento recopila una cantidad reducida de datos personales, debería ser razonable esperar, por ejemplo, que el interesado disponga de la información sobre la identidad y los datos de contacto del responsable del tratamiento, así como sobre la finalidad del tratamiento, cuando dicho tratamiento se realice 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 debería aplicarse a las asociaciones y clubes deportivos cuando 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 el acceso basándose en esta última disposición. Cuando no se aplique la excepción a las obligaciones del artículo 13, a fin de equilibrar la necesidad de exhaustividad y fácil comprensión por parte del interesado, los responsables del tratamiento podrán adoptar un enfoque por capas a la hora de facilitar la información requerida, en particular permitiendo a los usuarios navegar para obtener más información.

(37) Cuando el tratamiento se realice con fines de investigación científica y el suministro de información al interesado resulte imposible o suponga un esfuerzo desproporcionado, no será necesario facilitar la información prevista en el artículo 13 del presente Reglamento. El responsable del tratamiento deberá realizar esfuerzos razonables para obtener los datos de contacto si están fácilmente disponibles y su obtención no requiere

un esfuerzo desproporcionado. El suministro de la información supondría un esfuerzo desproporcionado, en particular cuando el responsable del tratamiento, en el momento de la recogida de los datos personales, no sabía ni preveía que trataría datos personales con fines de investigación científica en una fase posterior, en cuyo caso es posible que no disponga de datos de contacto fácilmente accesibles de los interesados. En tales situaciones, el responsable del tratamiento deberá informar a los interesados de forma indirecta, por ejemplo, haciendo pública la información. El suministro de dicha información debe garantizar que se llegue al mayor número posible de interesados. Los medios pertinentes para hacer pública la información 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 regulan el tratamiento de datos personales cuando el responsable del tratamiento toma decisiones que tienen efectos jurídicos o efectos igualmente significativos para el interesado, basándose únicamente en el tratamiento automatizado. A fin de proporcionar una mayor seguridad jurídica, debe aclararse que las decisiones basadas únicamente en el tratamiento automatizado están permitidas cuando se cumplen condiciones específicas, tal como se establece en el Reglamento (UE) 2016/679. También 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, tal como se establece en el artículo 22, apartado 2, letra a), del Reglamento (UE) 2016/679, no debe exigirse que la decisión pueda tomarse únicamente mediante un tratamiento automatizado. Esto significa que el hecho de que la decisión también pueda ser tomada por un ser humano no impide que el responsable del tratamiento tome la decisión mediante un tratamiento únicamente automatizado. Cuando existan varias soluciones de tratamiento automatizado igualmente eficaces, el responsable del tratamiento deberá utilizar la menos intrusiva.

(39) Con el fin de reducir la carga que recae sobre los responsables del tratamiento y garantizar 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 datos personales a la autoridad de control con arreglo al artículo 33 del Reglamento (UE) 2016/679 debe ajustarse al umbral para la comunicación de una violación de datos personales al interesado con arreglo al artículo 34 de dicho Reglamento. En el caso de una violación de datos que no sea susceptible de suponer un alto riesgo para los derechos y libertades de las personas físicas, no se debe exigir al responsable del tratamiento que notifique a la autoridad de control competente. El umbral más alto para notificar una violación de 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 el cumplimiento de dicho Reglamento, de conformidad con el artículo 5, apartado 2, del mismo. A fin de facilitar el cumplimiento por parte de los responsables del tratamiento y un enfoque armonizado en la Unión, el Comité debe elaborar una plantilla común para notificar las violaciones de datos a la autoridad de control competente y una lista común de circunstancias en las que una violación de datos personales puede suponer 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, la plantilla 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 una violación de datos personales pueda suponer un alto riesgo para los derechos y libertades de una persona física no debe afectar a la obligación 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 realicen una evaluación de impacto relativa a la protección de datos cuando el tratamiento de datos personales pueda suponer un alto riesgo para los derechos y libertades de las personas físicas. Las autoridades de control establecidas en virtud de dicho Reglamento deben elaborar y publicar una lista

de los tipos de operaciones de tratamiento que están sujetas al requisito de realizar una evaluación de impacto relativa a la protección de datos. Además, el Reglamento establece que las autoridades de control pueden elaborar y publicar una lista de los tipos de operaciones de tratamiento para las que no se requiere una evaluación de impacto relativa a la protección de datos. Con el fin de contribuir eficazmente al objetivo de convergencia de las economías y garantizar efectivamente 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 proporcionarse una lista única de operaciones de tratamiento a nivel de la UE, que sustituya a las listas nacionales existentes. Además, la publicación de una lista de los tipos de operaciones de tratamiento para los que no se requiere una evaluación de impacto relativa a la protección de datos, que actualmente es facultativa, debe ser obligatoria. 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 elaborar una plantilla común y una metodología común para realizar evaluaciones de impacto relativas a la protección de datos, que la Comisión adoptará 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 la evolución tecnológica, las listas y la plantilla y la metodología comunes deben revisarse al menos cada tres años y actualizarse cuando sea necesario.

(41) El Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[36] se aplica al tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión. La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo([37]) se aplica al tratamiento de datos personales por parte de las autoridades competentes con 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 armonizarse con las modificaciones del Reglamento (UE) 2016/679 introducidas por el presente Reglamento.

(42) Tal 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, ambos conjuntos de disposiciones deben interpretarse de manera homogénea, con arreglo a la jurisprudencia del Tribunal de Justicia de la Unión Europea. 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 que se ven afectadas por las modificaciones del Reglamento (UE)

---

[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, los órganos y los organismos de la Unión, a la libre circulación de dichos 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 la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos 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).

2016/679, en la medida en que estas últimas modificaciones también son pertinentes en el contexto del tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión.

(43) Con el fin de proporcionar un marco sólido y coherente de protección de datos en la Unión, las adaptaciones necesarias de la Directiva (UE) 2016/680 y cualquier otro acto jurídico de la Unión aplicable a dicho tratamiento de datos personales tras la adopción del presente Reglamento, a fin de permitir su aplicación lo más cerca posible de la entrada en vigor de las modificaciones del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725.

(44) El almacenamiento de datos personales, o el acceso a datos personales ya almacenados, en un equipo terminal y el posterior tratamiento de dichos datos deben regularse en un único marco jurídico, 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 más altos niveles de protección de los datos personales, al tiempo que simplifican la experiencia 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, al acceso o la recopilación de información de dicho equipo que implique el tratamiento de datos personales mediante cookies o tecnologías similares para obtener información del equipo terminal. Las normas pertinentes también deben aplicarse independientemente de que el equipo terminal sea propiedad de la persona física o de otra persona jurídica o física.

El almacenamiento de datos personales, o el acceso a datos personales ya almacenados, en un equipo terminal solo debe seguir estando permitido sobre la base del consentimiento. De manera similar al enfoque de la Directiva 2002/58/CE, este requisito no debe impedir el almacenamiento de datos personales, ni el 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, si cumple todas las condiciones de licitud establecidas en dicha disposición y se realiza con los fines establecidos en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.

Con el fin de reducir la carga que supone el cumplimiento de la normativa y proporcionar claridad jurídica a los responsables del tratamiento, y dado que determinados fines del tratamiento suponen un riesgo bajo 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 definir una lista limitativa de fines para los que se debe permitir el tratamiento sin consentimiento. Por lo que se refiere al almacenamiento de datos personales, o al acceso a datos personales ya almacenados, en un equipo terminal, y al tratamiento posterior necesario para esos fines, el presente Reglamento debe disponer que el tratamiento es lícito. El responsable del tratamiento, como un proveedor de servicios de medios de comunicación, puede encargar a un encargado del tratamiento, como una empresa de estudios de mercado, que realice el tratamiento en su nombre.

Para el tratamiento posterior de datos personales con fines distintos de los definidos en la lista limitativa, deben aplicarse el artículo 6 y, en su caso, el artículo 9 del Reglamento (UE) 2016/679. Es responsabilidad del responsable del tratamiento, a la luz del principio de responsabilidad, 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 fundamento para el tratamiento posterior de datos personales, el responsable del tratamiento debe demostrar que persigue el interés legítimo del responsable del tratamiento o de terceros, que el tratamiento es necesario para alcanzar el objetivo de ese interés legítimo y que los intereses o derechos fundamentales del interesado no se ven afectados.

prevalecer sobre los intereses perseguidos por el responsable del tratamiento. En este contexto, los responsables del tratamiento deben tener muy en cuenta los siguientes elementos: si el interesado es un niño; las expectativas razonables del interesado; el impacto en la persona, ya sea por la magnitud de los datos tratados o por la sensibilidad de los mismos; la magnitud del tratamiento en cuestión, en el sentido de que el tratamiento no puede ser especialmente extenso, ya sea por su volumen o por la variedad de categorías de datos; el tratamiento debe basarse en datos limitados a lo necesario y no puede basarse en la supervisión de gran parte de la actividad en línea de los interesados; y otros factores pertinentes, según proceda. El tratamiento no debe dar lugar a la vigilancia continua de la vida privada del interesado.

Cuando el responsable del tratamiento no pueda invocar el interés legítimo como base jurídica para el tratamiento posterior, el tratamiento debe basarse en otra base del artículo 6, apartado 1, en particular en el consentimiento de conformidad con los artículos 6 y 7 del Reglamento (UE) 2016/679, siempre que se cumplan todos los principios del Reglamento (UE) 2016/679.

(45) Los interesados que han denegado una solicitud de consentimiento se enfrentan a menudo a una nueva solicitud de consentimiento cada vez que vuelven a visitar el servicio en línea del mismo responsable del tratamiento. Esto puede tener efectos perjudiciales para los interesados, que pueden dar su consentimiento solo para evitar repetir las solicitudes. Por lo tanto, el responsable del tratamiento debe estar obligado a respetar la decisión del interesado de denegar una solicitud de consentimiento durante al menos un determinado período.

(46) Los interesados deben tener la posibilidad de basarse en indicaciones automatizadas y legibles por máquina de su elección de consentir o rechazar una solicitud de consentimiento u oponerse al tratamiento de datos. Dichos medios deben seguir los últimos avances tecnológicos. Pueden implementarse en la configuración de un navegador web o en la cartera de identidad digital de la UE, tal como se establece en el Reglamento (UE) 914/2014, o cualquier otro medio adecuado. Las normas establecidas en el presente Reglamento deben favorecer la aparición de soluciones impulsadas por el mercado con interfaces adecuadas. El responsable del tratamiento debe estar obligado a respetar las indicaciones automatizadas y legibles por máquina de las elecciones del interesado una vez que existan normas disponibles. Habida cuenta de la importancia del periodismo independiente en una sociedad democrática y con el fin de no socavar su base económica, los prestadores de servicios de medios de comunicación no deben estar obligados a respetar las indicaciones legibles por máquina de las elecciones del interesado. La obligación de los proveedores de navegadores web de proporcionar los medios técnicos para que los interesados puedan tomar decisiones con respecto al tratamiento no debe socavar la posibilidad de que los proveedores de servicios de medios de comunicación soliciten el consentimiento de los interesados.

(47) La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas («Directiva sobre la privacidad electrónica»), revisada por última vez en 2009, establece un marco para la protección del derecho a la intimidad, incluida la confidencialidad de las comunicaciones. También especifica el Reglamento (UE) 2016/679 en relación con el tratamiento de datos personales en el contexto de los servicios de comunicaciones electrónicas. Protege la privacidad y la integridad de los equipos terminales de los usuarios o abonados utilizados 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 accede no constituya ni dé lugar al tratamiento de datos personales.

(48) El artículo 4 de la Directiva 2002/58/CE debe derogarse. El artículo 4 de la Directiva 2002/58/CE 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 materia de medidas de gestión de riesgos de ciberseguridad y notificación de incidentes para dichos proveedores. Con el fin de reducir la duplicación de obligaciones para las entidades del

sector de las comunicaciones electrónicas, debe derogarse el artículo 4 de la Directiva 2002/58/CE. En lo que respecta a la seguridad del tratamiento de datos personales con arreglo al artículo 4 , apartados 1 y 1 bis, de la presente Directiva y a la notificación de violaciones de datos personales con arreglo al artículo 4, apartados 3 a 5, de la Directiva 2002/58/CE, el Reglamento (UE) 2016/679 ya establece normas exhaustivas y actualizadas. Por lo tanto, estas normas deben aplicarse a los proveedores de servicios de comunicaciones electrónicas disponibles al público y a los proveedores de redes públicas de comunicaciones, garantizando así que se aplique un único régimen a los responsables y a los encargados del tratamiento.

(49) Varios actos jurídicos horizontales o sectoriales de la Unión exigen la notificación del mismo hecho a diferentes autoridades utilizando diferentes medios y canales técnicos. El punto único de entrada para la notificación de incidentes debe permitir a las entidades cumplir las obligaciones de notificación establecidas en 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 una única interfaz. Además, el punto de entrada único debería ofrecer a las entidades la posibilidad de recuperar la información que hayan presentado anteriormente a través del mismo, lo que les ayudaría a realizar un seguimiento del cumplimiento de sus 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 que se plantean para la seguridad del punto de entrada único y la información presentada o difundida a través del mismo. Al evaluar el riesgo y la adecuación y proporcionalidad de dichas medidas, la ENISA debe tener en cuenta la sensibilidad de la información presentada o difundida de conformidad con los actos jurídicos pertinentes de la Unión. La ENISA debe consultar a las autoridades competentes en virtud de los actos jurídicos pertinentes de la Unión al elaborar las medidas técnicas, operativas y organizativas necesarias para establecer, mantener y gestionar de forma segura el punto de entrada único, utilizando los grupos y redes de cooperación existentes de los Estados miembros establecidos en virtud de dichos actos.

(51) Antes de habilitar la notificación de incidentes, la ENISA debe poner a prueba el funcionamiento del punto de entrada único, lo 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 buen funcionamiento, la fiabilidad, la integridad y la confidencialidad del punto de entrada único. La Comisión debe consultar a la red CSIRT y a las autoridades competentes en virtud de los actos jurídicos pertinentes de la Unión, utilizando los grupos y redes de cooperación existentes de los Estados miembros establecidos en virtud de dichos actos, al realizar la evaluación. Cuando la Comisión considere que el punto de entrada único garantiza el buen funcionamiento, la fiabilidad, la integridad y la confidencialidad, debe publicar un aviso a tal efecto en el Diario Oficial de la Unión Europea. En caso de que la Comisión considere que no se garantiza el buen funcionamiento, la fiabilidad, la integridad y la confidencialidad, 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, en la medida de lo posible, la ENISA deberá tener en cuenta dichas soluciones técnicas nacionales al elaborar las especificaciones sobre las medidas técnicas, operativas y organizativas necesarias para establecer, mantener y gestionar de forma segura el punto de entrada único. Además, la ENISA deberá tener en cuenta los protocolos y herramientas técnicos, como las interfaces de programación de aplicaciones y los estándares legibles por máquina

que permitan a las entidades integrar las obligaciones de notificación 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 en 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 sobre sus disposiciones nacionales.

(54) Sobre la base del Reglamento (UE) 2022/2554, el sector financiero ha estado a la vanguardia en la aplicación de un marco armonizado, completo y eficaz, también en lo que respecta a la notificación de incidentes. A fin de simplificar el cumplimiento, conviene armonizar el marco de notificación de incidentes establecido en el Reglamento (UE) 2022/2554 con el punto de entrada único, garantizando al mismo tiempo la continuidad y la estabilidad del marco de notificación existente, y teniendo en cuenta que el punto de entrada único sería operativo una vez que se hubiera evaluado que garantiza el buen funcionamiento, la fiabilidad, la integridad y la confidencialidad. Además, el Reglamento (UE) 2022/2554 ha introducido plantillas de notificación normalizadas que racionalizan el contenido de las notificaciones de incidentes graves relacionados con las TIC para el sector financiero. La experiencia adquirida con la adopción de estas plantillas proporciona información valiosa y buenas prácticas que deben tenerse en cuenta a la hora de especificar el tipo de información, el formato y el procedimiento de notificación a efectos de informar al punto de entrada único con arreglo a la Directiva (UE) 2022/2555, la Directiva (UE) 2022/2557 o el Reglamento (UE) 2016/679, según proceda. A tal fin, la Comisión debe tener debidamente en cuenta las normas técnicas reglamentarias adoptadas de conformidad con el Reglamento (UE) 2022/2554, que especifican el contenido de la notificación inicial, así como de los informes intermedios y finales, relativos a incidentes graves relacionados con las TIC. Este enfoque tiene por objeto garantizar la coherencia, promover las sinergias y reducir la carga administrativa de las entidades, minimizando el número de campos de datos que estas deben completar, lo que facilita unos procesos de notificación más eficientes y ágiles.

(55) En virtud de los actos jurídicos pertinentes de la Unión, determinada información específica sobre incidentes debe compartirse en una fase posterior entre las autoridades competentes para facilitar una supervisión y coordinación eficaces. Por lo tanto, el punto de entrada único debe diseñarse de manera que permita y facilite el intercambio de información a ese nivel para cada acto jurídico pertinente de la Unión, garantizando que los flujos de datos adecuados entre las autoridades se habiliten de manera segura, oportuna y eficiente, en caso de que los Estados miembros decidan hacer uso de esta función adicional.

(56) Para garantizar que la notificación de incidentes se realice a través del punto de entrada único, deben modificarse en consecuencia la Directiva (UE) 2022/2555, el Reglamento (UE) 2016/679, el Reglamento (UE) 2022/2554, el Reglamento (UE) 910/2014 y la Directiva (UE) 2022/2557. El punto único de entrada debería empezar a utilizarse a efectos de la notificación en virtud de dichos actos en un plazo de 18 meses a partir de la entrada en vigor del presente Reglamento. Cuando la Comisión ponga en marcha los mecanismos de la notificación que retrasa la fecha de aplicación a 24 meses a partir de la entrada en vigor del Reglamento, las disposiciones correspondientes de la Directiva (UE) 2022/2555, el Reglamento (UE) 910/2014, el Reglamento (UE) 2022/2554 y la Directiva (UE) 2022/2557 seguirán 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 deberán cumplir sus obligaciones de notificación

mediante medios alternativos. A tal fin, los destinatarios de las notificaciones de incidentes en virtud de los actos jurídicos pertinentes de la Unión deben asegurarse de que pueden recibir dichas notificaciones de incidentes a través de medios alternativos y deben poner a disposición del público la información sobre dichos medios alternativos.

(58) Se consultó al Supervisor Europeo de Protección de Datos de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[38] , y este emitió su dictamen el [FECHA]. Se consultó al Comité Europeo de Protección de Datos de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725, que emitió su dictamen el [FECHA].

(59) El Reglamento (UE) 2019/1150 establece un conjunto específico de normas obligatorias a nivel de la Unión para garantizar un entorno empresarial en línea justo, predecible, sostenible y fiable dentro del mercado interior. El Reglamento (UE) 2022/2065 y el Reglamento (UE) 2022/1925 proporcionan un marco regulador completo para garantizar entornos en línea seguros, predecibles y fiables para todos los usuarios finales de servicios en línea, y establecen condiciones de igualdad 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 materiales del Reglamento sobre las relaciones entre plataformas y empresas están ampliamente cubiertos por la Ley de Servicios Digitales y la Ley 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 digitales y los mercados digitales, al aproximar las medidas nacionales relativas a los requisitos que deben cumplir los proveedores de servicios de intermediación y a la contestabilidad y equidad de los servicios básicos de las plataformas prestados por los guardianes de acceso. A efectos de seguridad jurídica, determinadas definiciones del artículo 2, las disposiciones sobre restricciones y suspensiones del artículo 4, así como las relativas al sistema interno de tramitación de reclamaciones del artículo 11 del Reglamento (UE) 2019/1150, a las que se hace referencia en otros actos jurídicos, en particular la Directiva (UE) 2023/2831 sobre la mejora de las condiciones de trabajo en el trabajo en plataformas, y el artículo 15, que garantiza su aplicación, seguirán aplicándose temporalmente hasta que se modifiquen los actos originales.

(60) Dado el carácter técnico de las modificaciones propuestas en el presente Reglamento y la urgencia de establecer un marco jurídico simplificado, el presente Reglamento debe entrar en vigor inmediatamente después de su publicación en el Diario Oficial. Cuando proceda, deben concederse períodos transitorios a los Estados miembros y a las entidades reguladas para que se adapten a las normas.

[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, los órganos y los organismos de la Unión, y a la libre circulación de estos datos, y por el que se deroga 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).

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 queda modificado como sigue:

(a) en el apartado 1, se insertan los siguientes puntos:

«ea) el registro voluntario de los servicios de intermediación de datos;

eb) el registro voluntario de entidades que recopilan y tratan datos puestos a disposición con fines altruistas;

ec) el establecimiento de un Comité Europeo de Innovación en materia de Datos;

(ed) los requisitos de localización de datos y la disponibilidad de datos para las autoridades competentes;

ee) la reutilización de determinados datos y documentos en poder de organismos del sector público o de determinadas empresas públicas, así como de datos de investigación.

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

«g) El capítulo VII bis se aplica a los datos personales y no personales.

(h) El capítulo VII ter se aplica a cualquier dato no personal;

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

(i) documentos en poder de organismos del sector público de los Estados miembros a los que se refiere

(1) en el artículo 32 decies, apartado 1, letra a), o por empresas públicas, tal como se

(2) en 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 ter, apartado 1, letra a).»

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

«g) 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 que asignan, entre las autoridades públicas y los organismos de derecho público, competencias y responsabilidades en materia de tratamiento de datos sin remuneración contractual de particulares, así como de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que prevén la ejecución de dichas competencias y responsabilidades.

12. Cuando la legislación sectorial específica de la Unión o nacional exija a los organismos del sector público, a los proveedores de servicios de intermediación de datos o a las organizaciones reconocidas de altruismo de datos que cumplan requisitos técnicos, administrativos u organizativos adicionales específicos relacionados con los capítulos VII bis y VII ter, incluso mediante un régimen de autorización o certificación, también se aplicarán las disposiciones de dicha legislación sectorial específica de la Unión o nacional. Dichos requisitos adicionales específicos serán no discriminatorios, proporcionados y objetivamente justificados.

13. En 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 detalladas o estrictas, 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 siguientes puntos 4 bis), 4 ter) y 4 quater):

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

4 ter) «permiso»: el derecho que se concede a los usuarios de datos a tratar datos no personales;

4 quater) «acceso»: el uso de datos, de conformidad con requisitos técnicos, jurídicos u organizativos específicos, sin que ello implique necesariamente la transmisión o la descarga de datos;».

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

«13) «titular de los datos»: la persona física o jurídica que, de conformidad con el presente Reglamento, el Derecho de la Unión aplicable o la legislación nacional adoptada de conformidad con el Derecho de la Unión, tiene el derecho u obligación de utilizar o poner a disposición datos, incluidos, cuando así se haya acordado contractualmente, datos sobre productos o datos sobre servicios relacionados, que haya obtenido o generado durante la prestación de un servicio relacionado;

(c) Se insertan los siguientes puntos 28 bis) y 28 ter):

«28 bis) «organismos de derecho público»: los organismos que reúnen todas las características siguientes:

(a) se han creado con el fin específico de satisfacer necesidades de interés general, sin carácter industrial ni comercial;

(b) tienen personalidad jurídica;

(c) están financiados, en su mayor parte, por el Estado, las autoridades regionales o locales, u otros organismos de derecho público; o están sujetos a la supervisión de la gestión por parte de dichas autoridades u organismos; o tienen un consejo de administración, de gestión o de supervisión, más de la mitad de cuyos miembros son nombrados por el Estado, las autoridades regionales o locales, u otros organismos de derecho público;

(28 ter) «empresa pública»: cualquier empresa sobre la que un organismo del sector público pueda ejercer, directa o indirectamente, una influencia dominante en virtud de su propiedad, su participación financiera en ella o las normas que la rigen. Se presumirá la existencia de una influencia dominante

por parte de los organismos del sector público en cualquiera de los siguientes casos en los que dichos organismos, directa o indirectamente:

(a) posean la mayoría del capital suscrito de la empresa;

(b) controlan la mayoría de los votos correspondientes a las acciones emitidas por la empresa;

(c) puedan nombrar a más de la mitad de los miembros del órgano de administración, dirección o supervisión de la empresa;».

(d) Se insertan los siguientes puntos 38 bis) y 38 ter):

«38 bis) «servicio de intermediación de datos»: un servicio cuyo objetivo es establecer relaciones de carácter económico con fines de intercambio de datos entre un número indeterminado de interesados o titulares de datos y usuarios de datos, por medios técnicos, jurídicos o de otro tipo, incluso con el fin de ejercer los derechos de los interesados en relación con los datos personales, y que:

(1) no tiene como objetivo principal la intermediación de contenidos protegidos por derechos de autor;

(2) no son adquiridos conjuntamente por varias personas jurídicas para su uso exclusivo entre ellas;

38 ter) «altruismo de datos»: el intercambio voluntario de datos sobre la base del consentimiento de los interesados para tratar los datos personales que les conciernen, o de los permisos de los titulares de los datos para permitir el uso de sus datos no personales sin solicitar ni recibir una recompensa que vaya más allá de la compensación relacionada con los costes en que incurren cuando ponen sus datos a disposición para objetivos de interés general, tal como se establece en la legislación nacional, cuando proceda, como la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, la producción y la difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica con fines de interés general;».

(e) Se añaden los siguientes puntos 44) a 63):

«44) «mediana empresa»: una 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» o «SMC»: una pequeña empresa de mediana capitalización tal como se define en el artículo 2 del anexo de la Recomendación (UE) 2025/1099 de la Comisión;

(46) «universidad»: un organismo del sector público que imparte enseñanza superior postsecundaria conducente a la obtención de títulos académicos;

(47) «licencia estándar»: un conjunto de condiciones de reutilización predefinidas en formato digital, preferiblemente compatibles con las licencias públicas normalizadas disponibles en línea;

(48) «documento»:

(a) cualquier contenido no digital, independientemente de su soporte (papel o grabación sonora, visual o audiovisual); o

(b) cualquier parte de dicho contenido;

(50) «datos dinámicos»: datos y documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, en particular debido a su volatilidad u obsolescencia rápida; los datos generados por sensores se consideran normalmente datos dinámicos;

(51) «datos de investigación»: datos, distintos de las publicaciones científicas, que se recopilan o producen en el curso de actividades de investigación científica y se utilizan como prueba en el proceso de investigación, o que son comúnmente aceptados en la comunidad investigadora como necesarios para validar los hallazgos y resultados de la investigación;

(52) «Reutilización»: el uso por parte de personas físicas o jurídicas de documentos en poder de:

(a) organismos del sector público, con fines comerciales o no comerciales distintos de la finalidad inicial dentro de la función pública para la que se produjeron los documentos, salvo el intercambio de documentos entre organismos del sector público con el único fin de cumplir sus funciones públicas; o

(b) empresas públicas, con arreglo al capítulo VII quater, sección 2, con fines comerciales o no comerciales distintos del propósito inicial de prestar servicios de interés general para los que se produjeron los documentos, salvo el intercambio de documentos entre empresas públicas y organismos del sector público con el único fin de cumplir las funciones públicas de los organismos del sector público;

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

(54) «determinadas categorías de datos protegidos»: datos y documentos en poder de organismos del sector público que están protegidos por motivos de

(a) confidencialidad comercial, incluidos los secretos comerciales, profesionales y empresariales;

(b) la confidencialidad estadística;

(c) la protección de los derechos de propiedad intelectual de terceros; o

(d) la 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 que garantizan el cumplimiento del Derecho de la Unión, en particular en lo que respecta a los derechos de los interesados, los derechos de propiedad intelectual y la confidencialidad, integridad y accesibilidad comerciales y estadísticas, así como del Derecho nacional aplicable, y que permiten a la entidad que proporciona el entorno de tratamiento seguro determinar y supervisar todas las acciones de tratamiento de datos, incluida la visualización, el almacenamiento, la descarga y la exportación de datos y 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 en virtud del capítulo VII quater, o a investigar datos o determinadas categorías de datos protegidos;

(58) «formato legible por máquina»: un formato de archivo estructurado de tal manera que las aplicaciones de software puedan identificar, reconocer y extraer fácilmente datos específicos, incluidas declaraciones individuales de hechos, y su estructura interna;

(59) «formato abierto»: formato de archivo independiente de la plataforma y puesto a disposición del público sin ninguna restricción que impida la reutilización de documentos;

(60) «norma abierta formal»: una norma que se ha establecido por escrito y que detalla las especificaciones de los requisitos para garantizar la interoperabilidad del software;

(61) «rendimiento razonable de la inversión»: porcentaje del coste total, además del importe necesario para recuperar los costes subvencionables, que no supere en más de 5 puntos porcentuales el tipo de interés fijo del BCE;

(62) «requisito de localización de datos»: cualquier obligación, prohibición, condición, límite u otro requisito previsto en las disposiciones legales, reglamentarias o administrativas de un Estado miembro o resultante de prácticas administrativas generales y coherentes en un Estado miembro y en organismos de derecho público, incluido el ámbito de la contratación pública, sin perjuicio de lo dispuesto en la Directiva 2014/24/UE, que imponga el tratamiento de datos en el territorio de un Estado miembro específico u obstaculice el tratamiento de datos en cualquier otro Estado miembro;

(63) «seudonimización»: la seudonimización a que se refiere el artículo 4, apartado 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 titular de los datos que sea titular 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 por la divulgación de secretos comerciales o que la divulgación de secretos comerciales al usuario suponga un alto riesgo de adquisición, utilización o divulgación ilícitas a entidades de terceros países, o a 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 a la prevista en el Derecho de la Unión, dicho titular de los datos podrá denegar, caso por caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración se fundamentará debidamente en 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 y el carácter único y novedoso del producto relacionado. Se facilitará por escrito al usuario sin demora injustificada. Cuando el titular de los datos se niegue a compartirlos de conformidad con el presente apartado, lo notificará a la autoridad competente designada con arreglo al artículo 37.».

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

«11. En circunstancias excepcionales, cuando el titular de los datos que sea titular de secretos comerciales 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 por la divulgación de secretos comerciales o que la

divulgación de secretos comerciales al tercero supone un alto riesgo de adquisición, uso o divulgación ilícitos a entidades de terceros países, o a entidades establecidas en la Unión bajo el control directo o indirecto de dichas entidades, que están sujetas a jurisdicciones que ofrecen una protección más débil o no equivalente a la prevista en el Derecho de la Unión, dicho titular de los datos podrá denegar, caso por caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración se fundamentará debidamente en 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 y el carácter único y novedoso del producto relacionado. Se facilitará por escrito al tercero sin demora injustificada. Cuando el titular de los datos se niegue a compartirlos de conformidad con el presente apartado, lo notificará a la autoridad competente designada con arreglo al artículo 37.

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

**«PUESTA A DISPOSICIÓN DE LOS ORGANISMOS DEL SECTOR PÚBLICO, LA COMISIÓN, EL BANCO CENTRAL EUROPEO Y LOS ORGANISMOS DE LA UNIÓN DE DATOS POR MOTIVOS DE EMERGENCIA PÚBLICA»;**

6. Se suprimen los artículos 14 y 15.

7. Se inserta el siguiente artículo 15 bis:

«Artículo 15 bis

*Obligación de los titulares de datos de ponerlos a disposición en caso de 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 cumplir sus obligaciones legales en interés público al responder a una emergencia pública, mitigarla o apoyar la recuperación de la misma, podrá solicitar a los titulares de datos que sean personas jurídicas, distintas de los organismos del sector público, que pongan a disposición dichos datos, incluidos los metadatos necesarios para interpretarlos y utilizarlos. Previa solicitud debidamente motivada, los titulares de datos pondrán los datos y metadatos a disposición del organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión solicitante. También podrán presentarse solicitudes de este tipo cuando sea necesario elaborar 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, de conformidad con el apartado 1, no pueda obtenerlos por otros medios de manera oportuna y 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 datos personales y, cuando sea posible, ponerse a disposición en forma seudonimizada, con sujeción a las medidas técnicas y organizativas adecuadas para garantizar su protección.

3. Cuando los datos solicitados sean necesarios para mitigar o apoyar la recuperación de una emergencia pública, un organismo solicitante con arreglo al apartado 1 que actúe sobre la base del Derecho de la Unión o nacional podrá solicitar datos no personales específicos, cuya falta le impida mitigar o apoyar la recuperación de una emergencia pública. Dichas solicitudes no se dirigirán 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 organismos del sector público, la Comisión, el Banco Central Europeo u organismos de la Unión en relación con la prevención, investigación, detección o persecución de delitos penales o administrativos o la ejecución de sanciones penales, ni a la administración aduanera o fiscal. El presente capítulo no afecta al Derecho de la Unión o nacional que regula dichas actividades».

9. El artículo 17 se modifica como sigue:

(a) El apartado 1 se modifica como sigue:

(i) la frase introductoria se sustituye por el texto siguiente:

«Al solicitar datos con arreglo al artículo 15 bis, los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión:»;

(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, el uso previsto de los datos solicitados, incluido, en su caso, por un tercero de conformidad con el apartado 4 del presente artículo, la duración de dicho uso y, cuando proceda, cómo el tratamiento de los datos personales va a contribuir a hacer frente a la emergencia pública;»;

(b) el apartado 2 se modifica como sigue:

(i) la letra c) se sustituye por el texto siguiente:

«c) ser proporcionada a la emergencia pública y estar debidamente justificada, en lo que respecta a la granularidad y el volumen de los datos solicitados y la frecuencia de acceso a los mismos;»;

(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, la frase 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 titular de los datos podrá denegar o solicitar la modificación de una solicitud de puesta a disposición de datos en virtud del presente capítulo sin demora injustificada 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 injustificada y, en cualquier caso, a más tardar treinta días hábiles después de la recepción de una solicitud con arreglo al artículo 15 bis, apartado 3, por cualquiera de los motivos siguientes:»;

(b) se suprime el apartado 5;

11. El artículo 19 queda modificado como sigue:

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

«Los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión que reciban datos en virtud de una solicitud presentada con arreglo al artículo 15 bis:»;

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

«3. La divulgación de secretos comerciales a un organismo del sector público, a la Comisión, al Banco Central Europeo o a un organismo de la Unión solo será necesaria en la medida en que sea estrictamente necesario para alcanzar el objetivo de una solicitud con arreglo al artículo 15 bis. En tal caso, el titular de los datos o, cuando no sea la misma persona, el titular del secreto comercial, identificará los datos que están protegidos como secretos comerciales, incluidos los metadatos pertinentes. El organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, antes de la divulgación de secretos comerciales, adoptarán todas las medidas técnicas y organizativas necesarias y adecuadas para preservar la confidencialidad de los secretos comerciales, incluido, cuando proceda, 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 con arreglo al capítulo V*

1. Los titulares de datos pondrán a disposición, de forma gratuita, los datos necesarios para responder a una emergencia pública de conformidad con el 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 reconocerá públicamente al titular de los datos si este lo solicita.

2. El titular de los datos tendrá derecho a una compensación equitativa por la puesta a disposición de los datos en cumplimiento de una solicitud formulada de conformidad con el artículo 15 bis, apartado 3. Dicha compensación cubrirá los costes técnicos y organizativos en que se haya incurrido para cumplir la solicitud, incluidos, en su caso, los costes de anonimización, seudonimización, agregación y adaptación técnica, así como un margen razonable. A petición del organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, el titular de los datos facilitará información sobre la base de cálculo de los costes y el margen razonable.

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

4. Los poseedores de datos no tendrán derecho a compensación por poner a disposición datos en cumplimiento de una solicitud formulada con arreglo al artículo 15 bis, apartado 3, cuando la tarea específica realizada en interés público sea la elaboración de estadísticas oficiales y cuando la legislación nacional no permita la compra de datos. Los Estados miembros notificarán a la Comisión cuando la legislación 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 siguiente:

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

(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 con arreglo al apartado 1, lo notificará sin demora injustificada al titular de los datos de quien los haya recibido, indicando lo siguiente:

(a) la identidad y los datos de contacto de la organización o la 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, incluso cuando se trate de datos personales o secretos comerciales».

14. Se inserta el siguiente artículo 22 bis antes del capítulo VI:

Artículo 22 bis

*Derecho a presentar una reclamación*

Cuando surja un litigio en relación con una solicitud de datos en virtud del artículo 15 bis, incluida su denegación, modificación, el nivel de indemnización o la transmisión o puesta a disposición de datos, el titular de los 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, designada de conformidad con el artículo 37, del Estado miembro en el que esté establecido el titular de los datos.

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

«1 bis. Las obligaciones establecidas en el capítulo VI, con excepción del artículo 29, y en el artículo 34 no se aplicarán a los servicios de tratamiento de datos distintos de los contemplados en el artículo 30, apartado 1, cuando la mayoría de las características y funcionalidades del servicio de tratamiento de datos hayan sido adaptadas por el proveedor 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 esos servicios antes de su expiración si dicho contrato se celebró antes del 12 de septiembre de 2025. Cualquier disposición contractual contenida en ese contrato que sea contraria al artículo 29, apartados 1, 2 o 3, se considerará nula y sin efecto.

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

Cuando el proveedor de servicios de tratamiento de datos sea una pequeña o mediana empresa o una pequeña empresa de mediana capitalización, las obligaciones establecidas en el capítulo VI, con excepción del artículo 29, y en el artículo 34 no se aplicarán a los servicios de tratamiento de datos distintos de los contemplados 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.

Cuando el proveedor de un servicio de tratamiento de datos sea una pequeña o mediana empresa o una pequeña empresa de mediana capitalización, no estará obligado a renegociar o modificar un contrato de prestación de un servicio de tratamiento de datos distinto de

los contemplados en el artículo 30, apartado 1, antes de su expiración 1 si dicho contrato se celebró antes del 12 de septiembre de 2025 o en esa fecha. Cualquier disposición contractual contenida en dicho contrato que sea contraria al artículo 29, apartados 1, 2 o 3, se considerará nula y sin efecto».

16. El artículo 32 queda modificado 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 facilite 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 altruismo de datos adoptarán todas las medidas técnicas, organizativas y jurídicas adecuadas, incluidos los contratos, para impedir el acceso y la transferencia por parte de gobiernos internacionales y de terceros países de datos no personales conservados en la Unión, cuando dicha transferencia o acceso suponga un 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. Toda decisión o sentencia de un tribunal de un tercer país y toda decisión de una autoridad administrativa de un tercer país que exija a un proveedor de servicios de tratamiento de datos, al organismo del sector público que pone a disposición datos o documentos de conformidad con el capítulo VIIc, 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 VIIc, sección 3, un proveedor de servicios de intermediación de datos o una organización reconocida de altruismo de datos a transferir o dar acceso a datos no personales que entren en el ámbito de aplicación del presente Reglamento y se encuentren en la Unión, solo se reconocerá o será ejecutable de cualquier forma si se basa en un acuerdo internacional, como un tratado de asistencia judicial recíproca, vigente entre el tercer país solicitante y la Unión, o cualquier acuerdo de este tipo entre el tercer país solicitante y un Estado miembro».

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

«3. A falta de un acuerdo internacional como el mencionado en el apartado 2, cuando un proveedor de servicios de tratamiento de datos, el organismo del sector público que pone 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 altruismo de datos sea el destinatario de una resolución o sentencia de un tribunal o tribunal de un tercero 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 decisión o sentencia pudiera poner al destinatario en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro pertinente, la transferencia de dichos datos a la autoridad del tercer país o el acceso a los mismos solo tendrá lugar cuando:».

(c) 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 pone a disposición datos o documentos de conformidad con el capítulo VIIc, sección 3, la persona física o jurídica a la que

se le haya concedido el derecho a reutilizar datos o documentos de conformidad con el capítulo VIIc, sección 3, el proveedor de servicios de intermediación de datos o la organización reconocida de altruismo de datos proporcionarán la cantidad mínima de datos admisible 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 pertinente a que se refiere el párrafo 3, párrafo segundo.

5. El proveedor de servicios de tratamiento de datos, el organismo del sector público que pone a disposición datos o documentos de conformidad con el capítulo VIIc, 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 VIIc, sección 3, el proveedor de servicios de intermediación de datos o la organización de altruismo de datos reconocida informarán a la persona física o jurídica cuyos derechos e intereses puedan verse afectados de la existencia de una solicitud de una autoridad de un tercer país para acceder a sus datos antes de dar curso a dicha solicitud, salvo cuando la solicitud tenga fines policiales y durante el tiempo que sea necesario para preservar la eficacia de la actividad policial.

17. Se suprime el artículo 36.

18. Se insertan los siguientes capítulos VII bis, VII ter y VII quater:

**«CAPÍTULO VII bis**
**SERVICIOS DE INTERMEDIACIÓN DE DATOS Y ORGANIZACIONES DE ALTRUISMO DE DATOS»**

Artículo 32 bis

*Registros públicos de la Unión*

(1) La Comisión mantendrá y actualizará periódicamente registros públicos de la Unión de:

(a) los proveedores de servicios de intermediación de datos reconocidos y

(b) organizaciones de altruismo de datos reconocidas.

(2) Los proveedores de servicios de intermediación de datos inscritos en el registro público de la Unión mencionado en el apartado 1, letra a), podrán utilizar la etiqueta «proveedor de servicios de intermediación de datos reconocido en la Unión» en sus comunicaciones escritas y orales, así como el logotipo común mencionado en el apartado 4.

(3) Las organizaciones de altruismo de datos inscritas en el registro público de la Unión mencionado en el apartado 1, letra b), podrán utilizar la etiqueta «organización de altruismo de datos reconocida en la Unión» en sus comunicaciones escritas y orales, así como el logotipo común mencionado en el apartado 4.

(4) A fin de garantizar que los proveedores de servicios de intermediación de datos reconocidos en la Unión sean fácilmente identificables en toda la Unión, la Comisión estará facultada para adoptar actos de ejecución por los que se establezca el diseño del logotipo común. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento consultivo contemplado en el artículo 46, apartado 1 bis.

Artículo 32 ter

*Autoridades competentes para el registro de los proveedores de servicios de intermediación de datos y las organizaciones de altruismo de datos*

(1) Cada Estado miembro designará una o varias autoridades competentes responsables de la aplicación y el cumplimiento del presente capítulo, de conformidad con el artículo 37, apartado 1.

(2) Las autoridades competentes se establecerán de manera que se garantice su independencia respecto a cualquier proveedor de servicios de intermediación de datos reconocido o cualquier organización de altruismo de datos reconocida.

Artículo 32 quater

*Requisitos generales para el registro de los proveedores de servicios de intermediación de datos reconocidos*

Para poder inscribirse en el registro público de la Unión mencionado en el artículo 32 bis, apartado 1, letra a), un proveedor de servicios de intermediación de datos deberá cumplir todos los requisitos siguientes:

(a) no utilizar los datos para los que presta servicios de intermediación de datos con fines distintos a los de ponerlos a disposición de los usuarios de datos;

(b) los datos que recopile con respecto a cualquier actividad de una persona física o jurídica con el fin de prestar el 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 utiliza el servicio de intermediación de datos, se utilizarán únicamente para el desarrollo de dicho servicio de intermediación de datos;

(c) cuando ofrezcan herramientas y servicios adicionales a los titulares de los datos o a los interesados con el fin específico de facilitar el intercambio de datos, tales como el almacenamiento temporal, la conservación, la conversión, el cifrado, la anonimización y la seudonimización, dichas herramientas y servicios se utilicen únicamente a petición explícita o con la aprobación del titular de los datos o del interesado;

(d) 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 mencionados en la letra c), cumplan las siguientes condiciones:

  (i) los servicios de valor añadido son solicitados explícitamente por el usuario;

  (ii) los datos no se utilizan para fines distintos de la prestación del servicio de valor añadido;

  (iii) los servicios de valor añadido se ofrecen a través de una entidad funcionalmente independiente;

  (iv) la empresa que desea ofrecer los servicios de valor añadido no está designada como guardián de acceso con arreglo al artículo 3 del Reglamento (UE) 2022/1925;

  (v) las condiciones comerciales, incluidos los precios, para la prestación de servicios de intermediación de datos a un titular o usuario de datos no dependen de que el titular o usuario de datos utilice servicios de valor añadido prestados por el proveedor de servicios de intermediación de datos o por una entidad relacionada;

(e) el proveedor de servicios de intermediación de datos que ofrece servicios a los interesados actúa en el mejor interés de estos cuando facilita el ejercicio de sus derechos, en particular informando y, cuando proceda, asesorando a los interesados de manera concisa, transparente, inteligible y fácilmente accesible sobre los usos previstos de los datos por parte de los usuarios de datos y las condiciones generales asociadas a dichos usos antes de que los interesados den su consentimiento.

Artículo 32 quinquies

*Requisitos generales para el registro de organizaciones reconocidas de altruismo de datos*

Para poder inscribirse en el registro público de la Unión mencionado en el artículo 32 bis, apartado 1, letra b), una organización de altruismo de datos deberá cumplir todos los requisitos siguientes:

(a) realizar actividades de altruismo de datos;

(b) ser una persona jurídica constituida con arreglo al Derecho nacional para alcanzar objetivos de interés general previstos en el Derecho nacional, cuando proceda;

(c) operar sin ánimo de lucro y ser jurídicamente independiente de cualquier entidad que opere con ánimo de lucro;

(d) que lleve a cabo sus actividades de altruismo de datos a través de una estructura funcionalmente separada de sus otras 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 altruismo de datos 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 de altruismo de datos reconocidas 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 altruismo de datos que no tengan un establecimiento principal en la Unión designarán a un representante legal en uno de los Estados miembros. El representante legal estará facultado para ser contactado, además del proveedor de servicios de intermediación de datos o la organización de altruismo de datos, o en su lugar, por las autoridades competentes o los interesados y los titulares de los datos. El representante legal cooperará con la autoridad competente y le demostrará de manera exhaustiva, previa solicitud, las medidas adoptadas y las disposiciones establecidas por el proveedor de servicios de intermediación de datos o la organización de altruismo de datos para garantizar el cumplimiento del presente Reglamento.

Se considerará que el proveedor de servicios de intermediación de datos o la organización de altruismo de datos están bajo la jurisdicción del Estado miembro en el que se encuentre el representante legal. El nombramiento de un representante legal se entenderá sin perjuicio de cualquier acción legal que pueda iniciarse contra el proveedor de servicios de intermediación de datos o la organización de altruismo de datos.

(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 de conformidad con el apartado 3 del presente artículo y cumpla los requisitos establecidos en el artículo 32 quater, la autoridad competente, en un plazo de doce semanas a partir de la recepción de la solicitud de registro, decidirá si el proveedor cumple los criterios establecidos en el artículo 32 quater. Si el proveedor cumple los criterios, la autoridad competente presentará la información pertinente

información pertinente a la Comisión, que inscribirá a los proveedores en el registro público de la Unión como proveedores de servicios de intermediación de datos reconocidos.

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

El registro en el registro público de la Unión será válido en todos los Estados miembros.

(5) La autoridad competente podrá cobrar tasas por el registro de conformidad con la legislación nacional. Dichas tasas serán proporcionadas y objetivas y se basarán en los costes administrativos relacionados con el control del cumplimiento. En el caso de las pequeñas y medianas empresas, las empresas de pequeña y mediana capitalización y las empresas emergentes, la autoridad competente podrá cobrar una tasa reducida o eximir del pago de la misma.

(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 altruismo de datos en la Unión.

(7) La autoridad competente notificará sin demora y por medios electrónicos a la Comisión cualquier notificación realizada con arreglo al apartado 6. La Comisión actualizará sin demora injustificada el registro público de la Unión.

Artículo 32 septies

*Obligaciones de las organizaciones de altruismo de datos reconocidas*

(1) Las organizaciones de altruismo de datos reconocidas informarán a los interesados o a los titulares de los datos, antes de cualquier tratamiento de sus datos, de manera clara y fácilmente comprensible, de lo siguiente:

(a) los objetivos de interés general y, en su caso, la finalidad específica, explícita y legítima para la que se tratarán los datos personales y para la que se permite el tratamiento de sus datos por parte de un usuario de datos;

(b) la ubicación del tratamiento y los objetivos de interés general para los que permite cualquier tratamiento realizado en un tercer país, cuando el tratamiento lo lleve a cabo la organización reconocida de altruismo de datos.

(2) Las organizaciones de altruismo de datos reconocidas no utilizarán los datos para fines distintos de los objetivos de interés general para los que el interesado o el titular de los datos permite el tratamiento. La organización de altruismo de datos reconocida no utilizará prácticas comerciales engañosas para solicitar el suministro de datos.

(3) Las organizaciones de altruismo de datos reconocidas proporcionarán medios electrónicos para obtener el consentimiento de los interesados o los permisos para tratar los datos facilitados por los titulares de los datos, así como para su retirada.

(4) Las organizaciones de altruismo de datos reconocidas informarán sin demora a los titulares de los datos en caso de cualquier transferencia, acceso o uso no autorizado de los datos no personales que haya compartido.

(5) Cuando las organizaciones de altruismo de datos reconocidas faciliten el tratamiento de datos por parte de terceros, incluso proporcionando herramientas para obtener el consentimiento de los interesados o los permisos para tratar los datos facilitados por los titulares de los datos, especificarán, cuando proceda, el tercer país en el que se prevé utilizar los datos.

Artículo 32 octies

*Control del cumplimiento*

(1) Las autoridades competentes a que se refiere el artículo 32 ter supervisarán y controlarán, 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 de altruismo de datos reconocidas cumplen los requisitos establecidos en el presente capítulo, incluido 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 de altruismo de datos reconocidas, o a su representante legal, toda la información necesaria para verificar el cumplimiento de los requisitos establecidos en el presente capítulo. Toda solicitud de información será proporcionada al desempeño de la tarea y estará motivada.

(3) Cuando una autoridad competente constate que un proveedor de servicios de intermediación de datos reconocido o una organización de altruismo de datos reconocida no cumple uno o varios de los requisitos establecidos en el presente capítulo, notificará a dicha entidad, o a su representante legal, dichas constataciones y le dará la oportunidad de exponer su punto de vista en un plazo de 30 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, ya sea de forma inmediata o en un plazo razonable, y adoptará las medidas adecuadas y proporcionadas con el fin de garantizar el cumplimiento.

(5) Si un proveedor de servicios de intermediación de datos reconocido o una organización de altruismo de datos reconocida no cumple uno o varios de los requisitos establecidos en el presente capítulo, incluso después de haber sido notificado de conformidad con el apartado 3, dicha entidad:

(a) perderá su derecho a utilizar la etiqueta a que se refiere el artículo 32 bis en las comunicaciones escritas y orales;

(b) será eliminada del registro público de la Unión mencionado en el artículo 32 bis.

Cualquier decisión por la que se revoque el derecho a utilizar la etiqueta a que se refiere el párrafo primero, letra a), será hecha pública por la autoridad competente.

## «CAPÍTULO VII ter

## Libre circulación de datos no personales en la Unión»

«Artículo 32 nonies

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

(1) Se prohibirán los requisitos de localización de datos no personales, salvo que estén justificados por razones de seguridad pública, de conformidad con el principio de proporcionalidad, o se establezcan 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 un requisito de localización de datos 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 en poder de organismos del sector público

## SECCIÓN 1

## DISPOSICIONES

### GENERALES

Artículo 32i

*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 lo siguiente:

(a) los datos y documentos existentes en poder de organismos del sector público de los Estados miembros, incluidas determinadas categorías de datos protegidos;

(b) los datos y documentos existentes en poder de empresas públicas que:

(i) que operan en los ámbitos contemplados en el capítulo II de la Directiva 2014/25/UE del Parlamento Europeo y del Consejo;

(ii) actúan como operadores de servicios públicos de conformidad con el artículo 2 del Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo;

(iii) que actúan como compañías aéreas que cumplen obligaciones de servicio público de conformidad con el artículo 16 del Reglamento (CE) n.º 1008/2008 del Parlamento Europeo y del Consejo; o

(iv) actuar como armadores comunitarios que cumplen obligaciones de servicio público de conformidad con el artículo 4 del Reglamento (CEE) n.º 3577/92 del Consejo;

(c) datos de investigación de conformidad con las condiciones establecidas en el artículo 32 terdecies.

(2) El presente capítulo no se aplica a lo siguiente:

(a) los datos y documentos cuyo suministro sea una actividad que no entre en el ámbito de la función pública de los organismos del sector público de que se trate, tal como se define en la legislación u otras normas vinculantes del Estado miembro o, en ausencia de tales normas, tal como se define de conformidad con la práctica administrativa habitual en el Estado miembro en cuestión, siempre que el ámbito de las funciones públicas sea transparente y esté sujeto a revisión;

(b) los datos y documentos en poder de empresas públicas y:

(i) producidos fuera del ámbito de la prestación de servicios de interés general, tal como se definen en la legislación u otras normas vinculantes del Estado miembro;

(ii) relacionados con actividades directamente expuestas a la competencia y que, por lo tanto, de conformidad con el artículo 34 de la Directiva 2014/25/UE, no están sujetos a las normas de contratación pública;

(c) los datos y documentos, como los datos sensibles, cuyo acceso está excluido en virtud de los regímenes de acceso del Estado miembro por motivos de protección de la seguridad nacional (es decir, la seguridad del Estado), la defensa o la seguridad pública;

(d) los datos y documentos en poder de los organismos públicos de radiodifusión y sus filiales, así como 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 aplica a:

(a) los datos o documentos, como los datos o documentos sensibles, que están excluidos del acceso en virtud de los regímenes de acceso del Estado miembro, en particular por motivos de:

(i) confidencialidad estadística;

(ii) confidencialidad comercial (incluidos los secretos comerciales, profesionales o de la empresa );

(b) datos o documentos cuyo acceso esté restringido en virtud de los regímenes de acceso de los Estados miembros,

(i) incluidos los casos en los que los ciudadanos o las personas jurídicas deben demostrar un interés particular para obtener acceso a los documentos;

(ii) por motivos de protección de datos personales, y partes de datos o documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya sido definida por la ley como incompatible con la legislación relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales o que socave la protección de la intimidad y la integridad de la persona, en particular de conformidad con la legislación de la Unión o nacional en materia de protección de datos personales; logotipos, escudos e insignias;

(c) datos o documentos sobre los que terceros ostenten derechos de propiedad intelectual;

(d) los datos o documentos en poder de establecimientos culturales distintos de las bibliotecas, incluidas las bibliotecas universitarias, los museos y los archivos;

(e) los datos o documentos en poder de centros de enseñanza secundaria y de nivel inferior y, en el caso de todos los demás centros de enseñanza, los datos distintos de los mencionados 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 organismos de investigación y organismos de financiación de la investigación, incluidos los organismos creados para la transferencia de los resultados de la investigación;

(g) los datos o documentos cuyo acceso esté excluido o restringido por motivos de protección de información crítica sobre entidades o infraestructuras críticas, tal como se define en los puntos 1 y 4 del artículo 2 de la Directiva (UE) 2022/2557.

(4) La sección 3 del presente capítulo no se aplica a:

(a) los datos y documentos que no sean determinadas categorías de datos protegidos;

(b) los datos o documentos en poder de empresas públicas;

(c) los datos o documentos en poder de establecimientos culturales y centros educativos;

(d) los datos y documentos contemplados en la sección 2 del presente capítulo.

(5) El presente capítulo se basa en los regímenes de acceso de la Unión y nacionales, y se entiende sin perjuicio de los mismos, 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 la 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 los 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 (WCT).

(7) El derecho del creador de una base de datos previsto en el artículo 7, apartado 1, de la Directiva 96/9/CE no será ejercido por los organismos del sector público con el fin de impedir la reutilización de datos y documentos o de restringirla más allá de los límites establecidos en el presente capítulo.

(8) El presente capítulo regula la reutilización de datos y documentos existentes en poder de organismos del sector público y 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 entiende sin perjuicio del Derecho de la Unión y nacional y de los acuerdos internacionales en los que la Unión o los Estados miembros sean parte en materia de protección de las categorías de datos o documentos a que se refiere el artículo 2, apartado 54.

Artículo 32 undecies

*No discriminación*

(1) Las condiciones aplicables a la reutilización de datos o documentos serán no discriminatorias, transparentes, proporcionadas y objetivamente justificadas en lo que respecta a las categorías de datos o documentos y a los fines de la reutilización, así como a la naturaleza de los datos o documentos cuya reutilización se permite. Dichas condiciones no se utilizarán 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 insumo para sus actividades comerciales que no entran en el ámbito de sus funciones públicas, se aplicarán a la suministro de los datos o documentos para esas actividades los mismos cargos y otras condiciones que se aplican a otros reutilizadores.

Artículo 32k

*Acuerdos exclusivos*

(1) La reutilización de datos o documentos estará abierta a todos los agentes potenciales del mercado, incluso si uno o varios agentes del mercado ya explotan productos de valor añadido basados en dichos datos o documentos. Quedan prohibidos los acuerdos u otros arreglos 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, arreglos 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 en que

sea necesario para la prestación del servicio o el suministro del producto en las siguientes condiciones:

(a) el derecho exclusivo se conceda mediante un acto administrativo o un acuerdo contractual de conformidad con el Derecho de la Unión y el Derecho nacional aplicables y respetando los principios de transparencia, igualdad de trato y no discriminación.

(b) los acuerdos por los que se concede el derecho exclusivo, incluidas las razones por las que es necesario conceder dicho derecho, sean transparentes y se pongan a disposición del público en línea, en una forma que se ajuste al Derecho de la Unión aplicable en materia de contratación pública y al Derecho nacional.

(c) Salvo en el caso de los derechos exclusivos relacionados con la digitalización de recursos culturales, la validez de la razón para conceder derechos exclusivos sobre datos y documentos dentro del ámbito de aplicación de la sección 2 estará sujeta a una 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 definitivas de dichos acuerdos serán transparentes y se pondrán a disposición del público en línea.

(3) No obstante lo dispuesto en el apartado 1, cuando un derecho exclusivo se refiera a la digitalización de recursos culturales, el período de exclusividad no excederá, en general, de diez años. Cuando dicho período exceda de diez años, su duración se ajustará a la legislación aplicable de la Unión y nacional, sin perjuicio de su revisión durante el undécimo año y, en su caso, cada siete años a partir de entonces.

(4) En el caso de un derecho exclusivo contemplado en el apartado 3, se facilitará gratuitamente al organismo del sector público interesado una copia de los recursos culturales digitalizados como parte de dichos acuerdos. Dicha copia estará disponible para su reutilización al término del período de exclusividad.

(5) Para determinadas categorías de datos protegidos, la duración del derecho exclusivo de reutilización de los datos no excederá de doce meses. Cuando se celebre un contrato, la duración del mismo será la misma que la del derecho exclusivo.

(6) Los acuerdos u otros acuerdos o prácticas que, sin conceder expresamente un derecho exclusivo, tengan por objeto o puedan razonablemente dar lugar a una disponibilidad restringida para la reutilización de datos y documentos dentro del ámbito de aplicación de la sección 2 por parte de entidades distintas de las partes en dichos acuerdos, se pondrán a disposición del público en línea al menos dos meses antes de su entrada en vigor. El efecto de dichos acuerdos jurídicos o prácticos sobre la disponibilidad de los datos para su reutilización se someterá a revisiones periódicas y, en cualquier caso, se revisará cada tres años. Las condiciones definitivas de dichos acuerdos serán transparentes y se publicarán en línea.

(7) En el caso de los acuerdos exclusivos existentes, se aplicará lo siguiente:

(a) los acuerdos exclusivos relativos a datos y documentos incluidos en el ámbito de aplicación de la sección 2, existentes a 17 de julio de 2013, que no puedan acogerse a las excepciones establecidas en los apartados 2 y 3 y que hayan sido celebrados por organismos del sector público, se rescindirán al término del contrato y, en cualquier caso, a más tardar el 18 de julio de 2043;

(b) los acuerdos exclusivos relativos a datos y documentos incluidos en el ámbito de aplicación de la sección 2, vigentes a 16 de julio de 2019, que no puedan acogerse a las excepciones establecidas

en los apartados 2 y 3, y que hayan sido celebrados por empresas públicas, se rescindirán al término del contrato y, en cualquier caso, a más tardar el 17 de julio de 2049;

Artículo 32 terdecies

*Principios generales relativos a la tarificación*

(1) Cualquier tarifa establecida en virtud de la sección 2 o la sección 3 será transparente, no discriminatoria, proporcionada y objetivamente justificada, y no restringirá la competencia.

(2) En el caso de las tasas estándar por la reutilización de datos o documentos, las condiciones aplicables y el importe real de dichas tasas, incluida la base de cálculo de las mismas, se establecerán por adelantado y se publicarán, a ser posible y cuando proceda, por medios electrónicos.

(3) En el caso de los cargos por la reutilización distintos de los mencionados en el apartado 1, se indicarán desde el principio los factores que se tienen en cuenta en el cálculo de dichos cargos. Previa solicitud, el titular de los datos o documentos en cuestión indicará también la forma en que se han calculado dichos cargos en relación con una solicitud de reutilización específica.

(4) Los organismos del sector público velarán por que los cargos también puedan pagarse en línea a través de servicios de pago transfronterizos ampliamente disponibles, sin discriminación por el lugar de establecimiento del proveedor de servicios de pago, el lugar de emisión del instrumento de pago o la ubicación de la cuenta de pago dentro de la Unión.

Artículo 32 septodecies

*Información sobre las vías de recurso*

Los organismos del sector público velarán por que los solicitantes de reutilización de datos o documentos sean informados de las vías de recurso disponibles en relación con las decisiones o prácticas que les afecten.

## SECCIÓN 2

## REUTILIZACIÓN DE DATOS GUBERNAMENTALES ABIERTOS

Subsección 1 Ámbito de aplicación y principios

generales Artículo 32n

*Principio general para la reutilización de datos abiertos del gobierno*

(1) Los datos o documentos incluidos en el ámbito de aplicación de la presente sección serán reutilizables con 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 sobre los que las bibliotecas, incluidas las bibliotecas universitarias, los museos y los archivos, ostenten derechos de propiedad intelectual, y en el caso de los datos o documentos en poder de empresas públicas, cuando se permita la reutilización de dichos datos o documentos, estos serán reutilizables con fines comerciales o no comerciales, de conformidad con la sección 1 y la sección 2, subsección 3.

Subsección 2

Solicitudes de reutilización

Artículo 32o

*Tramitación de las solicitudes de reutilización*

(1) Los organismos del sector público tramitarán las solicitudes de reutilización, por medios electrónicos siempre que sea posible y adecuado, y pondrán el documento a disposición del solicitante para su reutilización o, si se necesita una licencia, finalizarán la oferta de licencia al solicitante en un plazo razonable que sea coherente con los plazos establecidos para la tramitación de las solicitudes de acceso a datos o documentos.

(2) Cuando no se hayan establecido plazos u otras normas que regulen la entrega oportuna de datos o documentos, los organismos del sector público tramitarán la solicitud y entregarán los datos o documentos para su reutilización al solicitante o, si se necesita una licencia, finalizarán la oferta de licencia al solicitante lo antes posible y, en cualquier caso, en un plazo de veinte días hábiles a partir de la recepción. Ese plazo podrá prorrogarse otros veinte días hábiles en caso de solicitudes extensas o complejas. En tales casos, se notificará al solicitante lo antes posible, y en cualquier caso en un plazo de tres semanas a partir de la solicitud inicial, que se necesita más tiempo para tramitar la solicitud y se le comunicarán los motivos.

(3) En caso de decisión negativa, los organismos del sector público comunicarán al solicitante los motivos de la denegación basándose en las disposiciones pertinentes del régimen de acceso de ese Estado miembro o en las disposiciones del presente Reglamento, en particular las letras a) a c) del apartado 2 del artículo 32 decies y las letras a) a d) del apartado 3 del artículo 32 decies o el artículo 32 novodecies (sección de principios generales de la ODD). Cuando una decisión negativa se base 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, si se conoce, o, en su defecto, al licenciante del que el organismo del sector público haya obtenido el material pertinente. Las bibliotecas, incluidas las bibliotecas universitarias, los museos y los archivos, no estarán obligados a incluir dicha referencia.

(4) Las vías de recurso incluirán la posibilidad de revisión por un órgano de revisión imparcial con los conocimientos especializados adecuados, como la autoridad nacional de competencia, la autoridad competente en materia de acceso a datos o documentos, la autoridad de control establecida de conformidad con el Reglamento (UE) 2016/679 o una autoridad judicial nacional, cuyas decisiones sean vinculantes para el organismo del sector público en cuestión.

(5) A los efectos del presente artículo, los Estados miembros establecerán disposiciones prácticas para facilitar la reutilización efectiva de los datos o documentos. Dichas disposiciones podrán incluir, en particular, los medios para facilitar información adecuada sobre los derechos previstos en el presente Reglamento y para ofrecer la asistencia y orientación pertinentes.

(6) El presente artículo no se aplicará a las siguientes entidades:

(a) empresas públicas;

(b) centros educativos, organismos de investigación y organismos de financiación de la investigación.

Subsección 3

Condiciones para la

reutilización Artículo 32 septies

*Formatos disponibles*

(1) Sin perjuicio de lo dispuesto en la subsección 5, los organismos del sector público y las empresas públicas pondrán a disposición sus datos o documentos en cualquier formato o idioma preexistente y, cuando sea posible y apropiado, por medios electrónicos, en formatos abiertos, legibles por máquina, accesibles, localizables y reutilizables, junto con sus metadatos. Tanto el formato como los metadatos deberán, en la medida de lo posible, cumplir con las normas abiertas formales.

(2) Los Estados miembros animarán a los organismos del sector público y a las empresas públicas a producir y poner a disposición datos o documentos que entren en el ámbito de aplicación de la presente sección, de conformidad con el principio de «abierto por diseño y por defecto».

(3) El apartado 1 no implicará la obligación de que los organismos del sector público creen o adapten datos o documentos o faciliten extractos para cumplir lo dispuesto en dicho apartado cuando ello suponga un esfuerzo desproporcionado que vaya más allá de una simple operación.

(4) No se exigirá a los organismos del sector público que continúen produciendo y almacenando un determinado tipo de documento con vistas a la reutilización de dichos datos o documentos por parte de una organización del sector público o privado.

(5) Los organismos del sector público pondrán a disposición los datos dinámicos para su reutilización inmediatamente después de su recogida, a través de API adecuadas y, cuando proceda, mediante descarga masiva.

(6) Cuando la puesta a disposición de datos dinámicos para su reutilización inmediatamente después de su recogida, tal como se menciona en el apartado 5, supere las capacidades financieras y técnicas del organismo del sector público, lo que supondría un esfuerzo desproporcionado, dichos 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 existentes en poder de empresas públicas que estén disponibles para su reutilización.

(8) Los conjuntos de datos de alto valor, enumerados de conformidad con el artículo 32 quinquies, apartado 1, se pondrán a disposición para su reutilización en formato legible por máquina, a través de interfaces de programación de aplicaciones (API) adecuadas y, cuando proceda, como descarga masiva.

Artículo 32 octies

*Principios que rigen la tarificación de los datos públicos abiertos*

(1) La reutilización de datos o documentos dentro del ámbito de aplicación de la presente sección será gratuita. No obstante, se podrá permitir que el organismo del sector público que posea los datos recupere los costes marginales incurridos por la reproducción, el suministro y la difusión de dichos datos o documentos, así como por la anonimización de los datos personales y las medidas adoptadas para proteger la información comercialmente confidencial.

(2) El apartado 1 no se aplicará a las siguientes entidades:

(a) los organismos del sector público que estén obligados a generar ingresos para cubrir una parte sustancial de los costes relacionados con el desempeño de sus funciones públicas;

(b) bibliotecas, incluidas las bibliotecas universitarias, museos y archivos;

(c) empresas públicas.

(3) Los Estados miembros publicarán en línea una lista de los organismos del sector público a que se refiere el apartado 2, letra a).

(4) En los casos contemplados en el apartado 2, letras a) y c), el importe total de las tasas se calculará con arreglo a criterios objetivos, transparentes y verificables. Dichos

criterios serán establecidos por los Estados miembros. Los ingresos totales procedentes del suministro y la autorización de la reutilización de datos o documentos durante el período contable correspondiente no superarán el coste de su recogida, producción, reproducción, difusión y almacenamiento, junto con un rendimiento razonable de la inversión y, en su caso, la anonimización de los datos personales y las medidas adoptadas para proteger la información comercialmente confidencial. Los cargos se calcularán de conformidad con los principios contables aplicables.

(5) Cuando los organismos del sector público a que se refiere el apartado 2, letra b), cobren tasas, los ingresos totales procedentes del suministro y la autorización de reutilización de datos o documentos durante el período contable correspondiente no superarán el coste de la recogida, producción, reproducción, difusión, almacenamiento de datos, conservación y obtención de derechos y, en su caso, la anonimización de datos personales y las medidas adoptadas para proteger la información comercialmente confidencial, junto con un rendimiento razonable de la inversión. Los cargos se calcularán de conformidad con los principios contables aplicables a los organismos del sector público implicados.

(6) Los organismos del sector público podrán fijar tasas más elevadas para la reutilización de datos y documentos por parte de empresas muy grandes que las previstas en los apartados 1, 4 y 5. Dichas 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 datos en virtud del Reglamento (UE) 2022/1925. Además de los elementos enumerados en el apartado 1 del presente artículo, dichos cargos podrán cubrir los costes de recopilación, producción, reproducción, difusión y almacenamiento de datos y, en su caso, los costes de anonimización o de medidas para proteger la confidencialidad de los datos o documentos, junto con un rendimiento razonable de la inversión.

(7) La reutilización de los siguientes datos será gratuita para el usuario:

(a) sin perjuicio de lo dispuesto en el artículo 32 quinquies, apartados 3, 4 y 5, los conjuntos de datos de alto valor, enumerados de conformidad con el apartado 1 de dicho artículo;

(b) los datos de investigación a que se refiere el artículo 32 decies, apartado 1, letra c).

Artículo 32 octies

*Licencias estándar*

(1) La reutilización de datos o documentos no estará sujeta a condiciones, salvo que dichas condiciones sean objetivas, proporcionadas, no discriminatorias y justificadas por motivos de interés público.

(2) Cuando la reutilización esté sujeta a condiciones, estas no restringirán innecesariamente las posibilidades de reutilización y no se utilizarán para restringir la competencia.

(3) En los Estados miembros en los que se utilicen licencias, los organismos del sector público velarán por que las licencias estándar para la reutilización de datos o documentos del sector público, que puedan adaptarse para satisfacer solicitudes de licencia específicas, estén disponibles en formato digital y puedan procesarse electrónicamente.

(4) Los organismos del sector público podrán establecer condiciones especiales para la reutilización de datos y documentos por parte de empresas de gran tamaño. Dichas condiciones serán proporcionadas y se basarán en criterios objetivos. Se establecerán teniendo en cuenta el poder económico o la capacidad de la entidad para adquirir datos, incluida, en particular, la designación como guardián de acceso en virtud del Reglamento (UE) 2022/1925.

Artículo 32 septies

*Disposiciones prácticas*

(1) Los Estados miembros adoptarán disposiciones prácticas que faciliten la búsqueda de datos o documentos disponibles para su reutilización, tales como listas de activos de datos o documentos principales con metadatos pertinentes, accesibles, cuando sea posible y apropiado, en línea y en formato legible por máquina, y sitios web que estén vinculados a las listas de activos. Siempre que sea posible, los Estados miembros facilitarán la búsqueda multilingüe de datos o documentos, en particular permitiendo la agregación de metadatos a escala de la Unión.

Los Estados miembros también animarán a los organismos del sector público a adoptar disposiciones prácticas que faciliten la conservación de los datos o documentos disponibles para su reutilización.

(2) Los Estados miembros, en cooperación con la Comisión, proseguirán sus esfuerzos para simplificar el acceso a los conjuntos de datos, en particular proporcionando un punto de acceso único y poniendo progresivamente a disposición conjuntos de datos adecuados en poder de organismos del sector público en relación con los datos o documentos a los que se aplica la presente sección, así como datos en poder de las instituciones de la Unión, en formatos accesibles, fácilmente localizables y reutilizables por medios electrónicos.

Subsección 4

Datos de

investigación

Artículo 32 ter

*Decisión del 18 de*

*diciembre de 2018*

(1) Los Estados miembros apoyarán la disponibilidad de los datos de investigación mediante la adopción de políticas nacionales
políticas y medidas pertinentes destinadas a que los datos de investigación financiados con fondos públicos estén disponibles de forma abierta («políticas de acceso abierto»), siguiendo el principio de «abierto por defecto» y en consonancia con los principios FAIR. En ese contexto, se tendrán en cuenta las preocupaciones relacionadas con los derechos de propiedad intelectual, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos, de conformidad con el principio de «tan abierto como sea posible, tan cerrado como sea necesario». Dichas políticas de acceso abierto se dirigirán a las organizaciones que realizan investigaciones y a las organizaciones que financian la investigación.

(2) Sin perjuicio de lo dispuesto en el artículo 32 quindecies, apartado 3, letra d), los datos de investigación serán reutilizables con fines comerciales o no comerciales de conformidad con la sección 1 y la sección 2, subsección 3, en la medida en que hayan sido financiados con fondos públicos y los investigadores, las organizaciones que realizan investigaciones o las organizaciones que financian la investigación ya los hayan puesto a disposición del público a través de un repositorio institucional o temático. En ese contexto, se tendrán 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 32u

*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, con el fin de modificar el anexo I añadiendo nuevas categorías temáticas de conjuntos de datos de alto valor que reflejen la evolución tecnológica y del mercado.

Artículo 32 quinquies

*Conjuntos de datos específicos de alto valor y disposiciones para su publicación y reutilización*

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

Dichos conjuntos de datos específicos de alto valor serán:

(a) disponibles de forma gratuita, sin perjuicio de lo dispuesto en los apartados 3, 4 y 5;

(b) legibles por máquina;

(c) proporcionados a través de API; y

(d) proporcionados como descarga masiva, cuando proceda.

Dichos actos de ejecución podrán especificar las modalidades de publicación y reutilización de conjuntos de datos de alto valor. Dichas modalidades serán compatibles con las licencias de estándar abierto.

Las modalidades podrán incluir condiciones aplicables a la reutilización, formatos de datos y metadatos y disposiciones técnicas para la difusión. Se tendrán en cuenta las inversiones realizadas por los Estados miembros en enfoques de datos abiertos, como las inversiones en el desarrollo y la implantación de determinadas normas, y se sopesarán con los posibles beneficios de la inclusión en la lista.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 46, apartado 2.

(2) La identificación de conjuntos de datos específicos de alto valor con arreglo al apartado 1 se basará en la evaluación de su potencial para:

(a) generar beneficios socioeconómicos o medioambientales significativos y servicios innovadores;

(b) beneficiar a un gran número de usuarios, en particular a las pymes y las microempresas;

(c) contribuir a la generación de ingresos; y

(d) combinarse con otros conjuntos de datos.

A efectos de identificar dichos conjuntos de datos específicos de alto valor, la Comisión llevará a cabo las consultas oportunas, incluso a nivel de expertos, realizará 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, en lo que respecta a la reutilización de datos o documentos. Dicha evaluación de impacto incluirá un análisis de costes y beneficios y un análisis de si el hecho de que los organismos del sector público que están obligados a generar ingresos para cubrir una parte sustancial de los costes relacionados con el desempeño de sus funciones públicas proporcionen conjuntos de datos de alto valor de forma gratuita tendría un impacto sustancial en el presupuesto de dichos organismos. Por lo que se refiere a los conjuntos de datos de alto valor en poder de empresas públicas, la evaluación de impacto prestará especial atención al papel de las empresas públicas en un entorno económico competitivo.

(3) No obstante lo dispuesto en el apartado 1, párrafo segundo, letra a), los actos de ejecución a que se refiere dicho apartado dispondrán que la disponibilidad gratuita de conjuntos de datos de alto valor no se aplique a conjuntos de datos de alto valor específicos en poder

por empresas públicas cuando ello suponga un falseamiento de la competencia en los mercados pertinentes.

(4) El requisito de poner a disposición de forma gratuita los conjuntos de datos de alto valor con arreglo a la letra a) del párrafo segundo del apartado 1 no se aplicará a las bibliotecas, incluidas las bibliotecas universitarias, los museos y los archivos.

(5) Cuando la puesta a disposición gratuita de conjuntos de datos de alto valor por parte de organismos del sector público que están obligados a generar ingresos para cubrir una parte sustancial de sus costes relacionados con el desempeño de sus funciones públicas tenga un impacto sustancial en el presupuesto de los organismos implicados, los Estados miembros podrán eximir a dichos organismos de la obligación de poner a disposición gratuitamente dichos conjuntos de datos de alto valor durante un período no superior a dos años a partir de la entrada en vigor del acto de ejecución pertinente adoptado de conformidad con el apartado 1.

Sección 3

Reutilización de determinadas categorías de datos protegidos en poder de organismos del sector público Artículo 32w

*Condiciones para la reutilización*

(1) Los organismos del sector público que, en virtud de la legislación nacional, sean competentes para conceder o denegar el acceso para la reutilización de datos o documentos pertenecientes a determinadas categorías de datos protegidos, pondrán a disposición del público las condiciones para permitir dicha reutilización y el procedimiento para solicitarla a través del punto único de información a que se refiere el artículo 32 bis bis. Cuando concedan o denieguen el acceso para la reutilización, podrán contar con la asistencia de los organismos competentes a que se refiere el artículo 32 septies, 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 32x.

(2) La reutilización de datos o documentos no afectará al carácter protegido de dichos datos o documentos y solo se permitirá:

(a) de conformidad con los derechos de propiedad intelectual.

(b) si los datos que se consideran confidenciales de conformidad con la legislación de la Unión o nacional sobre confidencialidad comercial o estadística no se divulgan como resultado de permitir la reutilización, a menos que dicha reutilización se permita sobre la base del consentimiento del interesado o la autorización del titular de los datos de conformidad con el apartado 5.

(c) de conformidad con el Reglamento (UE) 2016/679.

(3) Para garantizar la preservación 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 solo cuando el organismo del sector público o el organismo competente, tras la solicitud de reutilización, haya garantizado que dichos datos o documentos han sido:

(i) anonimizados, en el caso de los datos personales;

(ii) sometidos a otras formas de preparación de datos personales;

(iii) modificados, agregados o tratados mediante cualquier otro método de control de la divulgación, en el caso de información comercialmente confidencial, incluidos los secretos comerciales o los contenidos protegidos por derechos de propiedad intelectual;

(b) acceder y reutilizar los datos o documentos a distancia en un entorno de tratamiento seguro proporcionado o controlado por el organismo del sector público;

(c) acceder y reutilizar los datos o documentos en las instalaciones físicas en las que se encuentra el entorno de tratamiento seguro, de conformidad con normas de alta seguridad, siempre que no se pueda permitir el acceso a distancia sin poner en peligro los derechos e intereses de terceros.

En el caso de la reutilización permitida de conformidad con el primer párrafo, letra a), inciso i), la reutilización de datos o documentos estará sujeta a las normas sobre datos gubernamentales abiertos establecidas en la sección 2. Esto se entiende sin perjuicio del artículo 32y, que prevalecerá en caso de conflicto.

En el caso de la reutilización permitida 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 los resultados del tratamiento de los datos o documentos realizados por el reutilizador, con el fin de preservar la integridad de la protección de los datos o documentos. También se reservará el derecho de prohibir el uso de resultados que contengan información que ponga en peligro los derechos e intereses de terceros. La decisión de prohibir el uso de los resultados será comprensible y transparente para el reutilizador.

A menos que la legislación nacional establezca garantías específicas sobre las obligaciones de confidencialidad aplicables en relación con la reutilización de determinadas categorías de datos protegidos, el organismo del sector público condicionará la reutilización de los datos o documentos facilitados de conformidad con el apartado 3 al cumplimiento 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, 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 se pueda permitir la reutilización de datos o documentos de conformidad con los apartados 3 y 4, la reutilización solo será posible:

(a) cuando no exista otra base jurídica que el consentimiento para la transmisión de los datos con arreglo al Reglamento (UE) 2016/679, con el consentimiento de los interesados;

(b) con el permiso de los titulares de los datos cuyos derechos e intereses puedan verse afectados por dicha reutilización.

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

Cuando preste dicha asistencia, el organismo del sector público podrá contar con la ayuda de los organismos competentes a que se refiere el artículo 32z.

Artículo 32x

*Requisitos para la transferencia de datos no personales a terceros países por parte de los reutilizadores*

(1) Cuando un reutilizador tenga la intención de transferir determinadas categorías de datos protegidos que no sean personales a un tercer país, informará al organismo del sector público de su intención de transferir dichos datos y de la finalidad de dicha transferencia en el momento de solicitar la reutilización de los datos. En caso de reutilización basada en el permiso del titular de los datos, el reutilizador, con la ayuda del organismo del sector público cuando proceda, informará a la persona física o jurídica cuyos derechos e intereses puedan verse afectados de dicha intención, finalidad y garantías adecuadas. El organismo del sector público no permitirá la reutilización a menos que la persona física o jurídica dé su permiso para la transferencia.

(2) Los organismos del sector público transmitirán datos confidenciales no personales o datos protegidos por derechos de propiedad intelectual a un reutilizador que tenga la intención de transferir esos datos a un tercer país distinto de los designados de conformidad con el apartado 7 solo si el reutilizador se compromete contractualmente a:

(a) cumplir las obligaciones impuestas de conformidad con los derechos de propiedad intelectual y la legislación de la Unión o nacional en materia de confidencialidad comercial o estadística, incluso después de que los datos se hayan transferido al tercer país;

(b) aceptar la jurisdicción de los órganos jurisdiccionales del Estado miembro del organismo del sector público transmisor en relación con cualquier litigio relacionado con el cumplimiento de los derechos de propiedad intelectual y la legislación de la Unión o nacional sobre confidencialidad comercial o estadística.

(3) La Comisión podrá adoptar actos de ejecución por los que se 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, cuando proceda y en la medida de sus capacidades, proporcionarán orientación y asistencia a los reutilizadores para el cumplimiento de las obligaciones a que se refiere el apartado 2.

(5) Cuando esté justificado por el número considerable de solicitudes en toda la Unión relativas a la reutilización de datos no personales en terceros países específicos, la Comisión podrá adoptar actos de ejecución en los que se declare que las disposiciones legales, de supervisión y de ejecución de un tercer país:

(a) garantizar la protección de la propiedad intelectual y los secretos comerciales de una manera que sea esencialmente equivalente a la protección garantizada por el Derecho de la Unión;

(b) se apliquen y se hagan cumplir de manera efectiva; y

(c) ofrecen una tutela judicial efectiva.

(6) Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 46, apartado 2.

(7) Los actos legislativos específicos de la Unión podrán considerar que determinadas categorías de datos no personales en poder de organismos del sector público son altamente sensibles a efectos del presente artículo cuando su transferencia a terceros países pueda poner en peligro los objetivos de política pública de la Unión, como la seguridad y la salud pública, o pueda dar lugar al riesgo de reidentificación de datos no personales y anonimizados. Cuando se adopte un acto de este tipo, la Comisión adoptará actos delegados de conformidad con el artículo 45 que completen el presente Reglamento estableciendo condiciones especiales aplicables a las transferencias de dichos datos a terceros países.

Si así lo exige un acto legislativo específico de la Unión mencionado en el párrafo primero, dichas condiciones especiales podrán incluir condiciones aplicables a la transferencia o disposiciones técnicas al respecto, limitaciones en relación con la reutilización de datos en terceros países o categorías de personas autorizadas a transferir dichos datos a terceros países o, en casos excepcionales, restricciones en relación con las transferencias a terceros países.

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

Artículo 32y
*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 cobren tasas, adoptarán medidas para incentivar la reutilización de determinadas categorías de datos protegidos con fines no comerciales, como la investigación científica, y por parte de empresas emergentes, pymes y microempresas, de conformidad con las normas de la Unión en materia de ayudas estatales. A este respecto, los organismos del sector público también podrán poner los datos a disposición a un precio reducido o de forma gratuita, en particular a las empresas emergentes, las pymes y las PYME, la sociedad civil y los centros de investigación y enseñanza. A tal fin, los organismos del sector público podrán establecer una lista de categorías de reutilizadores a los que se pondrán a disposición datos o documentos para su reutilización a un precio reducido o de forma gratuita. Dicha lista, junto con los criterios utilizados para elaborarla, se hará pública.

(3) Las tarifas se derivarán 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, el suministro y la difusión de datos;

(b) la autorización de derechos;

(c) anonimización u otras formas de preparación de datos personales y datos comercialmente confidenciales, tal y como se establece en el artículo 32w, apartado 3 [condiciones para la reutilización];

(d) el mantenimiento de un entorno de tratamiento seguro;

(e) la adquisición del derecho a permitir la reutilización de conformidad con la presente sección por parte de terceros ajenos al sector público; y la asistencia a los reutilizadores en la obtención del consentimiento de los interesados y la autorización de los titulares de los datos cuyos derechos e intereses puedan verse afectados por dicha reutilización.

(4) Los criterios y la metodología para el cálculo de las tasas serán establecidos por los Estados miembros y se publicarán. El organismo del sector público publicará una descripción de las principales categorías de costes y las normas utilizadas para la asignación de los mismos.

(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 a las empresas de gran tamaño, basándose en criterios objetivos y teniendo en cuenta el poder económico o la capacidad de la entidad para adquirir datos, incluida, en particular, la designación como guardián de datos en virtud del Reglamento (UE) 2022/1925. Las tasas calculadas de este modo serán proporcionadas. Además de los elementos enumerados en el apartado 3 del presente artículo, podrán cubrir el coste de la recopilación y la producción de los datos, junto con un rendimiento razonable de la inversión.

Artículo 32z

*Órganos 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 específicos, pero que en conjunto deberán abarcar todos los sectores, para asistir a los organismos del sector público que conceden o deniegan el acceso para la reutilización de determinadas categorías de datos protegidos. Los Estados miembros podrán crear uno o varios organismos competentes nuevos o recurrir a organismos del sector público existentes o a servicios internos de organismos del sector público que cumplan las condiciones establecidas en la presente sección.

(2) Los organismos competentes podrán estar facultados para conceder acceso para la reutilización de determinadas categorías de datos protegidos de conformidad con el 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 k), 32 w), 32 x), 32 y) y 32 ab).

(3) Los organismos competentes dispondrán de los recursos jurídicos, financieros, técnicos y humanos adecuados para llevar a cabo las tareas que se les asignen, incluidos los conocimientos técnicos necesarios para poder cumplir la legislación de la Unión o nacional pertinente en materia de regímenes de acceso a las categorías de datos protegidos a que se refiere el artículo 2, apartado 54.

(4) La asistencia a que se refiere el apartado 1 incluirá, cuando sea necesario:

(a) la prestación de apoyo técnico mediante la puesta a disposición de un entorno de tratamiento seguro para facilitar el acceso con fines de reutilización de datos o documentos;

(b) la orientación y el apoyo técnico sobre la mejor manera de estructurar y almacenar los datos para que dichos datos o documentos sean fácilmente accesibles;

(c) la prestación de apoyo técnico para la anonimización, la seudonimización y los métodos más avanzados de protección de la privacidad. No se limita a los datos personales, sino también a la información comercialmente confidencial, incluidos los secretos comerciales o los contenidos protegidos por derechos de propiedad intelectual.

(d) ayudar a los organismos del sector público, cuando proceda, a prestar apoyo a los reutilizadores que soliciten el consentimiento de los interesados o la autorización de los titulares de los datos para la reutilización, de conformidad con sus decisiones específicas, incluida la jurisdicción en la que se pretende llevar a cabo el tratamiento de datos, y ayudar a los organismos del sector público a establecer mecanismos técnicos que permitan la transmisión de las solicitudes de consentimiento o autorización de los reutilizadores, cuando sea factible desde el punto de vista práctico;

(e) prestar asistencia a los organismos del sector público para evaluar la adecuación de los compromisos contractuales contraídos por un reutilizador de conformidad con el artículo 32x, apartado 2.

Artículo 32aa

*Punto único de información*

(1) Cada Estado miembro designará un punto único de información. Dicho punto pondrá a disposición información fácilmente accesible sobre la aplicación de los artículos 32w, 32x y 32y.

(2) El punto único de información será competente para recibir consultas o solicitudes de reutilización de determinadas categorías de datos protegidos y las transmitirá, cuando sea posible y apropiado por medios automatizados, a los organismos del sector público competentes o a los organismos competentes a que se refiere el artículo 32z, apartado 1, cuando proceda.

(3) El punto único de información podrá incluir un canal de información separado, simplificado y bien documentado para las pymes, las pymes en fase de arranque, las empresas emergentes y los centros de investigación, que responda a sus necesidades y capacidades a la hora de solicitar la reutilización de las categorías de datos a que se refiere el artículo 2, apartado 54.

(4) El punto único de información pondrá a disposición por medios electrónicos una lista de activos consultable que contenga una visión general de todos los recursos documentales disponibles, incluidos, cuando proceda, los recursos documentales disponibles en los puntos de información sectoriales, regionales o locales, con información pertinente que describa los datos o documentos disponibles, incluyendo al menos el formato y el tamaño de los datos y las condiciones para su reutilización.

(5) La Comisión establecerá un punto de acceso único europeo que ofrezca un registro electrónico consultable de los datos o documentos disponibles en los puntos de información únicos nacionales, así como información adicional sobre cómo solicitar datos o documentos a través de dichos puntos de información únicos nacionales.

Artículo 32 bis

*Procedimiento para las solicitudes de reutilización*

(1) A menos que se hayan establecido plazos más cortos de conformidad con la legislación nacional, los organismos del sector público competentes o los organismos competentes a que se refiere el artículo 32z, apartado 1, adoptarán una decisión sobre la solicitud de reutilización de determinadas categorías de datos protegidos en un plazo de dos meses a partir de la fecha de recepción de la solicitud.

(2) En el caso de solicitudes de reutilización excepcionalmente extensas y complejas, ese plazo de dos meses podrá prorrogarse hasta 30 días. En tales casos, los organismos del sector público competentes o los organismos competentes a que se refiere el apartado 1 del artículo 32z notificarán al solicitante lo antes posible que se necesita más tiempo para llevar a cabo el procedimiento, junto con los motivos del retraso.

(3) Cualquier persona física o jurídica directamente afectada por una decisión a que se refiere el apartado 1 tendrá derecho a interponer un recurso efectivo en el Estado miembro en el que se encuentre el organismo pertinente. Dicho derecho de recurso se establecerá en la legislación nacional e incluirá la posibilidad de revisión por un organismo imparcial con los conocimientos técnicos adecuados, como la autoridad nacional de competencia, la autoridad competente en materia de acceso a los documentos, la autoridad de control establecida de conformidad con el Reglamento (UE) 2016/679 o una autoridad judicial nacional, cuyas decisiones sean vinculantes para el organismo del sector público o el organismo competente de que se trate.

19. El artículo 38 se sustituye por el texto siguiente:

(1) «Sin perjuicio de cualquier otro recurso administrativo o judicial, las personas físicas y jurídicas tendrán derecho a presentar una reclamación, individual o, en su caso, colectivamente:

(a) ante la autoridad competente pertinente del Estado miembro de su residencia habitual, lugar de trabajo o establecimiento, si consideran que se han vulnerado sus derechos en virtud del presente Reglamento;

(b) cualquier asunto que entre en el ámbito de aplicación del presente Reglamento, en concreto contra un proveedor de servicios de intermediación de datos reconocido o una organización de altruismo de datos reconocida, ante la autoridad competente pertinente para el registro de los servicios de intermediación de datos

o ante la autoridad competente pertinente para el registro de organizaciones de altruismo de datos.

(2) El coordinador de datos facilitará, previa solicitud, toda la información necesaria a las personas físicas y jurídicas para que presenten sus reclamaciones ante la autoridad competente correspondiente.

(3) La autoridad competente ante la que se haya presentado la reclamación informará al reclamante, de conformidad con la legislación nacional, sobre:

(a) la marcha del procedimiento, la decisión adoptada; y

(b) los recursos judiciales previstos en el artículo 39.

20. En el artículo 40, se inserta el apartado 6:

«6. El presente artículo no se aplicará al capítulo VII quater».

21. Después del artículo 41, se inserta el siguiente título:

## «CAPÍTULO IX bis

## Comité Europeo de Innovación en materia de Datos»;

22. Se inserta el siguiente artículo 41 bis:

«Artículo 41 bis

*Consejo Europeo de Innovación en materia de Datos*

(1) Se crea el Comité Europeo de Innovación en materia de Datos con el fin de asesorar y asistir a la Comisión en la coordinación de la aplicación del presente Reglamento y servir de foro de debate para el desarrollo de una economía y unas políticas europeas en materia de datos.

(2) Estará compuesto, como mínimo, por representantes de los Estados miembros competentes en materia de datos, las autoridades competentes para la aplicación 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 las pymes de la UE o un representante designado por la red de representantes de las pymes. La Comisión podrá decidir añadir categorías adicionales de miembros. En el nombramiento de expertos individuales, la Comisión procurará lograr un equilibrio de género y geográfico entre los miembros del grupo.

(3) La Comisión decidirá 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 EDIB*

(1) El EDIB apoyará la aplicación coherente del presente Reglamento mediante:

(a) servir de foro para debates estratégicos sobre políticas de datos, gobernanza de datos, flujos internacionales de datos y avances intersectoriales relevantes para la economía europea de datos;

(b) el asesoramiento y la asistencia a la Comisión en lo que respecta al desarrollo de prácticas coherentes de las autoridades competentes en la aplicación de los capítulos II, III, V, VII, VII bis y VII quater;

(c) facilitará la cooperación entre las autoridades competentes mediante el desarrollo de capacidades y el intercambio de información;

(d) el fomento del 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. La facultad de adoptar actos delegados a que se refieren el artículo 29, apartado 7, el artículo 32 u, apartado 2, y el artículo 33, apartado 2, se confiere a la Comisión por un período de tiempo indeterminado».

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

«3. La delegación de poderes a que se refieren el artículo 29, apartado 7, el artículo 32 u, 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 fin a la delegación de la facultad especificada en dicha decisión. Surte efecto a la día siguiente de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior especificada en la misma. No afectará a la validez de los actos delegados ya en vigor».

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

«6. Los actos delegados adoptados con arreglo al artículo 29, apartado 7, al artículo 32 u, apartado 2, o al artículo 33, apartado 2, solo entrarán en vigor si ni el Parlamento Europeo ni el Consejo han formulado objeciones en un plazo de tres meses a partir de la notificación de dicho acto al Parlamento Europeo y al Consejo o si, antes de que expire dicho plazo, tanto el Parlamento Europeo como el Consejo han informado a la Comisión de que no formularán objeciones. Dicho plazo se prorrogará por 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. Cuando se haga referencia al presente apartado, se aplicará el artículo 4 del Reglamento (UE) n.º 182/2011».

26. El artículo 49 queda modificado como sigue:

(a) 1) El apartado 1 se modifica como sigue:

(i) La frase 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 dicha evaluación se analizará, en particular:».

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

«m) el impacto del presente Reglamento en las pymes y las pymes de capital abierto en lo que respecta a su capacidad de innovación y a la disponibilidad de servicios de tratamiento de datos para los usuarios de la Unión, así como la carga que supone el cumplimiento de las nuevas obligaciones».

(b) Se inserta el siguiente apartado 2 bis:

«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 y VII quater del presente Reglamento y presentará un informe sobre sus principales conclusiones al Parlamento Europeo y al Consejo, así como al Comité Económico y Social Europeo.

El informe evaluará, en particular:

(a) el estado de los registros de los servicios de intermediación de datos y el tipo de servicios que ofrecen;

(b) el tipo de organizaciones de altruismo de datos registradas y una visión general de los objetivos de interés general para los que se comparten los datos, con vistas a establecer criterios claros al respecto».

(c) el alcance y el impacto social y económico de la sección 2 del capítulo VII quater, incluyendo

(d) el alcance del aumento de la reutilización de los documentos del sector público a los que se aplica la sección 2 del capítulo VII quater, especialmente por parte de las pymes y las microempresas;

(e) el impacto de los conjuntos de datos de alto valor;

(f) la interacción entre las normas de protección de datos y las posibilidades de reutilización;

(g) Los Estados miembros facilitarán a la Comisión la información necesaria para la elaboración de dicho 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, cuando proceda, presentar al Parlamento Europeo y al Consejo una propuesta legislativa para modificar el presente Reglamento».

27. Se añade el anexo I que 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 «Creación, gestión y cierre de una empresa» se sustituye por el texto siguiente:

| | | |
|---|---|---|
| Acontecimientos vitales | Procedimientos | Resultado esperado, sujeto a la evaluación de la solicitud por parte de la autoridad competente in |

| | | |
|---|---|---|
| | | de conformidad con la legislación nacional, cuando proceda |
| Creación, gestión y cierre empresarios | Notificación de la actividad empresarial, permiso para el ejercicio de una actividad empresarial, cambios en la actividad empresarial o la solicitud de cese de una actividad empresarial que implique insolvencia o liquidación, para la autorización para excluyendo el registro inicial de una actividad empresarial en el registro mercantil y excluyendo los procedimientos relativa a la constitución o cualquier presentación posterior por parte de sociedades o empresas en el sentido del segundo párrafo del artículo 54 del TFUE | Confirmación de la recepción de la notificación |
| | Inscripción de un empleador (persona física) con los regímenes obligatorios de pensiones y seguros | confirmación de registro o número de la seguridad social número de registro |
| | Registro de empleados con pensión obligatoria y seguros | confirmación de número de registro o de la seguridad social número de registro |
| | Presentación de la declaración del impuesto de sociedades | Confirmación de la recepción de la declaración |
| | Notificación a los regímenes de la seguridad social del fin de la relación con un empleado, excluidos los procedimientos para la rescisión colectiva de los contratos de los empleados | Confirmación del contrato |
| | Pago de las cotizaciones sociales de los empleados | Recepción u otra forma de confirmación del pago de las cotizaciones sociales de los empleados |
| | Registro como proveedor de servicios de intermediación de datos | Confirmación de el registro |
| | Registro como organización de altruismo de datos reconocida en la Unión | Confirmación de la registro |

*Artículo 3*

*Modificaciones del Reglamento (UE) 2016/679 (RGPD)*

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

1. El artículo 4 queda modificado como sigue:

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

«La información relativa a una persona física no es necesariamente un dato personal para todas las demás personas o entidades, por el mero hecho de que otra entidad pueda identificar a dicha

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 pueda utilizar dicha entidad. Dicha información no se convierte en personal para esa entidad por el mero hecho de que un posible destinatario posterior disponga de medios que razonablemente puedan utilizarse para identificar a la persona física a la que se refiere la información».

(b) Se añaden los siguientes puntos:

«32) «equipo terminal»: el equipo terminal tal como se define en el artículo 1, apartado 1, de la Directiva 2008/63/CE;

(33) para «redes de comunicaciones electrónicas» se aplicará la definición del artículo 2, apartado 1, de la Directiva (UE) 2018/1972;

(34) «navegador web»: el navegador web tal como se define en el artículo 2, apartado 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, apartado 1, del Reglamento (UE) 2024/1083;

(36) «prestador de servicios de comunicación social»: un prestador de servicios de comunicación social tal como se define en el artículo 2, apartado 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»: cualquier investigación que también pueda apoyar la innovación, como el desarrollo tecnológico y la demostración. Estas acciones contribuirán al conocimiento científico existente 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 como objetivo promover un interés comercial.

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

«recogidos con fines determinados, explícitos y legítimos, y no tratados posteriormente de manera incompatible con dichos fines; el tratamiento posterior con fines de archivo en interés público, con fines de investigación científica o histórica o con fines estadísticos se considerará, de conformidad con el artículo 89, apartado 1, 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 siguientes letras:

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

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

(b) Se añade el siguiente apartado:

«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 cualquier otro tipo de tratamiento de categorías especiales de datos personales. Cuando, a pesar de la aplicación de dichas medidas, el responsable del tratamiento identifique categorías especiales de datos personales en los conjuntos de datos utilizados para el entrenamiento, las pruebas o la validación, o en el sistema o modelo de IA, el responsable del tratamiento eliminará dichos datos. Si la eliminación de esos datos requiere un esfuerzo desproporcionado, el responsable del tratamiento protegerá en cualquier caso, sin demora injustificada, dichos datos para que no se utilicen para producir resultados, se divulguen o se pongan 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 y cualquier comunicación y cualquier medida adoptada en virtud de los artículos 15 a 22 y 34 se proporcionarán de forma gratuita. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular por su carácter repetitivo o, en el caso de las solicitudes en virtud del artículo 15, porque el interesado abuse de los derechos que le confiere el presente Reglamento con fines distintos de la protección de sus datos, el responsable del tratamiento podrá:

(a) cobrar una tasa razonable teniendo en cuenta los costes administrativos de facilitar la información o la comunicación o de adoptar la medida solicitada; o

(b) denegar la solicitud.

El responsable del tratamiento tendrá la carga de demostrar que la solicitud es manifiestamente infundada o que existen motivos razonables para considerar 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 refieren las letras a) y c) del apartado 1, a menos que el responsable del tratamiento transmita los datos a otros destinatarios o categorías de destinatarios, transfiera los datos a un tercer país, lleve a cabo la toma de decisiones automatizada, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartado 1, o el tratamiento pueda dar lugar a 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:

«5. Cuando el tratamiento se realice con fines de investigación científica y el suministro de la información a que se refieren los apartados 1, 2 y 3 resulte imposible o suponga un esfuerzo desproporcionado, con sujeción a las condiciones y garantías a que se refiere el artículo 89, apartado 1, o en la medida en que la obligación a que se refiere el apartado 1 del presente artículo pueda imposibilitar o menoscabar gravemente la consecución de los objetivos de dicho tratamiento, el responsable del tratamiento no estará obligado a facilitar la información a que se refieren los apartados 1, 2 y 3. En tales casos, el responsable del tratamiento adoptará las medidas adecuadas para proteger los derechos y libertades y los intereses legítimos del interesado, incluida la divulgación pública de la información».

7. En el artículo 22, los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Una decisión que produzca efectos jurídicos para el interesado o que le afecte de manera similar y significativa solo podrá basarse en un tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión:

(a) sea necesaria para la celebración o el cumplimiento de un contrato entre el interesado y un responsable del tratamiento, independientemente de que la decisión pueda adoptarse por medios distintos de los puramente automatizados;

(b) esté autorizada por el Derecho de la Unión o de los Estados miembros al que esté sujeto el responsable del tratamiento y que también establezca 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 datos personales que pueda suponer un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento notificará la violación de datos personales sin demora injustificada y, cuando sea posible, a más tardar 96 horas después de haber tenido conocimiento de ella, a través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 a la autoridad de control competente de conformidad con los artículos 55 y 56. Cuando la notificación a la autoridad de control no se realice en un plazo de 96 horas, se acompañará de los motivos del retraso».

(b) Se añade el siguiente apartado:

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

(c) Se añaden los siguientes apartados:

«6. El Comité elaborará y transmitirá a la Comisión una propuesta de modelo común para notificar una violación de 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 una violación de datos personales puede suponer un alto riesgo para los derechos y libertades de una persona física. Las propuestas se presentarán a la Comisión en un plazo de [OP fecha = nueve meses a partir de la entrada en vigor del presente Reglamento]. La Comisión, tras el examen oportuno, 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.

7. La plantilla y la lista a que se refiere el apartado 6 se revisarán al menos cada tres años y se actualizarán cuando sea necesario. El Comité presentará su evaluación y las posibles propuestas de actualización a la Comisión a su debido tiempo. La Comisión, tras examinar debidamente las propuestas, las revisará y estará facultada para adoptar cualquier actualización siguiendo el procedimiento del 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 están sujetas al requisito de 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 operaciones de tratamiento para los que no se requiere una evaluación de impacto relativa a la protección de datos.

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

(b) Se insertan los siguientes apartados:

«6 bis. Las propuestas relativas a las listas mencionadas en los apartados 4 y 5 y al modelo y la metodología mencionados en el apartado 6 se presentarán a la Comisión en un plazo de [fecha de la OP = nueve meses a partir de la entrada en vigor del presente Reglamento]. La Comisión, tras examinarlas debidamente, las revisará, en caso 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 y la plantilla y la metodología a que se refiere el apartado 6 bis se revisarán al menos cada tres años y se actualizarán cuando sea necesario. El Comité presentará a la Comisión, a su debido tiempo, su evaluación y las posibles propuestas de actualización. La Comisión, tras examinar debidamente las propuestas, las revisará y estará facultada para adoptar cualquier actualización siguiendo el procedimiento del apartado 6 bis.

6 quater. Las listas de los tipos de operaciones de tratamiento que están sujetas al requisito de una evaluación de impacto relativa a la protección de datos y de los tipos de operaciones de tratamiento para las que no se requiere una evaluación de impacto relativa a la protección de datos, establecidas y publicadas por las autoridades de control, seguirán siendo válidas hasta que la Comisión adopte el acto de ejecución mencionado en el apartado 6 bis.

10. Se añade el siguiente artículo:

«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 actual de la técnica disponible;

(b) desarrollará criterios y/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 podrá utilizarse como elemento para demostrar que los datos no pueden dar lugar a la reidentificación de los interesados.

(4) La Comisión asociará estrechamente al CEPD a la preparación 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 de conformidad con el procedimiento de examen contemplado en el artículo 93, apartado 3.

11. En el artículo 57, apartado 1, se modifica lo siguiente:

(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 artículo 70, apartado 1, se insertan las siguientes letras:

«ha) preparar y transmitir a la Comisión una propuesta de lista de los tipos 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 dicha evaluación, de conformidad con el artículo 35.

hb) preparar y transmitir a la Comisión una propuesta de modelo común y una metodología común para realizar evaluaciones de impacto relativas a la protección de datos, de conformidad con el artículo 35.

h qu ter) preparar y transmitir a la Comisión una propuesta de modelo común para notificar una violación de datos personales a la autoridad de control competente, así como una lista de las circunstancias en las que una violación de datos personales puede suponer un alto riesgo para los derechos y libertades de una persona física, de conformidad con el artículo 33.

15. Después del artículo 88, se añaden los siguientes artículos:

«Artículo 88 bis

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

(1) El almacenamiento de datos personales o el acceso a datos personales ya almacenados en los equipos terminales de una persona física solo se permite cuando dicha persona ha dado su consentimiento, de conformidad con el presente Reglamento.

(2) El apartado 1 no impedirá el almacenamiento de datos personales, ni el acceso a datos personales ya almacenados, en los equipos terminales 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 establecidas en dicho artículo, para salvaguardar los objetivos a que se refiere el artículo 23, apartado 1.

(3) El almacenamiento de datos personales o el acceso a datos personales ya almacenados en el equipo terminal de una persona física sin su consentimiento, así como su posterior tratamiento, serán lícitos en la medida en que sean necesarios para cualquiera de los siguientes fines:

(a) realizar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas;

(b) prestar un servicio solicitado expresamente 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 de dicho servicio en línea exclusivamente para su propio uso;

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

(4) Cuando el almacenamiento de datos personales o el 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 rechazar las solicitudes de consentimiento de forma fácil e inteligible mediante un botón de un solo clic o un medio equivalente;

(b) si el interesado da su consentimiento, el responsable del tratamiento no volverá a solicitarlo para la misma finalidad durante el período en que pueda basarse legítimamente en dicho consentimiento;

(c) si el interesado rechaza una solicitud de consentimiento, el responsable del tratamiento no podrá volver a solicitarlo para la misma finalidad durante un período mínimo de seis meses.

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

(5) El presente artículo se aplicará a partir del [OP: insértese la fecha = seis meses después de la fecha de 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 personas físicas*

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

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

(b) rechacen una solicitud de consentimiento y ejerzan 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 elecciones realizadas 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 proveedores de servicios de medios de comunicación cuando presten un servicio de medios de comunicación.

(4) La Comisión, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, solicitará a uno o varios organismos europeos de normalización que elaboren normas para la interpretación de las indicaciones legibles por máquina de las elecciones de los interesados.

Las interfaces en línea de los controladores que sean conformes con las normas armonizadas o partes de las mismas cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* se considerarán conformes con los requisitos cubiertos por dichas normas o partes de las mismas, establecidos en el apartado 1.

(5) Los apartados 1 y 2 se aplicarán a partir del [OP: insértese la fecha = 24 meses después de la fecha de entrada en vigor del presente Reglamento].

(6) Los proveedores de navegadores web que no sean pymes proporcionarán los medios técnicos para que los interesados puedan dar su consentimiento y denegarlo, así como ejercer el derecho de oposición con arreglo al artículo 21, apartado 2, mediante los medios automatizados y legibles por máquina a que se refiere el apartado 1 del presente artículo, tal como se aplica con arreglo a los apartados 2 a 5 del presente artículo.

(7) El apartado 6 se aplicará a partir del [OP: insértese la fecha = 48 meses después de la fecha de entrada en vigor del presente Reglamento].

Artículo 88 quater

*Tratamiento en el contexto del desarrollo y 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 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 llevarse a cabo por intereses legítimos en el sentido del artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, cuando proceda, salvo cuando otras leyes de la Unión o nacionales exijan explícitamente el consentimiento, y cuando dichos intereses se vean superados por los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de los datos personales, en particular cuando el interesado sea un niño.

Cualquier tratamiento de este tipo estará sujeto a medidas organizativas y técnicas adecuadas y a garantías para los derechos y libertades del interesado, tales como garantizar el respeto de la minimización de datos durante la fase de selección de fuentes y la formación y prueba de un sistema o modelo de IA, proteger contra la divulgación de datos retenidos de forma residual en el sistema o modelo de IA para garantizar una mayor transparencia a los interesados y proporcionar a estos un derecho incondicional a oponerse al tratamiento de sus datos personales.»

*Artículo 4*

*Modificaciones del Reglamento (UE) 2018/1725 (EUDPR)*

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 siguientes frases:

«La información relativa a una persona física no es necesariamente un dato personal para todas las demás personas o entidades, por el mero hecho de que otra entidad pueda identificar a dicha 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 pueda utilizar dicha entidad. Dicha información no se convierte en personal para esa entidad por el mero hecho de que un posible destinatario posterior disponga de medios que razonablemente puedan utilizarse para identificar a la persona física a la que se refiere la información».

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

«25) por «redes de comunicaciones electrónicas» se entenderá lo dispuesto en el artículo 2, apartado 1, de la Directiva (UE) 2018/1972;»

(c) Se añaden los siguientes puntos:

«27) «aplicación móvil»: una aplicación móvil tal como se define en el artículo 3, apartado 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»: cualquier investigación que también pueda apoyar la innovación, como el desarrollo tecnológico y la demostración. Estas

acciones contribuirán al conocimiento científico existente 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 como objetivo promover un interés comercial».

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

«b) recogidos con fines determinados, explícitos y legítimos, y no tratados posteriormente de manera incompatible con dichos fines; el tratamiento posterior con fines de archivo en interés público, con fines de investigación científica o histórica o con fines estadísticos se considerará, de conformidad con el artículo 13, 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 siguientes letras:

«k) el tratamiento en el contexto del desarrollo y 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, con sujeción a las condiciones a que se refiere el apartado 4.

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

(b) Se añade el siguiente apartado 4:

«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 el tratamiento de categorías especiales de datos personales. Cuando, a pesar de la aplicación de dichas medidas, el responsable del tratamiento identifique categorías especiales de datos personales en los conjuntos de datos utilizados para el entrenamiento, las pruebas o la validación, o en el sistema o modelo de IA, el responsable del tratamiento eliminará dichos datos. Si la eliminación de esos datos requiere un esfuerzo desproporcionado, el responsable del tratamiento protegerá en cualquier caso, sin demora injustificada, dichos datos para que no se utilicen para producir resultados, se divulguen o se pongan 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 y cualquier comunicación y cualquier medida adoptada en virtud de los artículos 17 a 24 y 35 se proporcionarán de forma gratuita. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular por su carácter repetitivo o, en el caso de las solicitudes en virtud del artículo 17, porque el interesado abuse de los derechos que le confiere el presente Reglamento con fines distintos de la protección de sus datos, el responsable del tratamiento podrá negarse a atender la solicitud. Corresponderá al responsable del tratamiento demostrar que la solicitud es manifiestamente infundada o que existen motivos razonables para considerar que es excesiva».

5. En el artículo 15 se añade el nuevo apartado 5:

«5. Cuando el tratamiento se realice con fines de investigación científica y el suministro de la información a que se refieren los apartados 1, 2 y 3 resulte

imposible o implicaría un esfuerzo desproporcionado, con sujeción a las condiciones y garantías a que se refiere el artículo 13, o en la medida en que la obligación a que se refiere el apartado 1 del presente artículo pueda imposibilitar o menoscabar gravemente la consecución de los objetivos de dicho tratamiento, el responsable del tratamiento no estará obligado a facilitar la información a que se refieren los apartados 1, 2 y 3. En tales casos, el responsable del tratamiento adoptará las medidas adecuadas para proteger los derechos y libertades y los intereses legítimos del interesado, incluida la divulgación pública de la información.

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

«1. Una decisión que produzca efectos jurídicos para el interesado o que le afecte de manera similar y significativa solo podrá basarse en un tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión:

(a) sea necesaria para la celebración o el cumplimiento de un contrato entre el interesado y un responsable del tratamiento, independientemente de que la decisión pueda tomarse por medios distintos de los exclusivamente automatizados;

(b) esté autorizada por el Derecho de la Unión al que esté sujeto el responsable del tratamiento y que también establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o

(c) se basa 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 datos personales que pueda suponer un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento notificará la violación de datos personales al Supervisor Europeo de Protección de Datos sin demora injustificada y, cuando sea posible, a más tardar 96 horas después de haber tenido conocimiento de ella. Cuando la notificación al Supervisor Europeo de Protección de Datos no se realice en un plazo de 96 horas, se acompañará de los motivos del retraso».

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

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

(3) El apartado 1 no excluye el almacenamiento de datos personales, ni el acceso a 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 establecidas en dicho artículo, con el fin de salvaguardar los objetivos a que se refiere el artículo 25, apartado 1.

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

(a) realizar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas;

(b) prestar un servicio solicitado expresamente 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 de dicho servicio en línea exclusivamente para su propio uso;

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

(5) Cuando el almacenamiento de datos personales o el 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 rechazar las solicitudes de consentimiento de forma fácil e inteligible mediante un botón de un solo clic o un medio equivalente;

(b) si el interesado da su consentimiento, el responsable del tratamiento no volverá a solicitarlo para la misma finalidad durante el período en que pueda basarse legítimamente en dicho consentimiento;

(c) si el interesado rechaza una solicitud de consentimiento, el responsable del tratamiento no podrá volver a solicitarlo para la misma finalidad durante un período mínimo de seis meses.

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

(6) El presente artículo se aplicará a partir del [OP: insértese la fecha = seis meses después de la fecha de entrada en vigor del presente Reglamento].

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

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

(b) rechazar 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 que se ajusten a las normas armonizadas o a partes de las mismas a que se refiere el artículo 88 ter, apartado 4, del Reglamento (CE) 2016/679 cumplen los requisitos contemplados en dichas normas o partes de las mismas, establecidos en el apartado 7.

(10) Los apartados 7 a 9 se aplicarán a partir del [OP: insértese la fecha = 24 meses después de la fecha de 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 adoptadas por la Comisión y a las que se refiere el apartado 6 bis del artículo 35 del Reglamento (UE) 2016/679 se aplicarán al tratamiento de datos personales en virtud del presente Reglamento».

(b) Se suprimen los apartados 5 y 6.

(9) Se añade el siguiente artículo:

«Artículo 45 bis

Los criterios comunes adoptados por la Comisión y mencionados en el artículo 41 bis del Reglamento (UE) 2016/679 se aplicarán al tratamiento de datos personales en virtud del presente Reglamento».

*Artículo 5*

*Modificaciones de la Directiva 2002/58/CE (Directiva sobre la privacidad electrónica)*

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

1. Se suprime el artículo 4.

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

«El presente apartado no se aplicará si el abonado o usuario es una persona física y la información almacenada o a la que se accede constituye o da lugar 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 añade el siguiente artículo 23 bis:

«Artículo 23 bis

*Punto único de entrada 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 dichos 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 establecida en virtud de dicho Reglamento.

(2) La ENISA adoptará las medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que plantean para la seguridad del punto de entrada único y la información presentada o difundida a través de él. La ENISA tendrá en cuenta la sensibilidad de la información presentada o difundida de conformidad con 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 según lo exigido en dichos actos jurídicos de la Unión.

(3) La ENISA proporcionará y aplicará las especificaciones sobre las medidas técnicas, operativas y organizativas relativas al establecimiento, mantenimiento y funcionamiento seguro del punto de entrada único. La ENISA elaborará las especificaciones en cooperación con la Comisión, la red CSIRT y las autoridades competentes en virtud de los actos jurídicos de la Unión a que se refiere el apartado 1. Las especificaciones garantizarán que:

(a) se garantice la capacidad necesaria para la interoperabilidad con respecto a otras obligaciones de notificación pertinentes a que se refiere el apartado 1;

(b) se hayan establecido las disposiciones técnicas necesarias para que las entidades y autoridades pertinentes, con arreglo a los actos jurídicos de la Unión a que se refiere el apartado 1, puedan acceder, presentar, recuperar, transmitir o tratar de otro modo la información procedente del punto de entrada único, y se proporcionen protocolos y herramientas técnicos que permitan a las entidades y autoridades seguir tratando la información recibida en sus sistemas;

(c) se tengan debidamente en cuenta las especificidades de los requisitos de notificación de incidentes establecidos en los actos jurídicos de la Unión mencionados en el apartado 1;

(d) cuando proceda, el punto de entrada único sea interoperable y compatible con las carteras empresariales europeas a que se refiere *la [Propuesta de Reglamento: Insertar título de la propuesta]* y que las carteras empresariales europeas puedan utilizarse, como mínimo, para identificar y autenticar a las entidades que utilizan el punto de entrada único;

(e) las entidades que utilicen el punto de entrada único puedan recuperar y completar la información que hayan presentado previamente a través del punto de entrada único;

(f) una única notificación de la información presentada por una entidad a través del punto de entrada único puede utilizarse 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 que se disponga lo 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 enviadas a través del punto de entrada único.

(5) En un plazo de [18] meses a partir de la entrada en vigor del presente Reglamento, la ENISA pondrá a prueba el funcionamiento del punto de entrada único para cada acto jurídico de la Unión añadido, incluidas pruebas que tengan en cuenta las especificidades y los requisitos de las notificaciones establecidos en cada acto jurídico de la Unión respectivo, y previa consulta a la Comisión y a las autoridades competentes pertinentes en virtud de los respectivos actos jurídicos de la Unión. La ENISA permitirá la notificación de incidentes en virtud de cada acto jurídico de la Unión mencionado en el apartado 1 solo después de poner a prueba su funcionamiento y de que la Comisión haya publicado un aviso de conformidad con el apartado 6.

(6) La Comisión, en cooperación con la ENISA, evaluará el buen funcionamiento, la fiabilidad, la integridad y la confidencialidad del punto de entrada único. Cuando la Comisión, previa consulta a la red CSIRT y a las autoridades competentes en virtud de los actos jurídicos de la Unión mencionados en el apartado 1, considere que el punto de entrada único garantiza el buen funcionamiento, la fiabilidad, la integridad y la confidencialidad, publicará un aviso a tal efecto en el Diario Oficial de la Unión Europea.

(7) Si la Comisión concluye en su evaluación que el punto de entrada único no garantiza el buen funcionamiento, la fiabilidad, la integridad o la confidencialidad, la ENISA, en cooperación con la Comisión y sin demora injustificada, adoptará todas las medidas correctoras necesarias para garantizar sin demora el buen funcionamiento, la fiabilidad, la integridad o la confidencialidad, e informará a la Comisión de los resultados. A continuación, la Comisión volverá a evaluar el buen funcionamiento, la fiabilidad, la integridad o la confidencialidad del punto de entrada único y publicará un aviso 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 injustificada, a su CSIRT o, en su caso, a su autoridad competente, de

de conformidad con el apartado 4 del presente artículo, cualquier incidente que tenga un impacto significativo en la prestación de sus servicios, tal como se menciona en el apartado 3 del presente artículo (incidente significativo), a través del punto de entrada único establecido de conformidad con el artículo 23 bis».

(a) Se añade el siguiente apartado 12:

«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 la notificación de la 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, de forma voluntaria a través del punto de entrada único establecido de conformidad con el artículo 23 bis, por parte de:

(a) entidades esenciales e importantes en lo que respecta a incidentes, amenazas cibernéticas e incidentes evitados por poco;

(b) entidades distintas de las mencionadas en la letra a), independientemente de que entren en el ámbito de aplicación de la presente Directiva, en relación con incidentes significativos, amenazas cibernéticas e incidentes evitados por poco».

*Artículo 7*

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

El Reglamento (UE) n.º 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 supervisor y, en su caso, a otras autoridades competentes pertinentes, se realizarán 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 siguiente apartado 2 bis:

«2 bis. Las notificaciones previstas en el apartado 2, letra f ter), del presente artículo al organismo supervisor y, en su caso, a otros organismos competentes pertinentes, se realizarán a través del punto de entrada único previsto en el 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 previstas en el apartado 3 a la Comisión y al organismo supervisor competente se realizarán a través del punto de entrada único, de conformidad con el 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 queda modificado como sigue:

1. en el apartado 1, el párrafo primero se sustituye por el texto siguiente:

> «Las entidades financieras notificarán los incidentes importantes relacionados con las TIC a la autoridad competente pertinente a que se refiere el artículo 46 a través del punto de entrada único establecido de conformidad con el 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, de forma voluntaria, notificar a la autoridad competente pertinente, a través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555, las amenazas cibernéticas significativas cuando consideren que dichas amenazas son relevantes para el sistema financiero, los usuarios de los servicios o los clientes. La autoridad competente pertinente podrá facilitar dicha información a otras autoridades pertinentes a las que se refiere el apartado 6».

*Artículo 9*

*Modificaciones de la Directiva (UE) 2022/2557*

El artículo 15 de la Directiva (UE) 2022/2557 queda modificado como sigue:

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

> «Los Estados miembros velarán por que las entidades críticas notifiquen a la autoridad competente, sin demora injustificada, a través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555, los incidentes que perturben de manera significativa o puedan perturbar de manera significativa la prestación de servicios esenciales».

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

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

*Artículo 10*

*Derogaciones y disposiciones transitorias*

1. El Reglamento (UE) 2019/1150 queda derogado con efecto a partir del [fecha = fecha de entrada en vigor 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 2019/1024.

4. Las referencias al Reglamento (UE) 2022/868, al Reglamento (UE) 2018/1807 y a la Directiva 2019/1024 se leerán de conformidad con la tabla de correspondencias que figura en el anexo I del presente Reglamento.

*Artículo 11*

*Disposiciones finales*

El presente Reglamento entrará en vigor el tercer día siguiente al 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 los artículos 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 buen funcionamiento, la fiabilidad, la integridad o la confidencialidad, las obligaciones de informar 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,

*Por el Parlamento Europeo*
*El Presidente*

*Por el Consejo*
*El Presidente*

**FICHA FINANCIERA Y DIGITAL LEGISLATIVA**

## 1. MARCO DE LA PROPUESTA/INICIATIVA

### 1.1. Título de la propuesta/iniciativa e

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre 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 y la Directiva 2002/58/CE y la Directiva ( UE) 2022/2555, y por el que se derogan el Reglamento (UE) 2022/868, el Reglamento (UE) 2018/1807, el Reglamento (UE) 2019/1150 y la Directiva (UE) 2019/1024 (Omnibus digital para el acervo digital)

### 1.2. Ámbito(s) político(s) afectado(s)

Redes, contenidos y tecnologías de la comunicación;

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. Objetivos específicos*

Objetivo específico n.º 1

Mejorar la gobernanza y la aplicación efectiva del acervo digital reduciendo la complejidad de las normas, los costes administrativos para las empresas y las administraciones y derogando actos legislativos.

Objetivo específico n.º 2

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

#### *1.3.3. Resultados e impacto previstos*

*Especificar los efectos que la propuesta o iniciativa debería tener en los beneficiarios o grupos destinatarios.*

Reducción de los costes para las empresas gracias a la simplificación de la legislación y la racionalización de la presentación de informes.

#### *1.3.4. Indicadores de rendimiento*

*Especificar los indicadores para supervisar los avances y los logros.*

Indicador 1

Reducción calculada de los costes para las empresas.

Indicador 2

Ahorro de costes para la notificación de incidentes por

parte de las empresas. Indicador 3

### 1.4. La propuesta o iniciativa se refiere a un :

☐ □□□ nueva acción

☐ □□□ nueva acción tras un proyecto piloto o una acción preparatoria[39]

☒ la ampliación de una acción existente

☐ □□□ fusión o reorientación de una o varias acciones hacia otra acción o una nueva acción

## 1.5. Motivos de la propuesta/iniciativa e

*1.5.1. Requisitos que deben cumplirse a corto o largo plazo, incluido un calendario detallado para la puesta en marcha de la iniciativa*

*Se prevé que entre en vigor en un plazo de tres días a partir de su publicación en el Diario Oficial. La entrada en vigor debería ser inmediata, con excepciones notables para las normas que requieren un período transitorio. Para el capítulo III, relativo a la notificación de incidentes y las normas relacionadas con las plataformas, se requiere un período suficiente para la aplicación, adaptado a las necesidades de las empresas, los Estados miembros y los organismos de la UE.*

*1.5.2. Valor añadido de la participación de la UE (puede derivarse de diferentes factores, por ejemplo, ganancias de coordinación, seguridad jurídica, mayor eficacia o complementariedades). A efectos de la presente sección, se entiende por «valor añadido de la participación de la UE» el valor resultante de la acción de la UE, que se suma al valor que habrían creado por sí solos los Estados miembros.*

Las razones para actuar 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 UE (ex ante).

El valor añadido previsto para la UE (ex post) consiste en la racionalización del Derecho de la UE y la reducción de la carga administrativa y los costes para las empresas.

En lo que respecta al establecimiento de un punto único de entrada para la notificación de incidentes, el valor añadido específico se deriva de proporcionar una solución a escala de la Unión que responda a las necesidades nacionales. Los costes para las empresas se optimizan al proporcionar un punto único, independientemente de la ubicación de la entidad notificante en la Unión y de las autoridades encargadas de recibir las notificaciones.

*1.5.3. Lecciones aprendidas de experiencias similares en el pasado*

*Las modificaciones de los reglamentos respectivos se basan en la experiencia práctica adquirida en la aplicación de las normas, tal como se detalla en el documento de trabajo de los servicios de la Comisión que acompaña al presente documento. Se basan en amplias consultas con las partes interesadas, centrándose principalmente en la aplicación cotidiana de las normas.*

*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.

[39] Tal como se menciona en el artículo 58, apartado 2, letras a) o b), del Reglamento financiero.

*1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluido el margen para la reasignación*

| |
|---|
| N.A. |

## 1.6. Duración de la propuesta/iniciativa y de su impacto financiero e

5. ☐ Duración limitada

☐ en vigor desde el [DD/MM]AAAA hasta el [DD/MM]AAAA

☐ repercusión financiera de AAAA a AAAA para los créditos de compromiso y de AAAA a AAAA para los créditos de pago.

6. ☒ duración ilimitada

Aplicación con un período inicial de YYYY a YYYY, seguido de una

aplicación a gran escala.

## 1.7. Método(s) de ejecución presupuestaria previstos[40]

7. ☒ **Gestión directa** por parte de la Comisión

☒ por sus servicios, incluido el personal de las delegaciones de la Unión;

☐ por las agencias ejecutivas

8. ☐ **Gestión compartida** con los Estados miembros

9. ☐ **Gestión indirecta** mediante la delegación de tareas de ejecución presupuestaria en:

☐ terceros países o los organismos que hayan designado

☐ organizaciones internacionales y sus agencias (por 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 con una misión de servicio público, en la medida en que cuenten con garantías financieras adecuadas

☐ los organismos regidos por el Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una asociación público-privada y que cuenten con garantías financieras adecuadas

☐ Organismos o personas encargados de la ejecución de acciones específicas en el ámbito de la política exterior y de seguridad común, de conformidad con el título V del Tratado de Unión Europea, y que se identifiquen en el acto de base correspondiente

☐ organismos establecidos en un Estado miembro, regidos por el Derecho privado de un Estado miembro o por el Derecho de la Unión y aptos para que se les confíe, de conformidad con las normas sectoriales específicas
, la ejecución de fondos o garantías presupuestarias de la Unión, en la medida en que dichos organismos estén controlados por organismos de Derecho público o por organismos de Derecho privado con una misión de servicio público, y cuenten con garantías financieras adecuadas en forma de responsabilidad solidaria por parte del organismo de control

---

[40] Los detalles de los métodos de ejecución presupuestaria y las referencias al Reglamento financiero pueden consultarse en el sitio web BUDGpedia : https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

organismos o garantías financieras equivalentes y que, para cada acción, podrán limitarse al importe máximo de la ayuda de la Unión.

I

## 2. MEDIDAS DE GESTIÓN E

### 2.1. Normas de control y presentación de informes

10. Las modificaciones se supervisarán como parte de la legislación que se modifica.

### 2.2. Sistema(s) de gestión y control

*2.2.1. Justificación del método o métodos de ejecución presupuestaria, del mecanismo o mecanismos de ejecución de la financiación, de las modalidades de pago y de la estrategia de control propuesta*

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

*2.2.2. Información sobre los riesgos identificados y los sistemas de control interno establecidos para mitigarlos*

12. No se han identificado riesgos adicionales

*2.2.3. Estimación y justificación de la rentabilidad de los controles (relación entre los costes de control y el valor de los fondos gestionados relacionados) y evaluación de los niveles de riesgo de error previstos (en el momento del pago y en el momento del cierre)*

13. El coste del control no diferirá del coste anterior.

### 2.3. Medidas para prevenir el fraude y las irregularidades

14. Las mismas medidas preventivas siguen aplicándose a las modificaciones.

## 3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA E

### 3.1. Rúbricas del marco financiero plurianual y líneas presupuestarias de gastos es afectadas

Líneas presupuestarias existentes

15. Por orden de rúbricas del marco financiero plurianual y líneas presupuestarias.

| Rúbrica del marco financiero plurianual | Línea presupuestaria | Tipo de gasto | Contribución | | | |
|---|---|---|---|---|---|---|
| | Número | Dif./No dif.[41] | de los países de la AELC países [42] | de países candidatos y posibles candidatos [43] | De otros terceros países | otros ingresos asignados |
| | 20 02 06 Gastos administrativos | No dif. | NO | NO | NO | NO |
| | | | | | | |
| | | | | | | |

Nuevas líneas presupuestarias solicitadas

16. Por orden de rúbricas del marco financiero plurianual y líneas presupuestarias.

| Rúbrica del marco financiero plurianual | Línea presupuestaria | Tipo de gasto | Contribución | | | |
|---|---|---|---|---|---|---|
| | Número | Diferenciado/No diferenciado | de los países de la AELC países | de los países candidatos y potenciales candidatos | de otros terceros países | otros ingresos asignados |
| | | | | | | |
| | | | | | | |
| | | | | | | |

[41] Dif. = Créditos diferenciados / No dif. = Créditos no diferenciados.
[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 e es

### *3.2.1. Resumen del impacto estimado en los créditos operativos*

☒La propuesta/iniciativa no requiere el uso de créditos operativos opriations

☐ La propuesta/iniciativa requiere el uso de créditos operativos, tal y como se explica a continuación

#### 3.2.1.1. Créditos del presupuesto votado

Millones de euros (con tres decimales)

| **Rúbrica del marco financiero plurianual** | Número | |
|---|---|---|

| DG: <…….> | | | Año | Año | Año | Año | **TOTAL MFF 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 con cargo a la dotación de programas específicos[44] | | | | | | | |
| Línea presupuestaria | | (3) | | | | | **0,000** |
| **TOTAL de créditos para DG** <…….> | Compromisos | =1a+1b+3 | **0,00** | **0,00** | **0,00** | **0,00** | **0,00** |
| | Pagos | =2a+2b+3 | **0,000** | **0,000** | **0,00** | **0,00** | **0,000** |

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

Esta sección debe completarse utilizando los «datos presupuestarios de carácter administrativo» que deben insertarse en primer lugar en el anexo de la ficha financiera legislativa y digital (anexo 5[45] de la Decisión de la Comisión sobre las normas internas para la ejecución de la sección de la Comisión del presupuesto general de la Unión Europea), que se carga en DECIDE con fines de consulta entre servicios.

| DG: <…….> | | Año **2024** | Año **2025** | Año **2026** | Año **2027** | **TOTAL MFF 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 DG** <…….> | Asignaciones | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| DG: <…….> | | Año **2024** | Año **2025** | Año **2026** | Año **2027** | **TOTAL MFF 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 DG** <…….> | Asignaciones | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Total de 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** |

Millones de euros (con tres decimales)

| | Año | Año | Año | Año | **TOTAL MFF** |
|---|---|---|---|---|---|

[45] Si informa sobre el uso de los créditos de la rúbrica 7, es obligatorio cumplimentar el anexo 5.

| | | 2024 | 2025 | 2026 | 2027 | 2021-2027 |
|---|---|---|---|---|---|---|
| **TOTAL de créditos en las RÚBRICAS 1 a 7** | Compromisos | **0,000** | **0,00** | **0,00** | **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 externos asignados

Millones de euros (con tres decimales)

| **Rúbrica del marco financiero plurianual** | Número | |
|---|---|---|

| DG: <…….> | | | Año 2024 | Año 2025 | Año 2026 | Año 2027 | **TOTAL MFF 2021-2027** |
|---|---|---|---|---|---|---|---|
| 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 con cargo a la dotación de programas específicos[46] | | | | | | | |
| Línea presupuestaria | | (3) | | | | | **0,000** |
| **TOTAL de créditos para DG** <…….> | Compromisos | =1a+1b+3 | **0,00** | **0,00** | **0,00** | **0,00** | **0,00** |
| | Pagos | =2a+2b+3 | **0,000** | **0,000** | **0,00** | **0,00** | **0,00** |

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

| Rúbrica del marco financiero plurianual | 7 | «Gastos administrativos »[47] |
|---|---|---|

Millones de euros (con tres decimales)

| DG: <…….> | | Año 2024 | Año 2025 | Año 2026 | Año 2027 | TOTAL MFF 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 | **0,00** |
| **TOTAL DG** <…….> | Asignaciones | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| DG: <…….> | | Año 2024 | Año 2025 | Año 2026 | Año 2027 | TOTAL MFF 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 DG** <…….> | Asignaciones | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| **Total de 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** |
|---|---|---|---|---|---|---|

Millones de euros (con tres decimales)

| | Año 2024 | Año 2025 | Año 2026 | Año 2027 | TOTAL MFP 2021-2027 |
|---|---|---|---|---|---|

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Total de créditos de las RÚBRICAS 1 a 7** | Compromisos | **0,000** | **0,00** | **0,00** | **0,000** | **0,000** |
| del marco financiero plurianual | Pagos | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

*3.2.2. Resultados previstos financiados con créditos operativos (no se completará en el caso de las agencias descentralizadas)*

Créditos de compromiso en millones de euros (con tres decimales)

| **Indique los objetivos y los resultados** ⇩ | | | Año **2024** | | Año **2025** | | Año **2026** | | Año **2027** | | Introduzca tantos años como sea necesario para mostrar la duración del impacto (véase la sección 1.6). | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **RESULTADOS** | | | | | | | | | | | | | | | |
| | Tipo [48] | Coste medio | No | Coste | No | Coste | No | Coste | No | Coste | No | Coste | No | Coste | No | Coste | Total No | 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 deben suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidas, etc.).
[49] Tal y como se describe en la sección 1.3.2. «Objetivo(s) específico(s)»

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Subtotal para el objetivo específico n.º 2 | | | | | | | | | | | | | | | | |
| **TOTALES** | | | | | | | | | | | | | | | | |

### *3.2.3. Resumen del impacto estimado en los créditos administrativos*

☒La propuesta/iniciativa no requiere el uso de créditos de carácter administrativo

☐ La propuesta/iniciativa requiere el uso de créditos de carácter administrativo, tal y como se explica a continuación

#### 3.2.3.1. Créditos del presupuesto votado

| **CRÉDITOS APROBADOS** | Año **2024** | Año **2025** | Año **2026** | Año **2027** | **TOTAL 2021 - 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 RÚBRICA 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| **Fuera 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 fuera de la RÚBRICA 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,00** |
| | | | | | |
| **TOTAL** | **0,000** | **0,000** | **0,000** | **0,000** | **0,00** |

Los créditos necesarios para los recursos humanos y otros gastos de carácter administrativo se sufragarán con créditos de la DG ya asignados a la gestión de la acción y/o reasignados dentro de la DG, junto con, en su caso, cualquier asignación adicional que pueda concederse a la DG gestora en el marco del procedimiento de asignación anual y teniendo en cuenta las restricciones presupuestarias.

### *3.2.4. Necesidades estimadas de recursos humanos*

☒La propuesta/iniciativa no requiere el uso de recursos humanos

☐ La propuesta/iniciativa requiere el uso de recursos humanos, tal y como se explica a continuación

#### 3.2.4.1. Financiado con cargo al presupuesto votado

*Estimación expresada en unidades equivalentes a tiempo completo (ETC)*[50]

17.

| **CRÉDITOS APROBADOS** | Año **2024** | Año **2025** | Año **2026** | Año **2027** |
|---|---|---|---|---|
| • **Puestos de la 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 UE) | 0 | 0 | 0 | 0 |
| 01 01 01 01 (Investigación indirecta) | 0 | 0 | 0 | 0 |

[50] Especifique debajo del cuadro cuántos ETC del número indicado ya están asignados a la gestión de la acción y/o pueden reasignarse dentro de su DG y cuáles son sus necesidades netas.

| | | | | | |
|---|---|---|---|---|---|
| 01 01 01 11 (Investigación directa) | | 0 | 0 | 0 | 0 |
| Otras líneas presupuestarias (especificar) | | 0 | 0 | 0 | 0 |
| • **Personal externo (en ETC)** | | | | | |
| 20 02 01 (AC, FINAL de la «dotación global») | | 0 | 0 | 0 | 0 |
| 20 02 03 (AC, AL, FIN y JPD en las delegaciones de la UE) | | 0 | 0 | 0 | 0 |
| Línea de apoyo administrativo [XX.01.YY.YY] | - en la sede central | 0 | 0 | 0 | 0 |
| | - En las delegaciones de la UE | 0 | 0 | 0 | 0 |
| 01 01 01 02 (AC, END - Investigación indirecta) | | 0 | 0 | 0 | 0 |
| 01 01 01 12 (AC, END - Investigación directa) | | 0 | 0 | 0 | 0 |
| Otras líneas presupuestarias (especificar) - Rúbrica 7 | | 0 | 0 | 0 | 0 |
| Otras líneas presupuestarias (especificar) - Fuera de la rúbrica 7 | | 0 | 0 | 0 | 0 |
| **TOTAL** | | **0** | **0** | **0** | **0** |

*3.2.5. Resumen del impacto estimado en las inversiones relacionadas con la tecnología digital*

18. Obligatorio: en el cuadro siguiente debe figurar la mejor estimación de las inversiones relacionadas con la tecnología digital que conlleva la propuesta o iniciativa.

19. Excepcionalmente, cuando sea necesario para la ejecución de la propuesta o iniciativa, los créditos de la rúbrica 7 deberán presentarse en la línea designada.

20. Los créditos de las rúbricas 1 a 6 deben reflejarse como «Gastos de TI relacionados con las políticas en programas operativos». Estos gastos se refieren al presupuesto operativo que se utilizará para reutilizar, adquirir o desarrollar plataformas o herramientas de TI directamente vinculadas a la ejecución de la iniciativa y las inversiones asociadas (por ejemplo, licencias, estudios, almacenamiento de datos, etc.). La información facilitada en este cuadro debe ser coherente con los datos presentados en la sección 4, «Dimensiones digitales».

| **TOTAL Créditos digitales y de TI** | Año **2024** | Año **2025** | Año **2026** | Año **2027** | **TOTAL MFF 2021 - 2027** |
|---|---|---|---|---|---|
| **RÚBRICA 7** | | | | | |
| Gastos de TI (corporativos) | 0,00 | 0,00 | 0,00 | 0,00 | **0,000** |
| **Subtotal RÚBRICA 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,00** |
| **Fuera de la RÚBRICA 7** | | | | | |
| Gastos de política en TI para programas operativos | 0,000 | 0,000 | 0,000 | 0,000 | **0,00** |
| **Subtotal fuera 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 o iniciativa:

☒puede financiarse íntegramente mediante una redistribución dentro de la rúbrica pertinente del marco financiero plurianual (MFP)

☐ requiere el uso del margen no asignado en la rúbrica pertinente del MFP y/o el uso de los instrumentos especiales definidos en el Reglamento del MFP

☐ requiere una revisión del MFP

*3.2.7. Contribuciones de terceros*

22. La propuesta o iniciativa:

☒no prevé la cofinanciación por terceros

☐ prevé la cofinanciación por terceros estimada a continuación:

Asignaciones en millones de euros (con tres decimales)

| | Año **2024** | Año **2025** | Año **2026** | Año **2027** | Total |
|---|---|---|---|---|---|
| Especifique el organismo cofinanciador | | | | | |
| Total de créditos cofinanciados | | | | | |

3.3. Incidencia estimada en los ingresos

☒La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene las siguientes repercusiones financieras:

– ☐ sobre los recursos propios

– ☐ sobre otros ingresos

– ☐ indíquese si los ingresos se asignan a líneas de gasto

Millones de euros (con tres decimales)

| Línea presupuestaria de ingresos: | Créditos disponibles para el ejercicio financiero actual | Incidencia de la propuesta o iniciativa[51] | | | |
|---|---|---|---|---|---|
| | | Año **2024** | Año **2025** | Año **2026** | Año **2027** |
| Artículo …….. | | | | | |

23. Para los ingresos asignados, especifique la(s) línea(s) presupuestaria(s) de gastos afectada(s).

24. […]

25. Otras observaciones (por ejemplo, método o fórmula utilizados para calcular el impacto en los ingresos o cualquier otra información).

[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 tras deducir el 20 % en concepto de gastos de recaudación.

26. […]

27. 4. DIMENSIONES DIGITALES

## 4.1. Requisitos de relevancia digital

*Descripción general de los requisitos de relevancia digital y categorías relacionadas (datos, digitalización y automatización de procesos, soluciones digitales y/o servicios públicos digitales)*

| **Referencia al requisito** | **Descripción del requisito** | **Actores afectados o interesados por el requisito** | **Procesos de alto nivel** | **Categorías** |
|---|---|---|---|---|
| Artículo 1 | Modificación del artículo 1, apartado 1, de la Ley de datos, ampliando su ámbito de aplicación al establecimiento de lo siguiente:<br>• un marco para el registro de los servicios de intermediación de datos;<br>• un marco para el registro voluntario de entidades que recopilan y tratan datos puestos a disposición con fines altruistas;<br>• un marco para la creación de un Comité Europeo de Innovación en materia de Datos. | Comisión Europea<br>Servicios de intermediación de datos<br>Entidades de recogida y tratamiento de datos | Ampliación del ámbito de aplicación de la Ley de Datos | Servicio público digital |
| Artículo 1 | Modificación de los artículos 4(8) y 5(11) de la Ley de Datos. Los titulares de datos que se nieguen a compartir datos en virtud de la excepción relativa a los secretos comerciales deberán notificar adecuadamente dicha decisión. | Titulares de datos (titulares de secretos comerciales)<br>Solicitantes de acceso | Notificación | Datos |

| | | | | |
|---|---|---|---|---|
| Artículo 1 | Inserción del artículo 15 bis en la Ley de Datos. Obligación de poner a disposición los datos en caso de emergencia pública. | Organismo del sector público<br>Comisión Europea Banco Central Europeo Órgano de la Unión<br>Titulares de datos | Poner los datos a disposición | Datos |
| Artículo 1 | Modificación del artículo 21, apartado 5, de la Ley de Datos. Requisitos relativos al intercambio de datos obtenidos en el contexto de una emergencia pública con organismos de investigación u organismos estadísticos.<br>Inserción del artículo 22 bis en la Ley de Datos, que permite presentar reclamaciones en relación con el capítulo V (*«Puesta a disposición de datos a organismos del sector público, la Comisión, el Banco Central Europeo y organismos de la Unión sobre la base de una necesidad excepcional»*). | Organismo del sector público<br>Comisión Europea Banco Central Europeo Órgano de la Unión<br>Titular de los datos<br>Autoridad nacional competente | Intercambio de datos<br>Reclamaciones | Datos |
| Artículo 1 | Modificaciones del artículo 32, apartados 1 a 5, de la Ley de datos sobre el acceso de terceros países a datos no personales. | Proveedores de servicios de tratamiento de datos<br>Proveedores de servicios de intermediación de datos<br>Organizaciones de altruismo de datos<br>Organismos o autoridades nacionales | Acceso y transferencia internacional de datos gubernamentales | Datos<br>Servicio público digital |

| | | | | |
|---|---|---|---|---|
| Artículo 1 | Modificación del artículo 35, apartado 5, de la Ley de Datos, que permite a la Comisión adoptar especificaciones comunes en relación con la interoperabilidad de los servicios de tratamiento de datos. | Proveedores de servicios de tratamiento de datos<br>Comisión Europea | Adopción de especificaciones comunes | Servicio público digital |
| Artículo 1 | Modificaciones de los artículos 32 bis a 32 sexies de la Ley de Datos para introducir el capítulo VII bis sobre el marco regulador de una etiqueta europea para los servicios de intermediación de datos, que incluye la notificación, la creación de un registro público, las condiciones para la prestación de servicios, la designación de las autoridades competentes y el control del cumplimiento.<br>Modificaciones del artículo 32 nonies de la Ley de Datos para introducir el capítulo VII ter sobre la libre circulación de datos dentro de la Unión, incluida la prohibición de los requisitos de localización de datos, las obligaciones de notificación a la Comisión y la publicación de una lista consolidada. | Proveedores de servicios de intermediación de datos<br>Interesados, titulares de datos, usuarios de datos<br>Estados miembros<br>Autoridades competentes<br>Comisión Europea | Establecimiento de la etiqueta europea para los servicios de intermediación de datos<br>Establecimiento de la libre circulación de datos dentro de la Unión Europea | Datos<br>Solución digital<br>Digitalización de procesos<br>Servicio público digital |

| | | | | |
|---|---|---|---|---|
| Artículo 1 | Modificaciones del artículo 32 nonies de la Ley de Datos para introducir el capítulo VII ter sobre la libre circulación de datos dentro de la Unión, incluida 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<br>Comisión Europea | Establecimiento de la libre circulación de datos dentro de la Unión Europea | Proceso<br>de datos<br>Digitalización<br>Servicio público digital |
| Artículo 1 | Inserción del artículo 32i en la Ley de Datos, en el que se define el ámbito de aplicación del capítulo VIIc. En él se establece un conjunto de normas mínimas que regulan la reutilización y las disposiciones prácticas para facilitar la reutilización de los datos.<br>Inserción del artículo 32 undecies en la Ley de datos; disposición sobre la no discriminación en lo que respecta a la reutilización de datos y documentos. | Estados<br>miembros<br>Titulares de datos<br>Usuarios de datos | Definición del objeto y el ámbito de aplicación<br>No discriminación | Servicio público digital |
| Artículo 1 | Inserción del artículo 32k en la Ley de Datos. Normas relativas a los acuerdos exclusivos para la reutilización de datos. Incluye la obligación de hacer públicos los términos definitivos de los acuerdos. | Posibles actores en el mercado<br>Organismos del sector público | | Servicio público digital<br>Datos |

| | | | | |
|---|---|---|---|---|
| | disponibles. | Partes en dichos acuerdos | | |
| Artículo 1 | Modificaciones de la Ley de Datos:<br>• (41): Inserción del artículo 32-novies sobre el principio general de reutilización de los datos abiertos de la Administración.<br>• (42): Inserción del artículo 32o sobre la tramitación de las solicitudes de reutilización de datos.<br>• (43): Inserción del artículo 32p sobre los formatos para la reutilización de datos.<br>• (46): Inserción del artículo 32 septies sobre disposiciones prácticas que facilitan la búsqueda de datos o documentos disponibles para su reutilización. | Titulares de datos Usuarios de datos<br>Estados miembros (organismos del sector público)<br>Comisión Europea | Normas de reutilización de datos | Servicio público digital<br>Proceso de datos Digitalización |
| Artículo 1 | Inserción del artículo 32 ter en la Ley de Datos; obligación de apoyar la disponibilidad de los datos de investigación. | Estados miembros<br>Organizaciones de investigación<br>Usuarios de datos | Normas de reutilización de datos | Servicio público digital<br>Datos |
| Artículo 1 | Inserción del artículo 32u en la Ley de Datos. Establecimiento de disposiciones para la publicación y reutilización de conjuntos de datos específicos de alto valor. | Comisión Europea<br>Organismos del sector público, empresas públicas | Normas de reutilización de datos | Servicio público digital<br>Datos |
| Artículo 1 | Incorporación del artículo 32w a la Ley de Datos. Establecimiento de las condiciones para la reutilización de determinadas categorías de datos. Los procedimientos para solicitar y las condiciones para | Organismos del sector público Usuarios de datos | Normas de reutilización de datos | Servicio público digital<br>Los datos |

| | | | | |
|---|---|---|---|---|
| | que permiten dicha reutilización se pondrán a disposición del público a través del punto único de información. | | | |
| Artículo 1 | Inserción del artículo 32x en la Ley de Datos; requisitos para la transferencia de datos no personales a terceros países por parte de los reutilizadores. | Reutilizadores de datos<br>Organismos del sector público<br>Personas físicas o jurídicas cuyos derechos puedan verse afectados | Transferencia de datos a terceros países | Servicio público digital<br>Datos |
| Artículo 1 | Modificaciones de la Ley de datos:<br>• (55): Inserción del artículo 32z; medidas organizativas relativas a los organismos competentes.<br>• (57): Inserción del artículo 32ab sobre los procedimientos para las solicitudes de reutilización de datos.<br>• (58): Sustitución del artículo 38, apartados 1 y 2, sobre el derecho a presentar una reclamación. | Órganos competentes<br>Estados miembros<br>Órganos del sector público | Establecimiento de organismos competentes<br>Procedimientos de solicitud<br>Reclamaciones | Servicio público digital<br>Datos |
| Artículo 1 | Inserción del artículo 32 bis en la Ley de Datos. Obligatoriedad del uso de un punto único de información para facilitar la reutilización de datos. | Estados miembros<br>Titulares de datos<br>Usuarios de datos<br>Comisión Europea. | Establecimiento de un punto de acceso único | Soluciones digitales<br>Servicio público digital<br>Digitalización de procesos<br>Datos |

| | | | | |
|---|---|---|---|---|
| Artículo 1 | Modificaciones de los artículos 41 bis, 42, 45, 46, 48 bis, 49 y 49 bis de la Ley de Datos para introducir el capítulo IX bis, por el que se establece el Comité Europeo de Innovación en materia de Datos (EDIB) como grupo de expertos encargado de coordinar la aplicación de la normativa y facilitar el desarrollo de una economía europea de datos, incluidos los requisitos de composición, la función, la facilitación de la cooperación entre las autoridades competentes y el apoyo a la aplicación coherente de los requisitos legales. | Comisión Europea, Comité Europeo de Innovación en materia de Datos (EDIB)<br><br>Representantes de los Estados miembros competentes en materia de política de economía de datos<br><br>Autoridades competentes para la aplicación de los capítulos II, III y V<br><br>Autoridades competentes para la reutilización de la información del sector público (Directiva sobre datos abiertos)<br><br>Autoridades competentes para los servicios de intermediación de datos<br><br>Autoridades competentes para el registro de organizaciones de altruismo de datos<br><br>Comité Europeo de Protección de Datos (CEPD), Supervisor Europeo de Protección de Datos (SEPD)<br><br>ENISA (Agencia de la Unión Europea para la Ciberseguridad) | Creación del Comité Europeo de Innovación en materia de Datos (EDIB) | Servicio público digital<br><br>Datos |

| | | | | |
|---|---|---|---|---|
| | | Enviado de la UE para las pymes o representante de la red de enviados para las pymes<br>Otros representantes de organismos pertinentes en sectores específicos<br>Organismos con conocimientos específicos<br>Organismos de normalización<br>Parlamento Europeo, Consejo de la Unión Europea, Comité Económico y Social Europeo<br>Proveedores de servicios de intermediación de datos<br>Organizaciones reconocidas de altruismo de datos | | |
| Artículo 3 | Modificación del artículo 33 del Reglamento (UE) 2016/679 (RGPD), en lo que respecta a las notificaciones de violaciones de datos personales. Entre otras cosas, exige el uso del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 y prevé el uso de plantillas de notificación. | Interesados<br>Responsables del tratamiento<br>Autoridades de control<br>Comité Europeo de Protección de Datos<br>Comisión Europea | Notificación | Datos |

| | | | | |
|---|---|---|---|---|
| Artículo 3 | Modificación de los artículos 35 y 70, apartado 1, del Reglamento (UE) 2016/679 (RGPD). Obligación de la Junta Europea de Protección de Datos de transmitir a la Comisión propuestas para seguir desarrollando determinados aspectos de la evaluación de impacto relativa a la protección de datos. Entre ellos figura una plantilla común para dichas evaluaciones. | Comité Europeo de Protección de Datos<br>Comisión Europea | Propuestas del Comité transmitidas a la Comisión | Datos |
| Artículo 3 | Inserción del artículo 88 ter en el Reglamento (UE) 2016/679 (RGPD); los interesados podrán dar su consentimiento o ejercer su derecho de oposición por medios automatizados y legibles por máquina. Se prevé que las normas sean elaboradas por una o varias organizaciones europeas de normalización. | Interesados<br>Responsables del tratamiento<br>Organismos europeos de normalización<br>Comisión Europea | Indicaciones automatizadas y legibles por máquina de las elecciones de los interesados | Soluciones digitales<br>Automatización de procesos |
| Artículo 6 | Modificación de la Directiva (UE) 2022/2555 (NIS2):<br>• (1): Inserción del artículo 23 bis sobre el desarrollo y mantenimiento de un punto único de entrada para la notificación de incidentes.<br>• (3): Modificar el artículo 23, apartado 4, para exigir el uso del punto único de entrada para las notificaciones de incidentes graves.<br>• (4): Insertar el artículo 23, apartado 12, que garantiza que los incidentes graves solo se notifiquen una vez (ya sea en virtud de | Notificadores (entidades esenciales e importantes)<br>CSIRT/autoridades competentes (según proceda)<br>Comisión Europea ENISA | Notificación | Datos<br>Soluciones digitales<br>Servicio público digital |

| | | | | |
|---|---|---|---|---|
| | NIS2, o en virtud de la Ley de Ciberresiliencia);<br>• (5): Modificación del artículo 30, apartado 1, para garantizar que el punto de entrada único pueda utilizarse, de forma voluntaria, para las notificaciones de diferentes entidades. | | | |
| Artículo 7 | Modificación del Reglamento (UE) n.º 910/2014 (EUDIW) que exige el uso del punto de entrada único, de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555, para:<br>• Artículo 19 bis, apartado 1 bis: Notificaciones a que se refiere el apartado 1, letra b).<br>• Artículo 24, apartado 2 bis: Notificaciones a que se refiere el apartado 2, letra f ter). Artículo 45 bis, apartado 3 bis: Notificaciones a que se refiere el apartado 3. | Notificantes (prestadores de servicios de confianza no cualificados; prestadores de servicios de confianza cualificados; proveedores de un navegador web)<br>Órganos de supervisión<br>Otros organismos o autoridades competentes pertinentes<br>Comisión Europea | Notificación | Datos |

| | | | | |
|---|---|---|---|---|
| Artículo 8 | Modificación del Reglamento (UE) 2022/2554 (DORA) que exige el uso del punto de entrada único, de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555, para:<br>• Artículo 19, apartado 1: Incidentes graves relacionados con las TIC<br>• Artículo 19, apartado 2: notificaciones voluntarias de amenazas cibernéticas significativas. | Notificantes (entidades financieras)<br>Órganos de supervisión<br>Otros organismos o autoridades competentes pertinentes<br>Comisión Europea ENISA | Notificación | Datos |
| Artículo 9 | Modificación de la Directiva (UE) 2022/2557 (CER) que exige el uso del punto de entrada único, de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555, para:<br>• Artículo 15, apartado 1: Incidentes que perturban o pueden perturbar de manera significativa la prestación de servicios esenciales. | Notificantes (entidades críticas)<br>Órganos de supervisión<br>Otros organismos o autoridades competentes pertinentes<br>Comisión Europea ENISA | Notificación | Datos |

### 4.2. Datos

*Descripción general de los datos incluidos en el ámbito de aplicación*

| **Tipo de datos** | **Referencia al requisito o requisitos** | **Norma y/o especificación (si procede)** |
|---|---|---|
| Denegación de una solicitud de acceso a datos basada en la excepción del secreto comercial (*y notificación de la misma a la autoridad competente*) | Artículo 1 | Debe estar debidamente justificado sobre la base de elementos objetivos. |
| Datos que deben ponerse a disposición en el contexto de una emergencia pública | Artículo 1 | Incluidos los metadatos necesarios para interpretar y utilizar los datos. En el caso de los datos personales, se utilizarán seudónimos siempre que sea posible. |
| Notificación de la intención de poner a disposición datos en el contexto de una emergencia pública | Artículo 1 | Indicando la identidad y los datos de contacto de la organización o la persona que recibe los datos, la finalidad de la transmisión o puesta a disposición de los datos, el período durante el cual se utilizarán los datos y las medidas técnicas de protección y organizativas adoptadas. |
| Reclamaciones en virtud del capítulo V (*«Puesta a disposición de datos a organismos del sector público, la Comisión, el Banco Central Europeo y organismos de la Unión sobre la base de una* necesidad excepcional») | 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 permitida |

| | | |
|---|---|---|
| Notificación de la solicitud de reutilización de datos que está a punto de 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 altruismo de datos) | Artículo 1 | Formato recibido del interesado/titular de los datos, conversiones solo para mejorar la interoperabilidad o cumplir con las normas internacionales/europeas sobre datos |
| Información sobre los usos y condiciones de los datos (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | Debe proporcionarse de forma concisa, transparente, inteligible y fácilmente accesible |
| Solicitudes de inscripción en el registro público de la Unión y modificaciones de la información notificada (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1 | Las autoridades competentes establecerán los formularios de solicitud necesarios. |
| Solicitudes de inscripción aceptadas para su inclusión en el registro público de la Unión (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1 | // |
| Notificación de cambios posteriores a la información facilitada durante el proceso de solicitud (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1 | // |
| Recepción de la notificación de cambios posteriores (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | // |
| Información facilitada a los interesados/titulares de los datos antes del tratamiento (etiqueta europea para datos | Artículo 1 | // |

| | | |
|---|---|---|
| servicios de intermediación de datos y organizaciones de altruismo de datos) | | |
| Consentimiento (o retirada del consentimiento) para el tratamiento de datos por parte de una organización reconocida de altruismo de datos (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | Obtenible por medios electrónicos |
| Información sobre la jurisdicción de terceros países en la que se pretende utilizar los datos | Artículo 1 | // |
| Notificación de transferencias, accesos o usos no autorizados de datos no personales (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | // |
| Información para el control del cumplimiento (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | Las solicitudes deben ser proporcionadas y estar motivadas |
| Notificación de incumplimiento (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1 | // |
| Decisión de revocar el derecho a utilizar la etiqueta (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1 | // |
| Proyectos de ley sobre los requisitos de localización de datos | Artículo 1 | // |

| | | |
|---|---|---|
| Condiciones definitivas de los acuerdos exclusivos | Artículo 1 | // |
| Datos (y/o notificaciones) relativos a una solicitud de reutilización | Artículo 1 | En cualquier formato o idioma 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 investigación financiados con fondos públicos | Artículo 1 | Disponibles de forma abierta, siguiendo el principio de «abiertos por defecto» y compatibles con los principios FAIR. |
| Conjuntos de datos específicos de alto valor | Artículo 1 | Disponibles de forma gratuita; legibles por máquina; proporcionados a través de API y como descarga masiva (cuando sea pertinente). Se aplicarán actos de ejecución, que podrán 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 | Disponibles públicamente. |
| Notificación de la reutilización no autorizada de datos no personales | Artículo 1 | // |
| Notificación de la intención de transferir datos no personales a un tercer país y 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 32z [condiciones para la reutilización], 32aa [terceros países] y 32ab [tasas] de la Ley de datos. | Artículo 1 | Disponible y fácilmente accesible a través de un único punto de información. |
| Reclamación presentada por personas físicas o jurídicas en caso de que se hayan vulnerado sus derechos en virtud de la Ley de datos o en relación con otras cuestiones pertinentes. | Artículo 1 | // |
| Información sobre el curso de los procedimientos/recursos judiciales en relación con una reclamación presentada en virtud de la Ley de datos. | Artículo 1 | // |
| Datos sobre experiencias y buenas prácticas (EDIB) | Artículo 1 | // |
| Evaluación de los capítulos II, III, IV, V, VI, VII y VIII de la Ley de Datos<br>Evaluación de los capítulos VIIa, VIIb y VIIc de la Ley de Datos | Artículo 1<br>Artículo 1 | Se establecen los requisitos mínimos de contenido de los informes. |
| Notificaciones de violaciones de datos personales | Artículo 3 | A través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 (y respetando, por tanto, sus especificaciones).<br>El Comité Europeo de Protección de Datos elaborará una propuesta de plantilla común (*véase la siguiente entrada*). |
| Propuesta del CEPD para una plantilla común de notificación de violaciones de datos | Artículo 3 | // |

| | | |
|---|---|---|
| Propuestas del CEPD relativas a la evaluación del impacto de la protección de datos | Artículo 3 | // |
| Informes sobre incidentes significativos de conformidad con la Directiva NIS2 | Artículo 6 | A través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 (y respetando, por tanto, sus especificaciones). |
| Notificaciones de violaciones de datos personales | Artículo 3 | A través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 (y respetando, por tanto, las especificaciones del mismo). |
| Notificaciones de incidentes graves relacionados con las TIC de conformidad con el Reglamento DORA; notificaciones voluntarias de amenazas cibernéticas significativas de conformidad con el Reglamento DORA. | Artículo 8 | A través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 (y respetando, por tanto, las especificaciones del mismo) |
| Notificaciones de incidentes que perturben significativamente o puedan perturbar significativamente la prestación de servicios esenciales, de conformidad con la Directiva CER | Artículo 9 | A través del punto de entrada único establecido de conformidad con el artículo 23 bis de la Directiva (UE) 2022/2555 (y respetando, por tanto, sus especificaciones). |

**Alineación con la Estrategia Europea de Datos**

*Explicación de cómo los requisitos se ajustan a la Estrategia Europea de Datos*

Estas modificaciones de la Ley de Datos introducen la EDIB (capítulo IX bis), que coordina la aplicación de las normas y elabora directrices para los espacios de datos europeos comunes sectoriales; las etiquetas europeas para los servicios de intermediación de datos y las organizaciones de altruismo de datos (capítulo VII bis), que crean un ecosistema fiable para el intercambio de datos con protección de derechos; el capítulo VII ter aplica la libre circulación de datos no personales prohibiendo los requisitos injustificados de localización de datos; El capítulo VIIc racionaliza las normas sobre la reutilización de los datos del sector público, fusionando las disposiciones de la Directiva sobre datos abiertos y la Ley de gobernanza de datos; las normas sobre transferencias internacionales de datos refuerzan la soberanía digital europea al proteger los datos del acceso no autorizado de terceros países; por último, las exenciones para las pymes y la presencia del enviado de la UE para las pymes en la EDIB garantizan que la economía de datos sea también más accesible para las pequeñas empresas.

**Alineación con el principio de «una sola vez»**

*Explicación de cómo se ha tenido en cuenta el principio de «una sola vez» y cómo se ha estudiado la posibilidad de reutilizar los datos existentes.*

Estas modificaciones respaldan el principio de «una sola vez» mediante la creación de una infraestructura para la reutilización eficiente de los datos: la EDIB desarrolla normas de interoperabilidad en los espacios comunes de datos europeos para reducir la duplicación en el suministro de datos; los servicios de intermediación de datos actúan como intermediarios de confianza que permiten compartir de forma segura los datos existentes, eliminando la recopilación redundante; las organizaciones de altruismo de datos facilitan el intercambio voluntario de datos en beneficio del público, poniendo a disposición datos reutilizables para la investigación y los servicios públicos; las disposiciones sobre libre circulación evitan las barreras que exigen el almacenamiento duplicado en diferentes lugares; y las garantías de transferencia internacional aseguran la accesibilidad transfronteriza de los datos, al tiempo que mantienen la protección, lo que permite colectivamente a las personas y las empresas proporcionar sus datos una sola vez y satisfacer las necesidades posteriores mediante mecanismos de intercambio seguros y respetuosos con los derechos. Mientras tanto, las disposiciones relativas al punto de entrada único refuerzan el principio de «una sola vez» en lo que respecta a la notificación de incidentes.

*Explicación de cómo los datos recién creados son localizables, accesibles, interoperables y reutilizables, y cumplen con altos estándares de calidad*

Estas modificaciones garantizan que los datos de nueva creación cumplan los principios FAIR y los estándares de calidad mediante mecanismos coordinados: la EDIB desarrolla especificaciones técnicas comunes y protocolos de interoperabilidad accesibles en todos los espacios de datos sectoriales; las disposiciones sobre libre circulación evitan la fragmentación que socava la calidad de los datos; la función de coordinación de la EDIB puede permitir la aplicación armonizada de normas de metadatos, requisitos técnicos y parámetros 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. Concretamente, las disposiciones de la Ley de gobernanza de datos se transfieren a la Ley de datos.*

| **Tipo de datos** | **Referencia(s) al requisito(s)** | **Actores que proporcionan los datos** | **Actores que reciben los datos** | **Desencadenante del intercambio de datos** | **Frecuencia (si procede)** |
|---|---|---|---|---|---|
| Denegación de una solicitud de acceso a datos basada en la excepción del secreto comercial (*y notificación* | Artículo 1<br>*Modificación de los artículos 4, apartado 8, y 5, apartado 11, del* | Titular de los datos | Usuario de los datos (que presenta la solicitud); Competente | Denegación de una solicitud de acceso a datos basada en el secreto comercial | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| *de los mismos a la autoridad competente*) | *Ley de datos* | | designada de conformidad con el artículo 37 | excepción | |
| Datos que deben ponerse a disposición en el contexto de una emergencia pública | Artículo 1<br>*Inserción del artículo 15 bis en la Ley de datos* | Titular de los datos | Organismo del sector público; Comisión Europea; Banco Central Europeo; organismo de la Unión | Emergencia pública + Solicitud de acceso a datos que cumplan las condiciones necesarias | Ad hoc |
| Notificación de la intención de poner a disposición los datos en el contexto de una emergencia pública | Artículo 1<br>*Modificación del artículo 21, apartado 5, de la Ley de Datos* | Organismo del sector público; Comisión Europea; Banco Central Europeo; organismo de la Unión | Titular de los datos de quien se recibieron los datos | Emergencia pública + intención de transmitir o poner a disposición los datos | Ad hoc |
| Reclamaciones en virtud del capítulo V («Puesta a disposición de los datos a los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión sobre la base de una necesidad excepcional») | Artículo 1<br>*Inserción del artículo 22 bis en la Ley de Datos* | Titular de los datos; organismo del sector público; Comisión Europea; Banco Central Europeo; organismo de la Unión | Autoridad competente del Estado miembro en el que está establecido el titular de los datos | Cuando surja un litigio en relación con una solicitud de datos en virtud del artículo 15 bis de la Ley de Datos | Ad hoc |
| Datos no personales conservados en la Unión Europea | Artículo 1<br>*Modificación de los siguientes artículos de la Ley de Datos:*<br>*Artículo 32, apartado 1, artículo 32(3), artículo 32(4)* | Proveedores de servicios de tratamiento de datos, proveedores de servicios de intermediación de datos, organizaciones de altruismo de datos | Tribunales de terceros países,<br>Autoridades administrativas de terceros países, Clientes (titulares/interesados de los datos) | Solicitud de terceros países basada en un acuerdo internacional, solicitud de terceros países que cumple las condiciones del artículo 32, apartado 3, solicitud de clientes para acceso a sus propios | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| | | | | datos | |
| Datos que deben facilitarse en respuesta a una solicitud de reutilización de datos | Artículo 1<br>*Modificación del artículo 32, apartados 4 y 5, de la Ley de datos* | Proveedor de servicios de intermediación de datos u organización reconocida de altruismo de datos | El originador de la solicitud de reutilización de datos (autoridad de un tercer país) | Fecha de concesión de la solicitud de reutilización | Ad hoc |
| Notificación de la solicitud de reutilización de datos a punto de concederse | Artículo 1<br>*Modificación del artículo 32, apartados 4 y 5, de la Ley de Datos* | Proveedor de servicios de intermediación de datos u organización reconocida de altruismo de datos | Cliente | Solicitud de reutilización de datos de una autoridad de un tercer país concedida (*excepto cuando la solicitud tenga fines policiales*) | Ad hoc |
| Información que debe publicarse en los registros públicos (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 bis en la Ley de Datos* | Comisión Europea | Público | La información sobre los servicios de intermediación de datos o las organizaciones de altruismo de datos reconocidos está disponible o es necesario modificarla. | En curso (registro actualizado periódicamente) |
| Datos para los que se prestan servicios de intermediación (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 quater en la Ley de datos* | Interesados Titulares de datos | Usuarios de datos (a través del proveedor de servicios de intermediación de datos) | Consentimiento del interesado Permiso del titular de los datos Solicitud del usuario de datos | Según el acuerdo/contrato entre las partes |

| | | | | | |
|---|---|---|---|---|---|
| Información sobre los usos y condiciones de los datos (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 quater en la Ley de datos* | Proveedor de servicios de intermediación de datos | Interesados | Antes de que el interesado dé su consentimiento para el uso de los datos | Cada vez antes de solicitar el consentimiento |
| Solicitudes de inscripción en el registro público de la Unión y modificaciones de la información notificada (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 sexies en la Ley de datos* | Proveedores de servicios de intermediación de datos<br>Organizaciones de altruismo de datos | Autoridad competente en el Estado miembro de establecimiento principal | Aplicación | Ad hoc |
| Solicitudes de registro aceptadas para su inclusión en el registro público de la Unión (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 sexies en la Ley de Datos* | Autoridad competente | Comisión Europea | Solicitud aprobada | Ad hoc (en un plazo de 12 semanas tras la recepción de la solicitud, siempre que la decisión sea positiva) |
| Notificación de cambios posteriores a la información proporcionada durante el proceso de solicitud (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 sexies en la Ley de datos* | Entidades registradas | Autoridad competente | Cambios en la información facilitada o cuando las entidades cesan sus actividades en la Unión | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| Recepción de la notificación de cambios posteriores (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 sexies en la Ley de datos* | Autoridad competente | Comisión Europea | Las entidades registradas notifican el cambio (véase la entrada anterior) | Ad hoc, sin demora |
| Información facilitada a los interesados/titulares de los datos antes del tratamiento (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 septies en la Ley de Datos* | Organización reconocida de altruismo de datos | Interesados<br>Titulares de<br>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 altruismo de datos (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32f en la Ley de Datos* | Interesados<br>Titulares de datos (si se trata de datos no personales) | Organización de altruismo de datos | Consentimiento del interesado / Permiso del titular de los datos necesario para las actividades de tratamiento | Según el consentimiento/permiso otorgado, con posibilidad de revocarlo en cualquier momento |
| Información sobre la jurisdicción de terceros países en la que se pretende utilizar los datos | Artículo 1<br>*Inserción del artículo 32f en la Ley de Datos* | Organización de altruismo de datos | Titulares de datos | Cuando la organización de altruismo de datos facilita el tratamiento de datos por parte de terceros | Ad hoc |
| Notificación de transferencias, accesos o usos no autorizados de datos no personales (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 septies en la Ley de datos* | Organización de altruismo de datos | Titulares de datos | Acción no autorizada | Ad hoc, sin demora |
| Información para el cumplimiento | Artículo 1 | Datos | Competente | Solicitud de | Ad hoc (previa |

| | | | | | |
|---|---|---|---|---|---|
| supervisión (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | *Inserción del artículo 32g en la Ley de Datos* | proveedores de servicios de intermediación<br>Organizaciones de altruismo de datos | autoridades | Autoridad competente<br>Solicitud de una persona física o jurídica | solicitud, que debe ser proporcionada y motivada) |
| Notificación de incumplimiento (etiqueta europea para servicios de intermediación de datos y organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 octies en la Ley de datos* | Autoridad competente | Entidad que incumple | La autoridad competente determina que un proveedor de servicios de intermediación de datos reconocido o una organización de altruismo de datos reconocida incumple la normativa | Ad hoc (seguido de la oportunidad para que la entidad exponga sus opiniones en un plazo de 30 días) |
| Decisión de revocar el derecho a utilizar la etiqueta (etiqueta europea para los servicios de intermediación de datos y las organizaciones de altruismo de datos) | Artículo 1<br>*Inserción del artículo 32 octies en la Ley de datos* | Autoridad competente | Pública | Tras la decisión de revocación de la etiqueta | Ad hoc |
| Proyectos de ley sobre los requisitos de localización de datos | Artículo 1 | Estados miembros | Comisión Europea | Creación de un proyecto de acto que introduzca un nuevo requisito de localización de datos o modifique un requisito de localización de datos existente | Ad hoc, inmediatamente |
| Condiciones definitivas de los acuerdos exclusivos | Artículo 1 | Partes del acuerdo | Público | Acuerdos exclusivos | Ad hoc, al menos dos meses antes |

| | | | | | |
|---|---|---|---|---|---|
| | | | | establecido a partir del 16 de julio de 2019 | un acuerdo entra en vigor |
| Datos (y/o notificaciones) relativos a una solicitud de reutilización | Artículo 1<br>*Inserción del artículo 32p en la Ley de Datos* | Organismos del sector público | Solicitantes de reutilización de datos | Si se deben proporcionar cualquiera de los siguientes documentos: datos/documentos solicitados; oferta de licencia; notificaciones de retrasos; notificación de una decisión negativa. | Ad hoc |
| Condiciones definitivas de los acuerdos exclusivos | Artículo 1<br>*Inserción del artículo 32k en la Ley de Datos* | Partes de un acuerdo exclusivo | Público en general | Condiciones definitivas de un acuerdo exclusivo que se está alcanzando | Ad hoc |
| Condiciones para permitir la reutilización de los datos o documentos a que se refiere el artículo 2, apartado 54 | Artículo 1<br>*Inserción del artículo 32z en la Ley de Datos* | Organismos del sector público (competentes para conceder o denegar solicitudes de acceso) | Público en general | Cuando conceden la reutilización de datos o documentos | Ad hoc |
| Notificación de reutilización no autorizada de datos no personales | Artículo 1<br>*Inserción del artículo 32z en la Ley de datos* | Reutilizador (posiblemente con la ayuda del organismo del sector público) | Personas físicas o jurídicas cuyos derechos e intereses puedan verse afectados | Reutilización no autorizada realizada | Ad hoc |
| Notificación de la intención de transferir datos no personales a un tercer país y la finalidad de | Artículo 1<br>*Inserción del artículo 32 bis* | Reutilizador | Organismo del sector público | Intención de transferir datos a un tercer país | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| dicha transferencia (al organismo del sector público) | *en la Ley de Datos* | | | | |
| 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<br>*Inserción del artículo 32aa en la Ley de Datos* | Reutilizador (posiblemente con la ayuda del organismo público) | Persona física o jurídica cuyos derechos e intereses puedan verse afectados | Intención de transferir datos a un tercer país | Ad hoc |
| Toda la información pertinente relativa a la aplicación de los artículos 32z [condiciones para la reutilización], 32aa [terceros países] y 32ab [tasas] de la Ley de Datos. | Artículo 1<br>*Inserción del artículo 32ad en la Ley de Datos* | Estados miembros | Disponible para los usuarios del punto único de información | Es necesario proporcionar la información pertinente | Ad hoc |
| Reclamación presentada por personas físicas o jurídicas si se han infringido sus derechos en virtud de la Ley de datos o en relación con otros asuntos pertinentes | Artículo 1<br>*Modificación del artículo 38, apartados 1 y 2, de la Ley de Datos* | Personas físicas o jurídicas | Autoridad competente pertinente del Estado miembro correspondiente | Reclamación que debe presentarse | Ad hoc |
| Información sobre el estado de los procedimientos/recursos judiciales en relación con una reclamación presentada en virtud de la Ley de datos | Artículo 1<br>*Modificación del artículo 38, apartados 1 y 2, de la Ley de Datos* | Autoridad competente pertinente | Personas físicas o jurídicas que presentaron la denuncia | Denuncia presentada | Ad hoc |
| Datos sobre experiencia y buenas prácticas (EDIB) | Artículo 1<br>*Inserción del capítulo IX bis en la Ley de datos* | Comité Europeo de Innovación en materia de Datos | Comisión; autoridades competentes | Aportaciones que deben facilitarse | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| Evaluación de los capítulos II, III, IV, V, VI, VII y VIII de la Ley de Datos<br>Evaluación de los capítulos VII bis, VII ter y VII quater de la Ley de Datos | Artículo 1<br>*Modificación del artículo 49, apartado 1, de la Ley de Datos*<br>Artículo 1<br>*Modificación del artículo 49, apartado 2, de la Ley de Datos* | Comisión Europea | Parlamento Europeo; Consejo; Comité Económico y Social Europeo | Evaluación de la Ley de Datos realizada | Antes del 12 de septiembre<br>de<br>Antes de [entrada en vigor más 5 años] |
| Notificaciones de violaciones de datos personales | Artículo 3<br>*Modificación del artículo 33, apartado 1, del RGPD* | Responsable del tratamiento | Autoridad de control | Se ha producido una violación de datos | Ad hoc |
| Propuesta del CEPD para una plantilla común de notificación de violaciones de datos | Artículo 3<br>*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<br>Cada tres años |
| Propuestas del CEPD relativas a la evaluación del impacto en la protección de datos | Artículo 3<br>*Modificación del artículo 70, apartado 1, del RGPD* | Comité Europeo de Protección de Datos | Comisión | Propuesta que se presentará | Informes ad hoc |
| Informes sobre incidentes significativos de conformidad con la Directiva NIS2 | Artículo 6<br>*Inserción de los artículos 23 bis y 23 ter, modificación de los artículos 23 y 30, apartado 1, de la Directiva NIS2* | Entidades esenciales e importantes | CSIRT/autoridades competentes (según proceda) | Circunstancias descritas en el artículo 23, apartado 3, de la Directiva NIS2 | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| Notificaciones de violaciones de datos personales | Artículo 3<br>*Modificación del artículo 33 del RGPD* | Responsables del tratamiento | Autoridad de control | Violación de datos personales | Ad hoc |
| Notificaciones de incidentes graves relacionados con las TIC de conformidad con la DORA; notificaciones voluntarias de amenazas cibernéticas significativas de conformidad con la DORA | Artículo 8<br>*Modificación del artículo 19 de la DORA* | Entidades financieras | Autoridad competente pertinente | Incidentes importantes relacionados con las TIC; amenazas cibernéticas significativas. | Ad hoc |
| Notificaciones de incidentes que perturben significativamente o puedan perturbar significativamente la prestación de servicios esenciales de conformidad con la Directiva CER | Artículo 9<br>*Modificación del artículo 15 de la Directiva CER* | Entidades críticas | Autoridad competente | Incidentes que perturban significativamente o pueden perturbar significativamente la prestación de servicios esenciales | Ad hoc |

### 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. Concretamente, las disposiciones de la Ley de gobernanza de datos se transfieren a la Ley de datos.*

| Solución digital | Referencias a los requisitos | Principales funcionalidades obligatorias | Organismo responsable | ¿Cómo se garantiza la accesibilidad? | ¿Cómo se tiene en cuenta la reutilización? | Uso de tecnologías de IA (si procede) |
|---|---|---|---|---|---|---|
| Registro público de la Unión de servicios de intermediación de datos y organizaciones de altruismo de datos | *Inserción del artículo 32 bis en la Ley de Datos* | Almacenamiento y publicación de información obligatoria | Comisión Europea | // | // | N/A |
| Punto único de información (en virtud de la Ley de datos) | Artículo 1<br>*Inserción del artículo 32 bis en la Ley de datos* | Información que debe ponerse a disposición y ser accesible<br>Competente para recibir consultas o solicitudes de reutilización de las categorías de datos protegidos<br>Transmitir las solicitudes, cuando sea posible y apropiado por medios automatizados, al público competente | Comisión Europea | Punto de acceso único que ofrezca un registro electrónico consultable de los datos disponibles en los puntos únicos de información nacionales y más información sobre cómo solicitar datos a través de dichos puntos puntos únicos nacionales | 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 reutilización. | N/A |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | organismos sectoriales<br>Poner a disposición por medios electrónicos una lista de activos consultable que contenga una visión general de todos los recursos documentales disponibles. | | puntos de información | | |
| Punto único de entrada para la notificación de incidentes. | Artículo 6<br>*Inserción del artículo 23 bis en la NIS2* | Permitir la notificación de incidentes de conformidad con los actos pertinentes a nivel de la Unión.<br>Garantizar la interoperabilidad y la compatibilidad con las carteras electrónicas europeas | Comisión Europea; ENISA | Interoperabilidad y compatibilidad con las carteras empresariales europeas y sus propios medios de accesibilidad | Posibilidad de atender la notificación de incidentes en virtud de diferentes actos jurídicos; posibilidad de incorporar en el futuro nuevas bases jurídicas a la solución de punto de entrada único | N/A |

*Para cada solución digital, explicación de cómo la solución digital cumple con las políticas digitales y las disposiciones legislativas aplicables*

**Registro público de la Unión de servicios de intermediación de datos y organizaciones de altruismo de datos**

| **Política digital y/o sectorial (cuando sea aplicable)** | **Explicación de cómo se alinea.** |
|---|---|

| | |
|---|---|
| ***Ley de IA*** | N/A |
| ***Marco de ciberseguridad de la UE*** | N/A |
| ***eIDAS*** | N/A |
| ***Portal digital único e IMI*** | Modificación del Reglamento (UE) 2018/1724 para añadir «Registro como proveedor de servicios de intermediación de datos» y «Registro como organización de altruismo de datos reconocida en la Unión» en el anexo II. |
| ***Otros*** | N/A |

**Punto único de información (en virtud de la Ley de datos)**

| **Política digital y/o sectorial (cuando sea aplicable)** | **Explicación sobre cómo se alinea** |
|---|---|
| ***Ley de IA*** | N/A |
| ***Marco de ciberseguridad de la UE*** | Los organismos del sector público pueden establecer el requisito de acceder y reutilizar los datos o documentos de forma remota dentro de un entorno de procesamiento seguro proporcionado o controlado por el organismo del sector público. En tales casos, los organismos del sector público impondrán condiciones que preserven la integridad del funcionamiento de los sistemas técnicos del entorno de procesamiento seguro utilizado. |
| ***eIDAS*** | N/A |
| ***Portal digital único e IMI*** | N/A |
| ***Otros*** | El Punto Único de Información deberá cumplir con el Reglamento (UE) 2016/679 (RGPD). Los organismos del sector público podrán establecer requisitos para conceder acceso a la reutilización de datos o documentos solo cuando estos hayan sido anonimizados y/o sometidos a otra forma de preparación pertinente. Además, |

| | |
|---|---|
| | en caso de reutilización no autorizada de datos no personales, el reutilizador estará obligado a informar a las personas físicas cuyos derechos e intereses puedan verse afectados. |

**Punto único de entrada para la notificación de incidentes**

| **Política digital y/o sectorial (cuando sea aplicable)** | **Explicación de cómo se alinea** |
|---|---|
| ***Ley de IA*** | N/A |
| ***Marco de ciberseguridad de la UE*** | Como enmienda a la NIS2, existe un enfoque inherente en la ciberseguridad. En términos más generales, el punto de entrada único tiene como objetivo servir de puerta de enlace, canalizando todos los informes de incidentes relacionados con la ciberseguridad a las autoridades competentes respectivas, en virtud de varios actos jurídicos de la Unión. |
| ***eIDAS*** | El punto de entrada único también es obligatorio para la notificación de incidentes en virtud del Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).<br>La ENISA velará por que el punto de entrada único sea interoperable y compatible con las carteras empresariales europeas y por que estas últimas puedan utilizarse, como mínimo, para identificar y autenticar a las entidades que utilicen el punto de entrada único. La iniciativa política relativa a las carteras empresariales europeas se basará en el marco eIDAS. |
| ***Puerta digital única e IMI*** | N/A |
| ***Otros*** | La propuesta ha tenido en cuenta todo el acervo digital, incluidas las políticas relativas a los datos, la ciberseguridad y las telecomunicaciones. |

### 4.4. Evaluación de la interoperabilidad e

*Descripción general de los servicios públicos digitales afectados por los requisitos*

| **Servicio público digital o categoría de servicios públicos digitales** | **Descripción** | **Referencia(s) al requisito o requisitos** | **Solución(es) de Interoperable Europe**<br><br>**(NO APLICABLE)** | **Otras soluciones de interoperabilidad** |
|---|---|---|---|---|
| Infraestructura europea de gobernanza y transparencia de datos | Servicio público digital que permita la gobernanza de datos y la infraestructura de transparencia y aproveche, entre otras cosas, un registro público de la UE de servicios de intermediación de datos y organizaciones de altruismo de datos, y un punto único de información que ayude a los reutilizadores a encontrar información sobre la reutilización de determinadas categorías de datos protegidos.<br><br>Categoría de servicios públicos digitales según COFOG 04.9.0 - Asuntos económicos n.c.o.p. (CS) | Artículo 1 | // | // |
| Notificación de incidentes | Servicio público digital que permite la notificación de incidentes a través de un punto de entrada único.<br><br>Categoría de servicios públicos digitales según COFOG 03.6.0 Orden público y seguridad n.c.o.p. | Artículo 6 | // | Carteras empresariales europeas |

*Repercusión de los requisitos del servicio público digital en la interoperabilidad transfronteriza*

***Nota: En el análisis que figura a continuación, los números de artículo que aparecen en la sección «Medida(s)» hacen referencia a la(s) ley(es) que se modifica(n). La correspondencia con los requisitos de la Omnibus se realiza una sola vez, en la parte superior de cada celda.***

**Servicio público digital n.º 1: gobernanza de datos europeos e infraestructura de transparencia**

| **Evaluación** | **Medida(s)** | **Posibles obstáculos restantes (si procede)** |
|---|---|---|
| **Alineación con las políticas digitales y sectoriales existentes**<br><br>**Enumere las políticas digitales y sectoriales aplicables identificadas** | Artículo 1<br><br>La alineación con las políticas digitales y sectoriales existentes se refleja en los considerandos de la Ley de gobernanza de datos:<br><br>Puerta única digital (Reglamento (UE) 2018/1724) (Considerando 56): Los procedimientos de notificación para los servicios de intermediación de datos y los procedimientos de registro para las organizaciones de altruismo de datos deben estar disponibles a través de la puerta única digital, garantizando el acceso transfronterizo en línea.<br><br>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.<br><br>Componentes básicos de la CEF (Infraestructuras de servicios digitales del Mecanismo «Conectar Europa») (Considerando 54): Referencias «los vocabularios básicos y los componentes básicos de la CEF». El servicio digital debe aprovechar los componentes básicos de la CEF (como la entrega electrónica, la identificación electrónica y la firma electrónica) para su implementación técnica.<br><br>Requisitos de accesibilidad (Directivas (UE) 2016/2102 y (UE) 2019/882) (Considerando 62). Directiva (UE) 2016/2102 (Directiva sobre accesibilidad web): los registros públicos y los servicios digitales deben ser accesibles para las personas con discapacidad; Directiva (UE) 2019/882 (Ley Europea de Accesibilidad): los servicios digitales deben cumplir los requisitos de accesibilidad.<br><br>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.<br><br>Reglamento (UE) 2018/1725 (considerando 4): Cuando las instituciones de la UE traten datos a través de estos registros, deberán cumplir con este reglamento.<br><br>Directiva sobre datos abiertos (Directiva (UE) 2019/1024) (considerandos 6 y 10): «La Directiva (UE) 2019/1024 y la legislación sectorial de la Unión garantizan que los organismos del sector público faciliten el acceso y la reutilización de los datos que producen»: El servicio digital complementa 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 los principios de «abierto por diseño y por defecto» cuando sea aplicable.<br><br>Políticas sectoriales sobre espacios de datos europeos y datos sectoriales, incluidos el Espacio Europeo de Datos Sanitarios, el Espacio Europeo de Datos sobre Movilidad, el Pacto Verde Europeo/Datos sobre el clima y la energía, los datos sobre fabricación e industria, los datos sobre servicios financieros, los datos sobre agricultura, el Espacio de Datos de la Administración Pública y el Espacio de Datos sobre Competencias. | |

| | | |
|---|---|---|
| **Medidas organizativas para una prestación fluida de servicios públicos digitales transfronterizos**<br><br>**Enumere las medidas de gobernanza previstas** | Artículo 1<br><br>**Designación y coordinación de la autoridad competente**<br><br>- Artículo 32 ter: Cada Estado miembro designará una o varias autoridades competentes responsables del registro de los proveedores de servicios de intermediación de datos y de las organizaciones de altruismo de datos. Estas autoridades competentes mantendrán su independencia respecto a cualquier proveedor de servicios de intermediación de datos reconocido o cualquier organización de altruismo de datos reconocida.<br><br>Artículo 32 bis quater: Cada Estado miembro designará uno o varios organismos competentes para asistir a los organismos del sector público que conceden o deniegan el acceso para la reutilización de categorías de datos protegidos.<br><br>Artículo 32 octies: Las autoridades competentes controlarán y supervisarán el cumplimiento de las disposiciones de la Ley de Datos por parte de los proveedores de servicios de intermediación de datos reconocidos y las organizaciones de altruismo de datos reconocidas.<br><br>**Mecanismo de jurisdicción transfronteriza**<br><br>Artículo 32 sexies: Los servicios de intermediación de datos son competencia de la autoridad competente del Estado miembro en el que se encuentra el establecimiento principal. El mismo principio se aplica a las organizaciones de altruismo de datos.<br><br>**Reconocimiento mutuo y registro único**<br><br>Artículo 32 sexies: El registro como servicio de intermediación de datos u organización de altruismo de datos será válido en todos los Estados miembros.<br><br>Artículo 32 bis: Uso de un diseño de logotipo común<br><br>**Registros centralizados a nivel de la UE para la recopilación de datos y la transparencia**<br><br>Artículo 32 bis: Registros públicos de la Unión de todos los proveedores de servicios de intermediación de datos y organizaciones de altruismo de datos reconocidos.<br><br>Artículo 32, letra e): Las autoridades competentes notifican a la Comisión por vía electrónica y sin demora | |

| | | |
|---|---|---|
| | de los nuevos registros, cambios y eliminaciones, y la Comisión actualiza los registros de la UE en consecuencia<br><br>**Coordinación de la supervisión y la aplicación**<br><br>Autoridades nacionales competentes Comité<br><br>Europeo de Innovación en materia de Datos<br><br>**Gobernanza de la transferencia de datos a terceros países**<br><br>Artículo 32 bis bis: Requisitos para las transferencias de datos no personales a terceros países por parte de los reutilizadores.<br><br>**Acuerdos exclusivos**<br><br>Artículo 32k: Define la admisibilidad de los acuerdos exclusivos relativos a la reutilización de datos o documentos en poder de organismos del sector público. Exige transparencia en las condiciones finales. | |
| **Medidas adoptadas para garantizar una comprensión común de los datos**<br><br>**Enumere dichas medidas** | Artículo 1<br><br>**Normas comunes y marcos interoperables**<br><br>- La EDIB asesora a la Comisión Europea sobre las actividades de normalización que deben llevarse a cabo en relación con los aspectos intersectoriales del intercambio de datos, incluida la aparición de espacios de datos europeos comunes, teniendo en cuenta las actividades de normalización específicas de cada sector.<br>  ○ Artículo 42: La EDIB colabora en la adopción de «directrices que establecen marcos interoperables y prácticas comunes para el funcionamiento de los espacios comunes europeos de datos».<br>- Logotipo común para la identificación de los servicios de intermediación de datos y las organizaciones de altruismo de datos. | |

| | | |
|---|---|---|
| | - Artículo 32q: Los organismos del sector público y las empresas públicas pondrán a disposición sus datos o documentos, cuando sea posible y apropiado, por medios electrónicos, en formatos abiertos, legibles por máquina, accesibles, localizables y reutilizables, junto con sus metadatos. Tanto el formato como los metadatos cumplirán, en la medida de lo posible, las normas abiertas formales.<br><br>**Otras medidas pertinentes:**<br><br>- Artículo 32t: Los Estados miembros, en cooperación con la Comisión, proseguirán sus esfuerzos para simplificar el acceso a los conjuntos de datos, poniendo a disposición conjuntos de datos adecuados en formatos accesibles, fácilmente localizables y reutilizables por medios electrónicos.<br>- Artículo 32u: Los Estados miembros apoyarán la disponibilidad de datos de investigación de manera compatible con los principios FAIR. | |
| **Uso de especificaciones y normas técnicas abiertas acordadas conjuntamente**<br><br>**Enumere dichas medidas** | Artículo 1<br><br>**Medidas relativas a los datos legibles por máquina:**<br><br>- Artículo 32 bis: Registro de la Unión Europea legible por máquina de proveedores de servicios de intermediación de datos.<br>- Artículo 32 bis: Registro de la Unión Europea legible por máquina de organizaciones altruistas de datos.<br>- Artículo 32q: Los organismos del sector público pondrán a disposición sus datos y documentos, siempre que sea posible, en formatos abiertos, legibles por máquina, accesibles, localizables y reutilizables, junto con sus metadatos. Tanto el formato como los metadatos deberán, en la medida de lo posible, cumplir con las normas abiertas formales.<br>- Artículo 32 quater: Los conjuntos de datos de alto valor se pondrán a disposición para su reutilización en formato legible por máquina, a través de API adecuadas y, cuando proceda, como descarga masiva.<br>- Artículo 32 terdecies: Los Estados miembros adoptarán medidas prácticas que faciliten la búsqueda de datos o documentos disponibles para su reutilización, tales como listas de activos de datos o documentos principales con metadatos pertinentes, accesibles, cuando sea posible y apropiado | |

| | | |
|---|---|---|
| | en línea y en formato legible por máquina, y sitios web que estén vinculados a las listas de activos. Siempre que sea posible, los Estados miembros facilitarán la búsqueda multilingüe de datos o documentos.<br>- Artículo 32w: Los conjuntos de datos específicos de alto valor serán legibles por máquina. Los actos de ejecución podrán especificar las disposiciones relativas a los formatos de datos y metadatos y las disposiciones técnicas para su difusión.<br><br>**Medidas de interacción entre máquinas:**<br><br>- Artículo 32 bis quinquies: Obligatoriedad del uso del punto único de información. El punto único de información será competente para recibir consultas o solicitudes y las transmitirá, cuando sea posible y apropiado por medios automatizados, a los organismos públicos competentes o a los organismos competentes.<br><br>**Otras medidas pertinentes:**<br><br>- Artículo 48 bis: Modificación del anexo II del Reglamento (UE) 2018/1724 (Portal Digital Único). Se han estudiado las sinergias.<br>- Considerando 52 del Omnibus: En la medida de lo posible, la ENISA deberá tener en cuenta las soluciones técnicas nacionales existentes que facilitan la notificación de incidentes, como las plataformas nacionales, al elaborar las especificaciones sobre las medidas técnicas, operativas y organizativas relativas al establecimiento, mantenimiento y funcionamiento seguro del punto de entrada único. Además, la ENISA debería considerar 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 en los procesos empresariales y a las autoridades conectar el punto de entrada único con sus sistemas nacionales de notificación. | |

**Servicio público digital n.º 2: notificación de incidentes**

| Evaluación | Medidas | Posibles obstáculos restantes (si procede) |
|---|---|---|
| **Alineación con las políticas digitales y sectoriales existentes**<br><br>**Enumere las políticas digitales y sectoriales aplicables identificadas** | Artículo 6<br><br>La Directiva (UE) 2022/2555 (NIS2), que actualmente está modificando el Omnibus Digital, establece la alineación general con las políticas digitales y sectoriales existentes. Además, el Omnibus prevé sinergias con la Cartera Empresarial Europea y el Reglamento (UE) 2024/2847 (Ley de Ciberresiliencia). En particular:<br><br>• El artículo 23, apartado 4, exige el uso del punto de entrada único para la notificación de la NIS2.<br>• El artículo 23, apartado 1, establece que la notificación de un incidente grave con arreglo al artículo 14, apartado 3, del Reglamento (UE) 2024/2847 (Ley de Ciberresiliencia) constituirá también una notificación de información con arreglo a la Directiva (UE) 2022/2555 (NIS2). Esto se ajusta al principio de «una sola vez».<br>• El artículo 23 bis, apartado 3, letra d), establece el vínculo con las carteras empresariales europeas. | |
| **Medidas organizativas para una prestación fluida de servicios públicos digitales transfronterizos**<br><br>**Enumere las medidas de gobernanza previstas** | Artículo 6<br><br>El artículo 23 bis define las funciones y responsabilidades. En concreto, la ENISA deberá:<br><br>• Desarrollar y mantener un punto de entrada único para apoyar la obligación de notificar incidentes y sucesos relacionados en virtud de los actos jurídicos de la Unión.<br>• Adoptar medidas técnicas, operativas y organizativas para gestionar los riesgos que se plantean para la seguridad del punto de entrada único y la información presentada o difundida. Para ello, consultará a la Comisión, a la red CSIRT y a las autoridades competentes pertinentes. | |
| **Medidas adoptadas para garantizar un** | comprensión común | |

| | | |
|---|---|---|
| **comprensión de los datos**<br><br>**Enumere dichas medidas.** | El artículo 23 bis encarga a la ENISA la elaboración de especificaciones que garanticen la capacidad necesaria para la interoperabilidad con respecto a otras obligaciones de notificación pertinentes.<br><br>*Nota: 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 (NIS2). El artículo 23 bis, apartado 3, letra c), de la Directiva Ómnibus aclara que la ENISA velará por que se tengan debidamente en cuenta.* | |
| **Uso de especificaciones y normas técnicas abiertas acordadas conjuntamente**<br><br>**Enumere dichas medidas** | Artículo 6<br><br>El artículo 23 bis exige que se elaboren especificaciones:<br>• La ENISA proporcionará y aplicará las especificaciones sobre las medidas técnicas relativas al establecimiento, mantenimiento y funcionamiento seguro del punto de entrada único. Dichas especificaciones incluirán, entre otras cosas:<br>○ la capacidad necesaria para la interoperabilidad con respecto a otras obligaciones de notificación pertinentes.<br>○ disposiciones técnicas para que las entidades y autoridades pertinentes puedan acceder, presentar, recuperar, transmitir o tratar de otro modo la información del punto de entrada único, así como protocolos y herramientas técnicos que permitan a las entidades y autoridades seguir tratando la información recibida en sus sistemas.<br>• Cuando sea posible, el punto de entrada único será interoperable y compatible con las carteras empresariales europeas. | |

### 4.5. Medidas de apoyo a la implementación de la información digital sobre la propiedad ( )

*Descripción general de las medidas de apoyo a la implementación digital*

| Descripción de la medida | Referencia(s) a la | Función de la Comisión | Actores que deben | Requisitos |
|---|---|---|---|---|

| | **requisitos** | (si procede) | **implicados**<br>(si procede) | **Calendario**<br>(si procede) |
|---|---|---|---|---|
| Acto de ejecución: Diseño de un logotipo común para los proveedores de servicios de intermediación de datos | Artículo 1 | Establecer las características del logotipo común, incluido su diseño y modalidades de uso. | Comité de procedimiento de examen | // |
| Acto de ejecución: Diseño del logotipo común para el altruismo reconocido en materia de datos | Artículo 1 | Establecer las características del logotipo común, incluyendo su diseño y modalidades de uso. | Comité del procedimiento de examen | // |
| Seguimiento 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 altruismo de datos. | // |
| Acto de ejecución: Conjuntos de datos específicos de alto valor | Artículo 1 | Establecimiento de una lista de conjuntos de datos específicos de alto valor. Puede especificar las modalidades de publicación y reutilización de los conjuntos de datos de alto valor. | Comité del procedimiento de examen | // |

| | | | | |
|---|---|---|---|---|
| Directrices:<br>• La EDIB asesorará sobre las directrices para los espacios comunes europeos de datos<br>• EDIB adoptará directrices sobre marcos interoperables | Artículo 1 | Apoyo del EDIB | EDIB | // |
| Acto de ejecución: Plantilla común para notificar una violación de datos personales | Artículo 3 | Adoptar una plantilla común basada en la propuesta del CEPD. | Comité del procedimiento de examen | // |
| Acto delegado: Indicaciones automatizadas y legibles por máquina de las elecciones 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 la CER | Artículo 9 | Especificar con más detalle el tipo y el formato de la información notificada de conformidad con el artículo 15, apartado 1, de la Directiva (UE) 2022/2557 (CER). | // | // |