EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INGENIERÍA DE PROTECCIÓN DE DATOS PERSONALES EN LOS ESPACIOS DE DATOS DE LA UE

ENERO 2024

SOBRE ENISA

La Agencia de la Unión Europea para la Ciberseguridad, ENISA, es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por la Ley de Ciberseguridad, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la ciberpolítica de la UE, mejora la fiabilidad de los productos, servicios y procesos de las TIC con sistemas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Mediante el intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia colabora con sus principales interesados para reforzar la confianza en la economía conectada, impulsar la resistencia de las infraestructuras de la Unión y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Puede encontrar más información acerca de ENISA y su trabajo aquí: www.enisa.europa.eu.

CONTACTO

Para contactar con los autores diríjase a isdp@enisa.europa.eu
Para consultas de los medios de comunicación sobre este documento, diríjase a press@enisa.europa.eu

COLABORADORES

Isabel Barbera, Claude Castelluccia, Giuseppe D'acquisto, Marta Fydrych Gasowska, Marit Hansen, Jaap-Henk Hoepman, Meiko Jensen, Konstantinos Limniotis, Maria Raphael, Marie-Charlotte Roques Bonnet, Fernando Silva, Fatbardh Veseli, Barbara Vieira, Kim Wuyts, Christian Zimmermann, Luis de Salvador Carrasco, Peter Kraus, Teresa Martínez Sánchez y Prokopios Drogkaris.

EDITORES

Prokopios Drogkaris (ENISA), Javier Gómez Prieto (ENISA)

AGRADECIMIENTOS

Agradecemos a los colegas de la CE su revisión y sus valiosos comentarios.

AVISO LEGAL

AVISO SOBRE DERECHOS DE AUTOR

ISBN 978-92-9204-650-7, DOI 10.2824/210862

ÍNDICE

RESUMEN EJECUTIVO

Las recientes iniciativas legislativas de la UE que promueven la compartición de datos son instrumentos sectoriales e intersectoriales cuyo objetivo es facilitar el acceso a los datos regulando la reutilización de los datos de titularidad pública y privada, incluidos los datos personales. También facilitan la compartición de datos mediante la creación de nuevos intermediarios y entornos de compartición en los que las partes implicadas pueden poner en común datos e infraestructuras de forma fiable y segura.

Los espacios comunes europeos de datos (espacios de datos de la UE) son un concepto novedoso introducido en la estrategia europea de datos y desarrollado en el Reglamento de Gobernanza de Datos (DGA, por sus siglas en inglés). Se prevé que faciliten la innovación, el crecimiento económico y la transformación digital y que giren en torno a la creación de un marco para la compartición de datos que respete la privacidad, la seguridad y otras consideraciones normativas aplicables al tiempo que promuevan la colaboración intersectorial y la interoperabilidad.

Este informe intenta contextualizar los principios de diseño relativos a la protección de datos personales más relevantes y demonstrar cómo diseñar la protección de datos personales a través de dos casos de uso de un espacio de datos de la UE previsto en el ámbito farmacéutico.

A pesar del potencial de los espacios de datos de la UE, sigue habiendo consideraciones relativas a las medidas técnicas y organizativas adecuadas y a la forma de llevarlas a la práctica, tanto desde el punto de vista de la protección de datos como de la ciberseguridad Aunque ya existe un buen número de tecnologías de mejora de la privacidad que pueden ayudarnos a alcanzar objetivos específicos de protección de datos, no debemos descuidar el hecho de que estamos llamados a abordar nuevas operaciones de tratamiento, en las que las funciones y responsabilidades no siempre están claramente definidas.

1. INTRODUCCIÓN

1.1 INNOVACIÓN IMPULSADA POR DATOS

La Innovación Impulsada por Datos (DDI, por sus siglas en inglés) no es un concepto completamente nuevo; evoluciona en torno al tratamiento de grandes volúmenes de datos para extraer ideas significativas y crear innovaciones valiosas [1]. A lo largo de la última década hemos debatido tanto sobre las oportunidades como sobre los retos que plantean los macrodatos [2] [3] y [4]. Sin embargo, para aprovechar todo el potencial analítico de los datos e impulsar avances significativos, debemos ir más allá de los múltiples puntos de recopilación y análisis y adoptar un enfoque más colaborativo, sin dejar de respetar la protección de los datos personales y los datos sensibles/críticos empresariales.

La estrategia europea de datos [5] se anunció en 2020 y consiste en un plan quinquenal que presenta la visión de un 'espacio único europeo de datos', que se describe como "un auténtico mercado único de datos – abierto a datos de todo el mundo – en el que los datos personales y no-personales, incluidos los datos empresariales sensibles, estén seguros y las empresas tengan fácil acceso a datos industriales de alta calidad, impulsando el crecimiento y creando valor". En este contexto, la estrategia europea de datos reconoce la importancia estratégica de invertir en espacios comunes de datos de la UE como mecanismo para impulsar el crecimiento y la innovación en sectores económicos clave y ámbitos de interés público.

La estrategia europea de datos reconoce la importancia estratégica de invertir en los espacios de datos de la UE como mecanismo para impulsar el crecimiento y la innovación.

1.2 ESPACIOS COMUNES EUROPEOS DE DATOS

Los espacios comunes europeos de datos (en adelante, "espacios de datos de la UE") son un concepto novedoso introducido en la estrategia europea de datos y desarrollado en el Reglamento de Gobernanza de Datos (DGA) [6]. Se prevé que faciliten la innovación, el crecimiento económico y la transformación digital y que giren en torno a la creación de un marco para la compartición de datos que respete la privacidad, la seguridad y otras consideraciones reglamentarias aplicables, al tiempo que promueva la colaboración intersectorial mediante la aplicación del siguiente conjunto de medidas:

- fomentar el acceso y la reutilización de determinadas categorías de datos en poder de organismos del sector público que no pueden ponerse a disposición como datos abiertos debido a la protección que se aplica a los datos.
- garantizar que los intermediarios de datos actúen como facilitadores fiables de la puesta en común de datos en los espacios de datos de la UE.
- facilitar la puesta en común de datos, en concreto para permitir el uso de datos entre sectores y para determinados fines.

A pesar de las ventajas de los espacios de datos, el número de partes interesadas con objetivos estratégicos divergentes y necesidades de datos específicas que pueden resultar difíciles de conciliar constituye todo un reto. Además, dado que los espacios de datos de la UE operarán en el marco de la política y la legislación de la Unión, es crucial identificar los puntos comunes intersectoriales, la terminología común, los marcos de diseño y cumplimiento y articular herramientas adecuadas de ingeniería de datos [7].

1.3 PRINCIPIOS DE DISEÑO DE LOS ESPACIOS DE DATOS DE LA UE

Aunque la DGA proporciona un marco de gobernanza horizontal general para los espacios de datos de la UE, también destaca la necesidad de que funcionen de acuerdo con otras políticas y leyes de la Unión aplicables, como las relativas a la protección de datos, la ciberseguridad, la

propiedad intelectual, etc., y cumpliendo con la legislación sectorial pertinente. Un elemento esencial será la puesta en marcha de herramientas para poner en común, acceder, utilizar y compartir datos respetando la legislación aplicable, permitiendo a los titulares de los datos gestionar los derechos y condiciones de acceso a lo largo del tiempo. Estas consideraciones también se destacan en el reciente informe sobre finanzas abiertas [8] del Grupo de Expertos sobre el Espacio Europeo de Datos Financieros.

En segundo lugar, para que se pueda "acceder a ellos y utilizarlos de la manera más eficaz y responsable posible", los espacios de datos de la UE deben diseñarse, configurarse y mantenerse de modo que ofrezcan un entorno de tratamiento seguro y supervisado. También deben seguir siendo técnicamente interoperables con otros, garantizando al mismo tiempo, según sea necesario, la confidencialidad comercial o estadística, la protección de los derechos de propiedad intelectual de terceros y la protección de los datos personales. Por lo tanto, unas normas coherentes y predecibles sobre el acceso y la reutilización de los datos son fundamentales para que los titulares y los usuarios de los datos cumplan la política y la legislación de la Unión.

Por último, se adoptarán recomendaciones básicas y uniformes sobre las condiciones de reutilización y las medidas técnicas y organizativas conexas (TOMs, por sus siglas en inglés), en particular para ayudar a los titulares de los datos a comprender mejor cómo deben adaptar las normas de seguridad y confidencialidad y ajustar sus políticas corporativas para seguir cumpliendo los requisitos de protección de datos de la UE (RGPD).

1.4 LA INTEROPERABILIDAD EN EL CENTRO DE LOS ESPACIOS DE DATOS DE LA UE

Los titulares de los datos están sujetos a la obligación de fomentar la interoperabilidad. De hecho, los proveedores de servicios de compartición de datos "facilitarán la compartición de datos en el formato en que los reciban del titular de datos y convertirán los datos a formatos específicos únicamente para mejorar la interoperabilidad dentro de los sectores y entre ellos, o si así los solicita el usuario de los datos o lo exige la legislación de la Unión, o para garantizar la armonización con las normas internacionales o europeas en materia de datos". Esta interoperabilidad debe definirse ante todo a nivel de la UE, pero también teniendo en cuenta normas técnicas o especificaciones bien reconocidas.

Los intermediarios pueden facilitar la interoperabilidad y la puesta en común de datos personales, ayudando a los titulares de los datos a anonimizar o seudonimizar los datos personales, redactando y ejecutando acuerdos de compartición de datos personales o facilitando el ejercicio de los derechos de las personas.

1.5 ENFOQUE Y OBJETIVOS

Este informe aborda el diseño y despliegue de los espacios de datos de la UE desde una perspectiva de ingeniería, haciendo hincapié en la ingeniería de la protección de datos personales. Los principales objetivos de este informe son contextualizar los principales principios de diseño relativos a la protección de datos personales y demostrar cómo diseñar la protección de datos personales a través de dos casos de uso de un espacio de datos de la UE previsto en el ámbito farmacéutico.

Este trabajo está destinado a apoyar a los responsables políticos, los reguladores y los profesionales de la protección de datos y se realiza en el contexto de las tareas de ENISA en virtud del Reglamento de Ciberseguridad (CSA) [9] para apoyar a los Estados miembros en aspectos específicos de ciberseguridad de la política y la legislación de la Unión en relación con la protección de datos y la privacidad. Este trabajo se basa en las actividades de la

Agencia en el ámbito de la Ingeniería de Protección de datos y se realiza en colaboración con el Grupo de Trabajo Ad Hoc de ENISA sobre Ingeniería de Protección de datos[1].

1.6 ESTRUCTURA DEL DOCUMENTO

Este informe está estructurado en las cuatro secciones principales siguientes:

La Sección 1 proporciona el contexto de los espacios de datos de la UE y destaca las consideraciones clave relativas a la innovación impulsada por los datos, los principios de diseño de los espacios de datos y la interoperabilidad.

La Sección 2 profundiza en las consideraciones específicas de la protección de datos en los espacios de datos de la UE. Más concretamente, aborda la terminología y las funciones; los problemas de entrada y salida en términos de privacidad, así como el papel de la ingeniería de protección de datos en la aplicación de los espacios de datos. La sección también se centra en otras consideraciones clave como la interoperabilidad, la responsabilidad, la eficiencia, las evaluaciones de impacto, la selección de tecnologías de mejora de la privacidad (PETs, por sus siglas en inglés) y los derechos de los interesados.

La Sección 3 ofrece perspectivas de ingeniería de protección de datos sobre un espacio de datos farmacéuticos previsto, ilustrando dos casos concretos de aplicación. Cada caso de uso trata de poner de relieve el modo en que diferentes actores pueden desplegar técnicas específicas de seudonimización para proporcionar a los usuarios de datos conjuntos de datos útiles, pero adecuadamente protegidos.

La Sección 4 concluye el informe y resume las principales conclusiones y consideraciones relativas a la ingeniería protección de datos personales en los espacios de datos de la UE.

1 Agencia de Ciberseguridad de la Unión Europea, 'Ad-Hoc Working Group on Data Protection Engineering', sitio web de ENISA, https://www.enisa.europa.eu/topics/data-protection/ad-hoc-working-group-on-data-protection-engineering

2. CONSIDERACIONES SOBRE LA PROTECCIÓN DE DATOS EN LOS ESPACIOS DE DATOS DE LA UE

2.1 TERMINOLOGÍA Y ANÁLISIS DE FUNCIONES

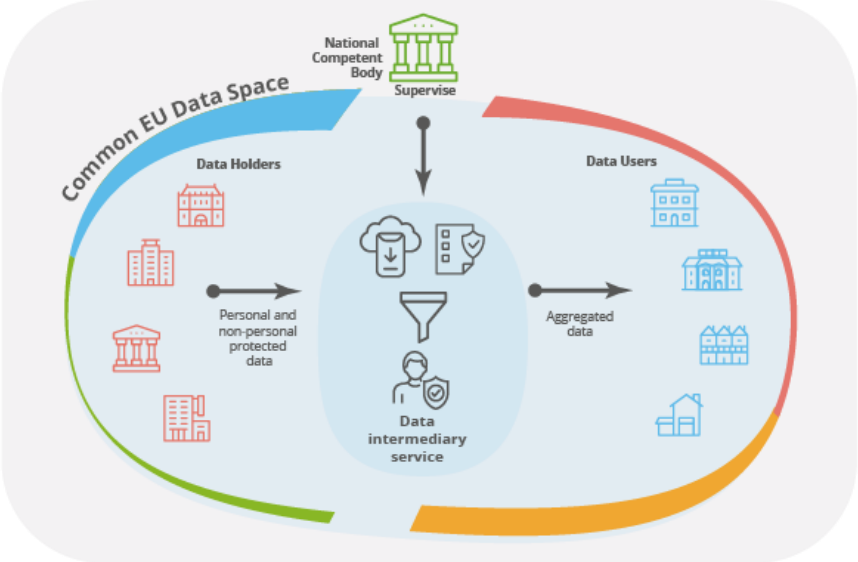
Un espacio de datos de la UE, tal como se define en la DGA, consta de tres actores principales; el titular o titulares de los datos, el intermediario de datos y el usuario o usuarios de datos. La DGA ofrece una definición para cada uno de ellos, que se presentan brevemente a continuación:

- **El titular de los datos** es una persona jurídica que no es un interesado con respecto a los datos específicos en cuestión, pero que tiene derecho a conceder acceso a determinados datos personales o no personales o a compartirlos.
- **El intermediario de datos** es una entidad que actúa como intermediario entre los titulares y los usuarios de datos. El intermediario de datos desempeña un papel a la hora de facilitar la compartición segura y controlado de datos mediante la prestación de servicios tales como el acceso a los datos.
- **El usuario de datos** es una persona física o jurídica que tiene acceso legal a determinados datos personales o no personales y tiene derecho a utilizar esos datos obtenidos del intermediario con fines comerciales o no comerciales.

La operación de tratamiento depende de cómo se realice la compartición de datos y de cuál sea la función real del intermediario de datos.

En la Figura 1 se ofrece una representación ilustrativa de las interacciones entre estos tres actores.

Figura 1: Principales actores del espacio de datos de la UE



La DGA se aplica a "cualquier representación digital de actos, hechos o información", incluidos los datos personales. Cuando los datos compartidos incluyen datos personales, es necesario establecer una correspondencia entre las funciones (y las responsabilidades pertinentes) entre la DGA y el RGPD. Sin embargo, esto puede no ser sencillo, ya que el tratamiento depende de cómo se realice la compartición de los datos y de cuál sea la función real del intermediario de datos.

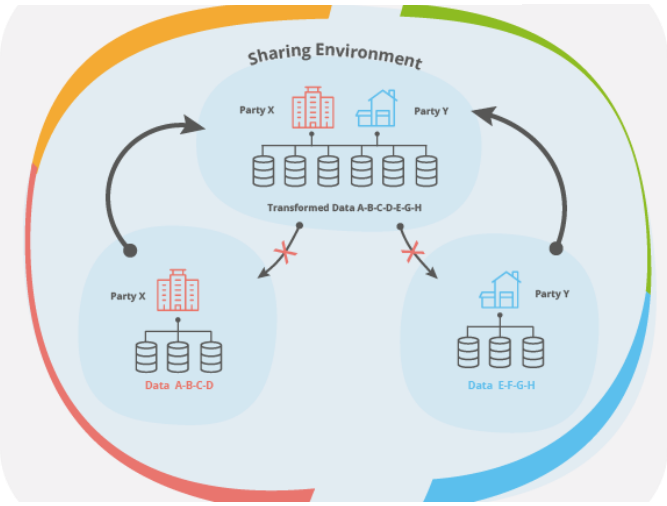
En el contexto de la DGA y del RGPD, el titular de los datos es responsable de garantizar la recogida, el tratamiento y el almacenamiento lícitos y adecuados de los datos, el intermediario de datos presta servicios para facilitar la compartición, el tratamiento y el almacenamiento controlados de los datos y el usuario de datos recibe y utiliza los datos para diversos fines, como el análisis, la investigación u otros intereses legítimos. Incluso basándose en estas descripciones más bien genéricas, no puede establecerse con seguridad quién actúa como responsable del tratamiento, si hay más de un responsable del tratamiento, si actúan como corresponsables, si hay un encargado del tratamiento y si los usuarios de datos son destinatarios de los datos. Aunque el RGPD establece requisitos específicos que debe cumplir cada función, no queda claro en el modelo genérico qué entidad sola o qué entidades colectivamente “determinan los fines y medios del tratamiento de datos personales”, qué entidad actúa “en nombre del responsable del tratamiento” y si es una entidad “a la que se comunican los datos personales”. Como se señala en la reciente publicación [10] de la Agencia Española de Protección de Datos (AEPD) “El aspecto más importante que define una operación de tratamiento es su finalidad”.

En esencia, la DGA y el RGPD crean un marco en el que los titulares de datos, los intermediarios de datos y los usuarios de datos trabajan juntos para garantizar la compartición, el tratamiento y el uso responsables y conformes de los datos. Deben alinear sus prácticas con los principios y obligaciones descritos en ambos actos legislativos para proteger los derechos y la privacidad de las personas, fomentando al mismo tiempo la innovación y las iniciativas impulsadas por los datos.

2.2 PROBLEMAS DE PRIVACIDAD DE ENTRADA Y PRIVACIDAD DE SALIDA

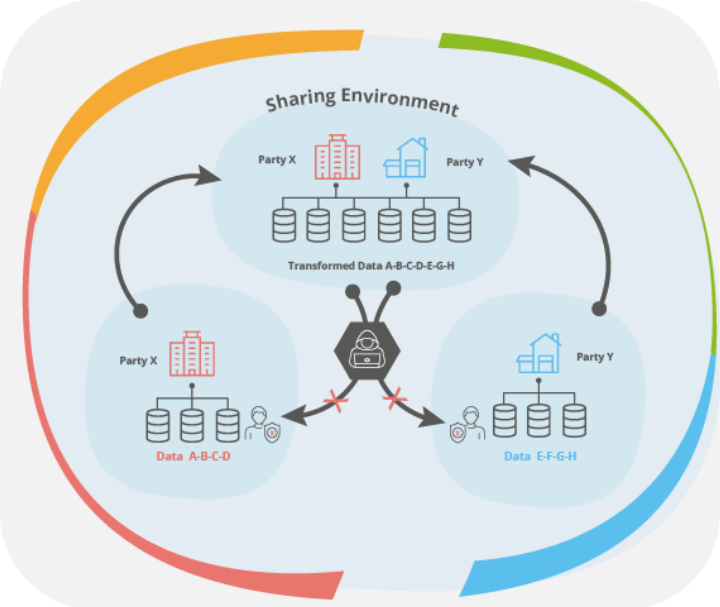
Antes de iniciar un proceso de compartición de datos, hay que considerar los posibles riesgos para los interesados que puedan surgir durante el tratamiento que realizará el entorno de puesta en común. Se pueden identificar dos retos principales, que se presentan a continuación:

Figura 2: Problema de la privacidad de entrada



- **El problema de la privacidad de entrada**: El objetivo es permitir el tratamiento de los datos compartidos, pero garantizando al mismo tiempo que el entorno de intercambio no pueda volver a los datos iniciales, lo que podría dar lugar a la individualización o identificación de personas.
- **El problema de la privacidad de salida:** El objetivo es evitar que se señale o identifique a una persona después de que se hayan hecho los cálculos en el entorno compartido.

Figura 3: Problema de la privacidad de salida



La ingeniería de protección de datos ofrece a los responsables del tratamiento una opción factual para compartir datos minimizando el riesgo de uso indebido de la información, violación de datos, etc.

Tanto la privacidad de entrada como la de salida son aspectos cruciales de la privacidad y la seguridad de los datos en entornos de intercambio como los espacios de datos de la UE. Garantizar la protección de los datos personales desde el momento en que se recogen hasta el momento en que se comparten los resultados es un elemento integral para la confianza en estos marcos de intercambio [11]. La forma de hacer frente a estos dos riesgos consiste en desplegar los elementos básicos de la ingeniería de protección de datos [12] respetando al mismo tiempo los principios del RGPD.

2.3 LA FUNCIÓN DE LA INGENIERÍA DE PROTECCIÓN DE DATOS

La ingeniería de protección de datos puede ser un facilitador muy importante para el despliegue de espacios de datos de la UE en los que las oportunidades de compartir datos y la protección de datos personales puedan coexistir fructíferamente y no obstaculizarse mutuamente. No abordar las limitaciones jurídicas y técnicas de los requisitos de protección de datos inherentes a la implantación de espacios de datos de la UE puede ser un factor de bloqueo contra la adopción del paradigma de compartición de datos y puede limitar el alcance de la estrategia de datos de la UE. Este requisito previo se destaca no solo en la DGA, sino también en un informe reciente publicado por la AEPD [13].

La ingeniería de protección de datos no es una mera “herramienta de cumplimiento” del RGPD. Al aplicar las medidas adecuadas y las salvaguardias necesarias para reforzar los principios de protección de datos y permitir el ejercicio de los derechos de las personas, la ingeniería de protección de datos ofrece a los responsables del tratamiento una opción factual para compartir datos, minimizando al mismo tiempo el riesgo de uso indebido de la información, violación de

datos u otras amenazas a la seguridad. El desarrollo de casos de uso persuasivos y convincentes para una compartición segura y legal de datos es uno de los retos más cruciales para el éxito de la aplicación de los espacios de datos de la UE. La ingeniería de protección de datos tiene el potencial de lograr un equilibrio entre la compartición de datos y su protección. El riesgo de utilizar medidas nuevas y poco conocidas puede desincentivar su adopción. Esto puede ser especialmente cierto en el caso de las tecnologías emergentes, que pueden no contar aún con mejores prácticas establecidas. El desarrollo de normas y el aprovechamiento de las buenas prácticas existentes pueden reducir la complejidad y la incertidumbre asociadas a la adopción de estas técnicas. Esto puede ayudar a aumentar la confianza en las herramientas e ingeniería de protección de datos y promover su adopción generalizada.

Otro aspecto no trivial es el papel de un intermediario de datos en un escenario de compartición en un espacio de datos de la UE, ya que podría implicar una toma de decisiones relativa a la mitigación de riesgos. Una vez que el responsable del tratamiento de datos ha identificado los riesgos potenciales de la actividad de tratamiento de datos prevista, se plantea la cuestión de cómo mitigar los riesgos identificados. Los métodos estándar de mitigación de riesgos, documentados por ejemplo en las Estrategias de Diseño de la Privacidad [14], abarcan, p. ej., la aplicación de tecnologías de mejora de la privacidad (PETs), o la decisión de dividir las actividades de tratamiento entre múltiples actores separados. En [12], [15] y [16] se analizan enfoques avanzados a este respecto.

El intermediario de datos puede o no formar parte del grupo de responsables de la toma de decisiones (por ser un responsable o un encargado del tratamiento de datos), pero sin duda es una de las entidades que deben aplicar realmente el conjunto del PETs elegido. Si la seudonimización (avanzada) de datos (o incluso la anonimización) se identifica como el mejor medio para abordar un determinado riesgo de la evaluación de impacto (EIPD), la tarea de implementar la seudonimización en el conjunto de datos considerado debe ser realizada por alguno de los actores. Por supuesto, sería posible que el intermediario de datos entregara el conjunto de datos completo, no seudonimizado, a otro encargado, que a su vez realiza la seudonimización, pero este diseño introduciría en realidad un nuevo vector de riesgo, por lo que no mitigaría idealmente el riesgo de divulgación de datos en cuestión. En el mejor de los casos, el conjunto de datos se seudonimizaría en el propio intermediario de datos (o en los lugares de almacenamiento de datos de los que el intermediario se encargue). Sin embargo, este planteamiento exigiría que los responsables del tratamiento que consulten los conjuntos de datos al intermediario de datos le indiquen exactamente cómo llevar a cabo el sistema específico de seudonimización en cuestión. Posteriormente, el intermediario de datos tendría que instanciar y realizar la seudonimización de los datos por sí mismo, proporcionando únicamente el conjunto de datos seudonimizado al usuario de datos que realiza la consulta.

La misma necesidad de mitigación del riesgo es válida para todos los demás medios de mitigación del riesgo, como se ha expuesto anteriormente. Si se decide utilizar el aprendizaje federado como medio (de protección de la privacidad) para entrenar un modelo de aprendizaje automático, el responsable del tratamiento de los datos deberá aplicar y coordinar esta decisión, en estrecha colaboración con el intermediario de datos que proporciona acceso a las ubicaciones de almacenamiento de datos. Si se va a utilizar un esquema de k-anonimidad o de privacidad diferencial para proteger los datos de divulgación, dicha técnica deberá aplicarse en el lugar donde se almacenan los datos.

Como puede verse, para aplicar razonablemente tecnologías de mejora de la privacidad en escenarios de espacios de datos, es esencial que el intermediario de datos sea capaz de llevar a cabo dichas tareas, es decir, que disponga de implementaciones listas para desplegar estas técnicas en los conjuntos de datos en cuestión, y que sea capaz de desplegar estas implementaciones dinámicamente en cada escenario de compartición de datos en cuestión – según las instrucciones del responsable del tratamiento.

2.4 EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS EN LOS ESPACIOS DE DATOS

La ingeniería de protección de datos puede ser útil en términos de (semi)automatización de la recopilación y entrega necesaria con respecto a las EIPD realizadas por los responsables del tratamiento de datos. Dado que una actividad clave en toda EIPD es la obtención y evaluación de los riesgos para los derechos y libertades de los interesados, el intermediario de datos puede realizar una primera vez dicha actividad para sus propios sistemas y servicios y proporcionar automáticamente a los responsables del tratamiento los riesgos identificados y la información pertinente correlacionada. De este modo, los responsables del tratamiento pueden incorporar esta lista de riesgos en su EIPD.

Es esencial comprender que el proceso de una EIPD requiere algo más que la mera concatenación de las listas de riesgos obtenidos de los responsables y encargados del tratamiento. Los riesgos adicionales pueden derivarse de la constelación de entidades colaboradoras (es decir, responsables y encargados del tratamiento) y, por lo tanto, dependen de las interacciones exactas sustanciadas en el tratamiento. Estos riesgos interorganizativos solo pueden observarse cuando se analizan las colaboraciones y la operación de tratamiento en su conjunto. Por ejemplo, consideremos el caso en que los datos personales cifrados se almacenan en un encargado de la cadena del tratamiento y la clave de cifrado correspondiente se almacena en otro encargado del tratamiento. Realizar la EIPD para cada uno de ellos por separado puede dar lugar a riesgos bajos. O bien los datos están cifrados (y, por tanto, protegidos de los adversarios), o bien los datos ni siquiera se almacenan (salvo la clave de descifrado). Por separado, es probable que ninguno de los dos riesgos obtenga una puntuación muy alta en una evaluación de la EIPD.

Sin embargo, si resulta que estos dos encargados utilizan el mismo encargado para el almacenamiento real, la combinación de ambas instancias puede convertirse en un grave riesgo para el tratamiento, ya que ahora tanto la clave de descifrado como los datos cifrados están en manos de la misma organización (y de todos sus posibles piratas informáticos que tengan acceso a los datos). Como puede verse, la elección y constelación de responsables y encargados en el tratamiento es un aspecto muy relevante de toda EIPD compositiva, que no puede prepararse estáticamente antes de que se manifieste realmente un escenario de compartición. En este sentido, estos riesgos de composición son diferentes de los riesgos de una sola organización, como los cortes locales de electricidad o la evaluación del personal de seguridad. En resumen, la tarea de apoyar una EIPD holística con múltiples responsables del tratamiento e intermediarios de datos no es trivial. Requiere especial atención durante la ingeniería de todo el tratamiento y el despliegue del espacio de datos de la UE.

El apoyo a una EIPD holística con múltiples responsables e intermediarios de datos requiere un enfoque holístico.

2.5 PRINCIPALES ELEMENTOS CONSTITUTIVOS DE LA RESPONSABILIDAD PROACTIVA (ACCOUNTABILITY BUILDING BLOCKS)

Un aspecto adicional relacionado con el establecimiento de la confianza reside en la noción de responsabilidad (principio) del responsable del tratamiento. El responsable del tratamiento es responsable del cumplimiento de los principios establecidos en el artículo 5.1 del RGPD. Así pues, es obligación del responsable adoptar las medidas necesarias para cumplir los requisitos del RGPD, y poder demonstrar dicho cumplimiento en cualquier momento, sin necesidad de que la autoridad de control lleve a cabo investigaciones y solicitudes específicas para evaluar la conformidad, en el ejercicio de sus competencias.

Tanto si los responsables como los encargados del tratamiento son entidades públicas o privadas, todos los titulares de datos que deseen promover la reutilización de datos personales para el bien social y económico deben demostrar su responsabilidad proactiva, mediante, según proceda, mecanismos internos renovados (políticas, procedimientos, evaluaciones basadas en el riesgo, controles y otras medidas relacionadas con la compartición de datos),

acuerdos de compartición de datos y programas adecuados de gestión de la privacidad (PMPs).

Basándose en las disposiciones de la DGA sobre los espacios de datos de la UE, los principales elementos para lograr la responsabilidad proactiva o “accountablity building blocks” son los siguientes:

1. Identificación clara de las responsabilidades y las obligaciones de los titulares de datos y los usuarios de datos

Los titulares de los datos deben cumplir sus obligaciones legales, como las previstas en el RGPD (es decir, establecer una base jurídica antes de compartir los datos personales con cualquier otra parte), tanto como los usuarios de datos que reciben los datos personales (es decir, establecer sobre qué base jurídica pretenden llevar a cabo su tratamiento). Estas obligaciones pueden establecerse útilmente en un acuerdo (véase el principio 9).

2. Gobernanza interna eficaz de la compartición de datos personales

Se requiere una gestión eficiente de las responsabilidades y obligaciones derivadas de la compartición de datos (es decir, redacción de acuerdos de compartición de datos, medidas técnicas y organizativas adicionales que deben adoptarse y aplicarse). Este modelo de gobernanza debería enmarcar específicamente los casos en los que la compartición de datos implica la supervisión del tratamiento concertada con los encargados y subencargados del tratamiento (o también con intermediarios y terceras partes competentes).

3. Gobernanza externa cooperativa de la compartición de datos personales

Definir el modo en que los titulares de los datos cooperarán entre sí (socios específicos) dentro de los organismos sectoriales y las autoridades competentes, pero también con la Comisión Europea, el Comité Europeo de Innovación en materia de Datos (EDIB, por sus siglas en inglés) y cualquier parte interesada encargada de enmarcar mejor la reutilización de los datos (por ejemplo, en relación con la posible gestión de las brechas de datos).

4. Aplicación del programa de compartición de datos

Definir políticas, procedimientos y otras medidas que garanticen que los titulares de los datos seguirán siendo responsables cuando compartan datos personales, mitigando eficazmente los riesgos derivados de dicha compartición de datos.

5. Diseño de herramientas específicas de rendición de cuentas en materia de compartición de datos

Reducir los riesgos derivados de la compartición de datos personales, incluidos los mecanismos de seguridad centrados en el acceso ad hoc, así como cualquier diligencia debida suplementaria que deba imponerse a los titulares o usuarios de los datos.

6. Equilibrar los objetivos de seguridad y mitigación de riesgos con la necesidad de compartir datos de calidad suficiente

Los titulares y usuarios de datos deben integrar la protección de datos en el diseño de aplicaciones, dispositivos y sistemas (es decir, PETs), asegurándose al mismo tiempo de que tales medidas no privan a los usuarios de datos de utilizar datos cualitativos, pertinentes y bastante fiables. En la práctica, la eficiencia de la compartición de datos debe evaluarse en relación tanto con la seguridad de los datos, como en el frente de la calidad de los datos.

7. Evaluación ética de las prácticas previstas para compartir datos

Las evaluaciones especificas deben considerar los riesgos vinculados al tratamiento de datos compartidos (es decir, la ausencia de prácticas ilegales, desleales o engañosas, o de cualquier intención de compartir datos personales para perjudicar o poner en desventaja a una persona o a un grupo de personas) frente a los beneficios de dicho tratamiento de datos compartidos (es decir, cualquier interés público que se vería perjudicado por la ausencia de reutilización de datos para el bien público).

8. Compartición transparente de información entre el titular y el usuario de los datos

El destinatario de los datos personales debe llevar a cabo una evaluación de riesgos específica en relación con la finalidad prevista del tratamiento, dejándoselo claro al titular de los datos. El titular de los datos debe considerar cualquier salvaguardia o control adicional que desee imponer al receptor para garantizar la seguridad, imparcialidad y confidencialidad de los datos.

9. Marco contractual de las prácticas de compartición de datos dentro de los espacios de datos de la UE (acceso) y de un espacio de datos a otro (interoperabilidad) mediante acuerdos de compartición de datos sectoriales o específicos

Los titulares y usuarios de datos deben considerar sus responsabilidades y obligaciones específicas y enmarcarlas claramente, de forma adecuada y proporcional a los riesgos identificados (análisis caso por caso). Definir las responsabilidades respectivas, establecer obligaciones vinculantes y determinar el encuadramiento de la responsabilidad es esencial para generar confianza. En concreto, los acuerdos podrían detallar las cualificaciones específicas de las partes como titular de los datos, usuario de los datos, responsable del tratamiento, encargado del tratamiento, subencargado del tratamiento, intermediario o tercero en virtud del acuerdo de compartición de datos. Opcionalmente, la diligencia debida para garantizar que todos los datos personales se han recogido legalmente y que se ha facilitado información transparente también podría enmarcarse en cláusulas que hagan referencia a salvaguardias como la limitación voluntaria y transparente de los usos de los datos o salvaguardias contractuales específicas.

10. Transparencia hacia las personas

Tanto los titulares como los usuarios de los datos deben asegurarse de que las personas entienden cómo se comparten y reutilizan sus datos personales y cómo pueden ejercer sus derechos en la práctica (es decir, el derecho a optar por no compartir los datos o el derecho a suprimirlos). Estas obligaciones de “transparencia” pueden depender de si la compartición de datos es obligatoria por ley/decidido por el sector público o resulta de decisiones ad hoc o caso por caso.

Los titulares y los usuarios de datos que asumen estas funciones en virtud del Reglamento General de Protección de Datos también asumen obligaciones de responsabilidad o rendición de cuentas que pueden abordarse mediante la aplicación de los elementos básicos antes mencionados.

2.6 ESPACIOS DE DATOS EFICIENTES EN LA UE MEDIANTE SALVAGUARDAS E INTERMEDIARIOS DE CONFIANZA

Los programas de rendición de cuentas y la gestión no son la única forma de crear un eje central común, coherente y normalizado de la UE para que los espacios de datos de la UE sean eficaces e interoperables en la práctica. Sin ambigüedades, antes de poner en marcha proyectos de compartición de datos, los titulares de los mismos se beneficiarían al considerar si es necesario un acuerdo de compartición de datos con los destinatarios para cumplir sus obligaciones de rendición de cuentas o mitigar los riesgos identificados para las personas en particular, especificando la finalidad de la compartición de datos, definiendo las medidas de seguridad y garantizando que cada parte tenga claras sus funciones y responsabilidades, sus respectivas obligaciones de gobernanza y las disposiciones en materia de responsabilidad. Por otra parte, los intermediarios de datos, ya estén “concebidos para ayudar a las personas a ejercer sus derechos en virtud del Reglamento General de Protección de Datos (RGPD)” o para “facilitar la agregación y la compartición de cantidades sustanciales de datos relevantes” y reforzar la “compartición eficiente de datos, así como para facilitar el intercambio bilateral de datos”, tendrán un papel crucial que desempeñar, aunque su papel y sus obligaciones estén aún por afinar y evidenciar en la práctica. Dado que una característica esencial del intermediario es que “no utilice los datos compartidos para ningún otro fin”, habrá que acordar y especificar en la práctica medidas técnicas y organizativas.

3. SALUD – CASOS DE USO FARMACÉUTICO

3.1 CONTEXTO

La estrategia farmacéutica de la UE [17] se anunció en 2020 con el objetivo de abordar diversos retos y oportunidades dentro del sector farmacéutico para garantizar la disponibilidad, accesibilidad, asequibilidad y sostenibilidad de los medicamentos para los ciudadanos de la UE. En la actualidad, la legislación farmacéutica de la UE ha permitido la autorización de medicamentos seguros, eficaces y de alta calidad. Sin embargo, también existe un problema creciente de escasez de medicamentos para muchos países de la UE/EEE, como se manifiesta en la exposición de motivos de la reciente propuesta de directiva de la CE sobre medicamentos de uso humano [18]. Además, también existe una necesidad creciente de apoyo científico y de evaluación y autorización aceleradas de medicamentos que ofrezcan avances terapéuticos en áreas de necesidades médicas no cubiertas.

El presente caso de uso analiza un espacio de datos farmacéuticos como posible medio para abordar la disponibilidad de productos farmacéuticos en el mercado en función de las necesidades actuales, las posibles necesidades futuras y la vigilancia en relación con el uso de productos farmacéuticos. Las autoridades sanitarias nacionales tratan de garantizar la disponibilidad de productos farmacéuticos en el mercado basándose tanto en las necesidades actuales como en las posibles necesidades futuras (por ejemplo, debido al posible aumento del número de tratamientos específicos, enfermedades por región geográfica, etc.). Los datos iniciales para estos análisis pueden obtenerse de los datos de prescripción, las empresas farmacéuticas que ofrecen los productos al mercado, los proveedores de asistencia sanitaria, las instituciones de investigación y las autoridades reguladoras nacionales.

3.2 DEFINICIÓN DE LOS PROBLEMAS

El espacio de datos farmacéuticos previsto pretende apoyar los siguientes análisis para el usuario de los datos, que en este caso es la autoridad sanitaria nacional:

- Disponibilidad de productos farmacéuticos en el mercado: Este análisis se realizará a partir de los datos de prescripción de los últimos años, la disponibilidad de productos farmacéuticos por parte de las empresas farmacéuticas y los indicadores de las instituciones de investigación sobre posibles necesidades eminentes debidas a posibles aumentos de enfermedades específicas. El análisis se realizará a nivel de regiones geográficas.
- Investigación y análisis de la eficacia de los productos farmacéuticos: Este análisis se realizará a partir de los datos de prescripción y datos sobre cuál era la medicación recetada para cada diagnóstico médico.

Dado que los datos comunicados al intermediario de datos pueden muy bien incluir datos personales, los titulares de los datos y el intermediario de datos deben prestar especial atención al nivel de protección de estos datos. Además, hay un aspecto importante que debe destacarse con respecto a si el alcance del tratamiento de estos datos personales entra dentro del uso primario de la recogida inicial o entra dentro del uso secundario de los datos, y los responsables del tratamiento deben llevar a cabo una evaluación de si son compatibles con la finalidad inicial de la recogida.

3.3 CASO DE USO – DISPONIBILIDAD DE PRODUCTOS FARMACÉUTICOS EN EL MERCADO

Uno de los usos pensados del espacio de datos farmacéuticos previsto es garantizar la disponibilidad de productos farmacéuticos en el mercado. Se supone que existen tres tipos principales de titulares de datos, que se enumeran a continuación junto con la información que cada tipo de titular de datos comparte con el intermediario de datos. Cada titular de datos almacena datos adicionales a los presentados anteriormente, sin embargo, solo los datos enumerados a continuación se consideran necesarios para la prestación del servicio al usuario de datos.

- El **sistema nacional de prescripción electrónica** que comparte información relacionada con las prescripciones farmacéuticas;

Número de la Seguridad Social	Fecha de naci-miento	Género	Código postal	Medicación recetada	Dosis	Síntomas	Fecha de prescripción	Fecha de prescripción

- Las **empresas farmacéuticas** que comparten información sobre cada medicamento que ponen a disposición del mercado;

Medicación	Descripción	Cantidad disponible

- Los **profesionales sanitarios** que comparten información sobre la medicación que se utiliza para las enfermedades diagnosticadas y las posibles interacciones no deseadas entre los distintos medicamentos.

Enfermedad	Interacción no deseada de medicamentos	Indicadores de síntomas de interacción

El usuario de datos es la autoridad reguladora nacional, que pretende recopilar información sobre el estado actual de las prescripciones de medicamentos, combinado con la disponibilidad de productos de las empresas farmacéuticas y la necesidad de productos farmacéuticos alternativos en los casos en que no se recomiendan combinaciones específicas.

3.3.1 Tecnologías a utilizar

Uno de los objetivos de diseño, en lo que se refiere a la aplicación de la ingeniería de protección de datos, es que el intermediario pueda responder a las solicitudes del usuario de los datos (autoridad nacional de reglamentación), sin poder identificar o individualizar a las personas. Para alcanzar este objetivo, los titulares de los datos deberán aplicar técnicas específicas para enmascarar de la ingeniería de protección de datos al compartir los datos, como se muestra a continuación.

1. El **proveedor nacional de rectas electrónicas** crea un identificador para cada registro que se va a compartir sustituyendo campos específicos por un seudónimo generado de forma determinista, basado en una clave *k* que solo conoce el titular de los datos. La misma *k* se aplica a todos los registros. Podría ser, por ejemplo, una función hash con clave (p. ej. un código de autenticación de mensaje – MAC, por sus siglas en inglés) como se describe en [19]. En el escenario actual, el Número de la Seguridad Social (NUSS) puede utilizarse como identificador.

2. El conjunto de datos compartidos por el proveedor de recetas no puede considerarse totalmente seudonimizado, ya que no se han abordado todos los riesgos para la protección de datos. Siguen existiendo riesgos de reidentificación debido a los denominados cuasi-identificadores [20], por lo que deben ser enmascarados adecuadamente por el titular de datos. A este respecto, existen técnicas como la generalización de atributos. En nuestro caso de uso, tales cuasi-identificadores (y sus posibles generalizaciones) son los siguientes:
    i) Fecha de nacimiento: se sustituye por un intervalo de edades (p.ej. 50-55)
    ii) Código postal: se sustituye por los tres primeros caracteres del código postal; estos tres números deberían bastar para proporcionar información sobre la zona de residencia más amplia.
    iii) Fecha de prescripción: se sustituye solo por el mes y el año en lugar de la fecha completa.

El grado de cada una de las generalizaciones anteriores depende del nivel de riesgo de la salida resultante, que no permitirá la reidentificación o singularización con respecto a un individuo [21].

Las decisiones sobre cómo se generalizará cada atributo están estrechamente relacionadas con el nivel de riesgo de reidentificación o singularización de un individuo.

Las **empresas farmacéuticas** y **los proveedores de asistencia sanitaria** no comparten datos personales, por lo que, desde el punto de vista de la ingeniería de protección de datos, no es necesario el enmascaramiento.

3.3.2 Consideraciones

El caso de uso descrito anteriormente contempla un escenario de compartición de datos en el que el enmascaramiento y la generalización **corren a cargo de los titulares de datos**, antes de compartir los conjuntos de datos con el intermediario de datos. Sin embargo, aparte del hecho de que, por estos medios, los titulares de los datos pasan a ser responsables de aplicar una generalización sólida, este enfoque plantea varios retos también desde el punto de vista de su aplicación.

Más concretamente, es esencial establecer un mecanismo que garantice que los distintos titulares de datos apliquen la generalización al mismo nivel; por ejemplo, si un titular de datos escoge un campo generalizado “45-50” para la edad, no debería haber otro titular de datos que elija un campo generalizado diferente como, p. ej., “40-50”. Por lo tanto, parece que esta naturaleza distribuida de los titulares de datos plantea algunas limitaciones, ya que es necesario que “acuerden conjuntamente” algunos parámetros. Teniendo en cuenta que la selección adecuada de estos parámetros depende en gran medida de cada conjunto de datos específicos, no se trata de una tarea sencilla.

3.4 CASO DE USO - INVESTIGACIÓN Y ANÁLISIS SOBRE LA EFICACIA DE LOS PRODUCTOS FARMACÉUTICOS

Otra posible utilización adicional del espacio de datos farmacéuticos previsto es apoyar la investigación y el análisis sobre la eficiencia de los productos farmacéuticos. Para simplificar, se supone que solo existen los dos tipos de titulares de datos, similares al caso de uso anterior, que se enumeran a continuación junto con la información que cada uno comparte con el intermediario de datos. Cada titular de datos almacena datos adicionales a los presentados; sin embargo, solo los datos enumerados a continuación se consideran necesarios para la prestación del servicio al usuario de datos.

- El **sistema nacional de prescripción electrónica** que comparte información relacionada con las recetas farmacéuticas;

Número de la Seguridad Social	Fecha de naci-miento	Género	Código postal	Medicación recetada	Dosis	Síntomas	Fecha de prescripción	Duración de la prescripción

- Los **proveedores sanitarios** que comparten información con respecto a:
    - la medicación que se utiliza para las enfermedades diagnosticadas y las posibles interacciones no deseadas entre los distintos medicamentos.

Enfermedad	Interacción no deseada de medicamentos	Indicadores de síntomas de interacción

    - El diagnóstico médico, los resultados de laboratorio y pruebas y la medicación prescrita de los pacientes tratados.

Número de la Seguridad Social	Diagnósticos médicos	Resultados de laboratorio y pruebas	Medicación prescrita

Los usuarios de datos son instituciones de investigación que pretenden recopilar información sobre la eficacia de los productos farmacéuticos para tratar síntomas específicos y sobre cómo han afectado a su eficacia las interacciones no deseadas de los medicamentos.

3.4.1 Tecnologías a utilizar

Dentro de este caso de uso, hay dos objetivos de diseño en cuanto a la aplicación de la ingeniería de protección de datos. El primer objetivo es que el intermediario pueda responder a las solicitudes de los usuarios de los datos (instituciones de investigación), sin poder identificar o individualizar a las personas. El segundo objetivo es que los usuarios de los datos tampoco puedan identificar o individualizar a las personas, y que tampoco puedan correlacionar los datos. Para alcanzar estos dos objetivos, los titulares de los datos deben aplicar técnicas específicas para enmascarar de la ingeniería de protección de datos al compartirlos.

1. El **proveedor nacional de recetas electrónicas** enmascara partes del conjunto de datos que se van a compartir de forma similar al caso de uso anterior. Una vez más, el campo del Número de la Seguridad Social (NUSS) se sustituye por un seudónimo generado de forma determinista, basado en una clave *k* que solo conoce el titular de los datos, y los cuasi-identificadores se sustituyen por rangos.
   Cabe señalar de nuevo que el grado de cada una de las generalizaciones anteriores depende del nivel de riesgo de que la salida resultante no permita la reidentificación o individualización respecto a una persona [16].
2. Los **proveedores de asistencia sanitaria** enmascaran también la parte del NUSS del conjunto de datos que se va a compartir con un seudónimo generado de forma determinista, basado en una clave *k* que solo conoce el titular de los datos.

Dado que el mismo campo será seudonimizado por distintos titulares de datos con una clave diferente, el intermediario de datos no podrá correlacionar los datos recibidos de distintos titulares de datos que hagan referencia al mismo NUSS.

3. El **intermediario** utilizará el Cifrado Polimórfico y Seudonimización (PEP, por sus siglas en inglés) [22] para los conjuntos de datos que se transmitirán a los usuarios de datos y actuará como transcriptor, como se explica también en [11]. A cada conjunto

de datos se le asignarán seudónimos diferentes para cada usuario de datos, evitando así la vinculación de seudónimos entre varios usuarios de datos. En este caso, el intermediario, aunque enmascare datos ya seudonimizados/generalizados, actúa como una entidad seudonimizadora tercera de confianza [19].

3.4.2 Consideraciones

El caso de uso descrito anteriormente prevé un escenario de compartición de datos en el que el enmascaramiento y la generalización **corren a cargo de los titulares de datos**, antes de compartir los conjuntos de datos con el intermediario de datos, pero el enmascaramiento adicional **corre a cargo del intermediario de datos.** Esta operación refuerza el papel de los intermediarios como organizadores fiables en lugar de meros intermediarios de la comparición de datos. Sin embargo, también aumento las responsabilidades y obligaciones del intermediario, tal y como se expone en el apartado 2.4.

Además de la interoperabilidad de la generalización analizada en los casos de uso anteriores, el papel adicional del intermediario conlleva responsabilidades adicionales que deben cumplirse. Incluso sin analizar si el intermediario debe considerarse responsable del tratamiento o encargado del tratamiento, tiene que ser capaz de hacer frente a las necesidades y los derechos de los interesados y los usuarios de datos, llevar un registro de las fuentes de datos y las actividades de tratamiento y, posiblemente, evaluar y actualizar las políticas de uso de datos en múltiples etapas a lo largo del ciclo de vida del tratamiento.

4. CONCLUSIONES

Los espacios comunes europeos de datos son un concepto emergente, esbozado por la estrategia europea de datos, cuyo objetivo es fomentar las actividades europeas hacia la economía de los datos. *Espacios de Datos* es un término paraguas que corresponde a cualquier ecosistema de posibles interacciones entre entidades de los sectores público y privado junto con nuevos procesos de gobernanza y empresariales. Estas competencias [23] tendrán que seguir un enfoque de ingeniería de datos para cumplir todos los requisitos y obligaciones legales.

La ingeniería de protección de datos no es una mera "herramienta de cumplimiento" del RGPD. Al aplicar las medidas adecuadas y las salvaguardias necesarias para reforzar los principios de protección de datos y permitir el ejercicio de los derechos de las personas, la ingeniería protección de datos ofrece a los responsables del tratamiento una opción práctica para compartir datos, minimizando al mismo tiempo el riesgo de uso indebido de la información, brechas de datos u otras amenazas de la seguridad [12]. El Desarrollo de casos de uso persuasivos y convincentes para compartir datos de forma segura y legal es uno de los retos más cruciales para el éxito de la aplicación de los Espacios Comunes Europeos de Datos.

Partiendo de la definición de los principales actores y de las disposiciones de la DGA en torno a los Espacios de Datos de la UE, la identificación de los elementos constitutivos y los requisitos representa el punto de partida para su desarrollo o despliegue satisfactorios. En el marco del presente informe, se ha intentado proporcionar un conjunto de elementos constitutivos en relación con la responsabilidad del responsable o responsables del tratamiento y del encargado o encargados. Estos elementos constitutivos pretenden abarcar mecanismos internos aplicables y renovados (políticas, procedimientos, evaluaciones basadas en el riesgo, controles técnicos y organizativos y otras medidas relacionadas con la compartición de datos), acuerdos de compartición de datos y programas de gestión de la privacidad (PMPs) adecuados.

Al tiempo que se intenta analizar más a fondo la incorporación de técnicas de enmascaramiento de datos personales en operaciones de tratamiento específicas, este informe esboza un espacio de datos previsto en el ámbito farmacéutico. A través de dos casos de uso concretos, se muestran las distintas funciones y responsabilidades que los titulares de los datos pueden asignar a los intermediarios en materia de protección de datos personales. Dados los diferentes objetivos de protección de datos de cada caso de uso, se demuestra cómo el intermediario podría participar activamente en el proceso de enmascaramiento de datos seudonimizados. Aunque este enfoque ya se haya debatido en un escenario típico de compartición de datos [11], puede explotarse aún más, ya que proporciona nuevos incentivos para la soberanía de los datos y las consideraciones de gobernanza de datos. Además, también se ha mostrado cómo los titulares de los datos y los intermediarios pueden aplicar en la práctica técnicas específicas de enmascaramiento y generalización.

A pesar del potencial de los espacios de datos de la UE, siguen existiendo consideraciones relativas a las medidas técnicas y organizativas adecuadas y a la forma de ponerlas en práctica, tanto desde el punto de vista de la protección de datos como de la ciberseguridad. Aunque ya existe un buen número de tecnologías de mejora de la privacidad que pueden ayudarnos a alcanzar objetivos específicos de protección de datos, no debemos descuidar el hecho de que estamos llamados a abordar nuevas operaciones de tratamiento, en las que las funciones y responsabilidades no siempre están claramente definidas.

5. REFERENCIAS

[1] Joint Research Centre, "Emerging approaches for data-driven innovation in Europe," 2022.

[2] ENISA, "Big Data Threat Landscape," 2016.

[3] ENISA, "Big Data Security," 2016.

[4] ENISA, "Privacy by design in big data," 2015.

[5] Comisión Europea, "Estrategia europea de datos," 2020.

[6] Unión Europea, "Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)," 2022.

[7] Joint Research Centre (European Commission), "European data spaces: Scientific insights into data sharing and utilisation at scale," 2023.

[8] Directorate-General for Financial Stability, Financial Services and Capital Markets Union, "Report on open finance," 2022.

[9] Unión Europea, "Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad)," 2019.

[10] AEPD, " Aproximación a los espacios de datos desde la perspectiva del RGPD," 2023.

[11] ENISA, "Ingeniería de compartición de datos personales," 2023.

[12] ENISA, "Ingeniería de la protección de datos: De la teoría a la práctica," 2022.

[13] AEPD, "Aproximación a los espacios de datos desde la perspectiva del RGPD," 2023.

[14] ENISA, "Privacy and Data Protection by Design," 2015.

[15] ENISA, "La adopción de técnicas de seudonomización", 2022.

[16] ENISA, "Data Pseudonymisation: Advanced Techniques and Use Cases," 2021.

[17] Comisión Europea, "COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEAO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y LAL COMITÉ DE LAS REGIONES Estrategia farmacéutica para Europa," 2020.

[18] Comisión Europea, "Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO por la que se establece un código de la Unión sobre medicamentos para uso humano y por la que se derogan la Directiva 2001/83/EC y la Directiva 2009/35/EC," 2023.

[19] ENISA, "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation," 2019.

[20] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 5, p. 557–570, 2002.

[21] B. Chen, D. Kifer and K. LeFevre, "Privacy-Preserving Data Publishing," *Foundations and Trends in Databases,* vol. 2, pp. 1-167, 2009.

[22] M. Hildebrandt, E. Verheul, B. Jacobs, C. Meijer and J. de Ruiter, "Polymorphic Encryption and Pseudonymisation for Personalised Healthcare: A Whitepaper," 2016.

[23] S. Scerri, T. Tuikka, I. de Vallejo and E. Curry, "Common European Data Spaces: Challenges and Opportunities," in *Data Spaces*, Springer, Cham, 2022.

[24] M. Hildebrandt, E. Verheul, B. Jacobs, C. Meijer and J. de Ruiter, "Polymorphic Encryption and Pseudonymisation for Personalised Healthcare: A Whitepaper," 2016.

[25] ENISA, "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation," 2019.

TP-03-23-445-EN-N

SOBRE ENISA

La Agencia de la Unión Europea de para la Ciberseguridad (ENISA) es un centro de conocimiento sobre seguridad de las redes y de la información para la UE, sus Estados Miembros, el sector privado y los ciudadanos europeos. ENISA trabaja con estos grupos para elaborar consejos y recomendaciones sobre buenas prácticas en materia de seguridad de la información. Ayuda a los estados miembros de la UE a aplicar la legislación comunitaria pertinente de la UE y trabaja para mejorar la resistencia de las infraestructuras y redes de información críticas de Europa. ENISA trata de mejorar los conocimientos técnicos existentes en los Estados Miembros de la UE apoyando el desarrollo de comunidades transfronterizas comprometidas con la mejora de la seguridad de las redes y la información en toda la UE. Más información sobre ENISA y su trabajo puede encontrarse en www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-650-7
doi: 10.2824/210862