APROXIMACIÓN A LOS ESPACIOS DE DATOS DESDE LA PERSPECTIVA DEL RGPD

v. mayo de 2023

RESUMEN EJECUTIVO

La tecnología permite que tanto las empresas privadas como las Administraciones Públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. La transformación digital y el creciente uso de los servicios digitales también entraña nuevos riesgos y desafíos para los destinatarios individuales de los correspondientes servicios, las empresas y la sociedad en su conjunto.

En dicho marco, el propósito del RGPD es proporcionar un marco sólido y coherente para la protección de los derechos fundamentales con relación a la protección de datos en la Unión Europea y, de esta forma, garantizar un nivel uniforme, homogéneo y elevado de protección a lo largo de la Unión. De esta forma, garantizando el control por parte de las personas físicas de sus propios datos personales, se genera confianza y se refuerza la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las Administraciones Públicas. Unas garantías eficaces del derecho fundamental a la protección de los datos personales y un conjunto de principios, derechos y herramientas de cumplimiento homogéneas entre los Estados de la Unión Europea tendrán como consecuencia la libre circulación de datos personales en la Unión, y el desarrollo del mercado digital europeo. Por lo tanto, el marco jurídico de la UE en el ámbito de la protección de los datos personales es un elemento facilitador, y no un obstáculo, para el desarrollo de una economía de los datos que corresponda a los valores y principios de la Unión, y es la base sobre la que construir un modelo europeo de gobernanza de datos.

Un Espacio de Datos se puede definir como una infraestructura federada y abierta para permitir el acceso soberano de datos, basada en una gobernanza, políticas, reglas y estándares que definen un marco de confianza para todos los intervinientes. Las iniciativas de Espacios de Datos europeas y nacionales plantean modelos de tratamientos de gran complejidad organizativa y tecnológica, así como de una gran escala en el número de sujetos afectados, en la diversidad de categorías de datos tratados, en los estamentos sociales involucrados, en la amplitud geográfica, en los periodos de conservación, en el número de intervinientes y otros. Estas iniciativas no se plantean como una reducción o un compromiso de los derechos y libertades de las personas físicas con relación a la protección de sus datos personales, sino que abren un horizonte de posibilidades que, para garantizar la sostenibilidad con relación al modelo europeo de derechos y libertades, obligan a realizar un análisis objetivo y crítico de su implementación desde el diseño que sea acorde al impacto del tratamiento.

El presente documento constituye una primera aproximación para el cumplimiento RGPD de los Espacios de Datos mediante la aplicación de los principios de responsabilidad proactiva y protección de datos desde el diseño. Sin buscar trasladar el texto del RGPD a este documento, ni de ser exhaustivos, el documento aborda el conjunto de definiciones procedentes del RGPD, de las distintas normas europeas, de normas específicas y vocabulario del ámbito de los Espacios de Datos. A continuación, se realiza una somera enumeración del marco normativo básico, y en desarrollo al momento de la elaboración de este documento, que afecta a los Espacios de Datos cuando implican el tratamiento de

datos personales. Seguidamente se realiza una aproximación a los tratamientos de datos personales en el marco de los Espacios de Datos.

El documento se cierra con dos grandes capítulos. El primero sobre la aplicabilidad de la protección de datos desde el diseño en los Espacios de Datos. Para ello, se ha de tener en cuenta que el acceso a los datos que permite un Espacio de Datos se define como toda utilización de datos de conformidad con unos requisitos específicos, pero, y es de gran importancia matizarlo, sin que ello implique necesariamente la transmisión o la descarga de los datos. A este respecto, existen distintos recursos tecnológicos que permiten la reutilización de datos personales con garantías de protección de datos ofreciendo más opciones que la anonimización. El documento se cierra con un capítulo sobre cuestiones relativas a la protección de datos en Espacios de Datos con relación a aspectos tan importantes como la implicación de los Delegados de Protección de Datos, o la gestión del riesgo para los derechos y libertades de las personas físicas, tanto desde el punto de vista de su individualidad como desde su perspectiva social, entre otros.

La "Aproximación a los espacios de datos desde la perspectiva de la normativa de protección de datos" está dirigida a los responsables y encargados de tratamiento que intervengan en los Espacio de Datos, así como a los Delegados de Protección de Datos, a los asesores en protección de datos y a todos los intervinientes que en el marco de un modelo de compartición de datos realicen tratamientos de datos personales, o que autoricen, supervisen o faciliten su tratamiento.

Palabras clave: Espacio de Datos, Protección de datos desde el diseño, gestión del riesgo, estrategia europea de datos, RGPD, Reglamento de Gobernanza de Datos, DGA.

Elaborado en colaboración y con la revisión del Dr. Alberto Palomo Lozano (Jefe de la Oficina del Dato de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) del Ministerio de Asuntos Económicos y Transformación Digital (MINETD)), de D. Carlos Alonso Peña (Director de la División de la Oficina del Dato de la SEDIA-MINETD), de D. Rafael Pérez Galindo (Subdirector General para la Sociedad Digital de la SEDIA-MINETD, de D. Jesús Jiménez López (Director del Consejo de Transparencia y Protección de Datos de Andalucía (CTPD)), de D. Manuel González Seco (Responsable del Gabinete de Cumplimiento del CTPD), de D. de la Dra. Sara Degli-Esposti (Investigadora Científica del IFS-CSIC del Consejo Superior de Investigaciones Científicas), del Dr. Rafael Pastor (Director/Decano de la Escuela Técnica Superior de Ingeniería Informática de la Universidad Nacional de Educación a Distancia) y del Dr. Ricard Martínez Martínez (Profesor Contratado Doctor del Departamento de Derecho Constitucional de la Universitat de València).

ÍNDICE

Índice de figuras

Acrónimos

AAPP:	Administraciones Públicas
AEPD:	Agencia Española de Protección de Datos
AIA:	Artificial Intelligence Act
CEPD:	Comité Europeo de Protección de Datos
DA:	Data Act
DGA:	Data Governance Act
DMA:	Digital Market Act
DSA:	Digital Service Act
DMZ:	Zona segura
DPD:	Delegado de Protección de Datos
EDPB:	European Data Protection Board
EDPS:	European Data Protection Supervisor
EHDS:	European Health Data Space
EIPD:	Evaluación de Impacto de Protección de Datos
ENISA:	European Union Agency for Cybersecurity
ENS:	Esquema Nacional de Seguridad
ETL:	Extract, Transform, Load
IoT:	Internet of Things
PET:	Privacy-Enhancing Technology
PIR:	Private Information Retrieval
RGPD:	Reglamento General de Protección de Datos
SEPD:	Supervisor Europeo de Protección de Datos
SDK:	Software Development Kit
SMPC:	Secure Multi-Party Computation
TEDH:	Tribunal Europeo de Derechos Humanos
TJUE:	Tribunal de Justicia de la Unión Europea
UE:	Unión Europea

I. INTRODUCCIÓN

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante Reglamento general de protección de datos, o RGPD) es la norma que protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de datos personales[1].

La protección de las personas físicas en relación con el tratamiento sus datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan[2].

La tecnología permite que tanto las empresas privadas como las Administraciones Públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades[3]. La transformación digital y el creciente uso de los servicios digitales también entraña nuevos riesgos y desafíos para los destinatarios individuales de los correspondientes servicios, las empresas y la sociedad en su conjunto[4]. Por ello, el RGPD nace de la exigencia de que se refuercen y especifiquen los derechos de los Interesados o Sujetos de los Datos y las obligaciones de quienes tratan y determinan el tratamiento de los datos personales[5].

El propósito del RGPD es proporcionar un marco sólido y coherente[6] para la protección de los derechos fundamentales con relación a la protección de datos en la Unión Europea y, de esta forma, garantizar un nivel uniforme, homogéneo y elevado de protección a lo largo de la Unión[7]. El objetivo de la norma es garantizar el control por parte de las personas físicas de sus propios datos personales[8], generar confianza y reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas. Para conseguir dicho objetivo, además de la existencia de la norma, será necesaria su ejecución estricta[9] y una supervisión ejercida de forma equivalente[10] entre los Estados Miembros.

Unas garantías eficaces del derecho fundamental a la protección de los datos personales y un conjunto de principios, derechos y herramientas de cumplimiento homogéneas[11] entre los Estados de la Unión Europea tendrán como consecuencia la libre

[1] Artículo 1.2 RGPD
[2] Considerando 1 del RGPD
[3] Considerando 7 del RGPD
[4] Considerando 1 del Reglamento de Servicios Digitales (DSA)
[5] Considerando 11 del RGPD
[6] Considerando 7 del RGPD
[7] Considerando 10 del RGPD
[8] Considerando 7 del RGPD
[9] Considerando 7 del RGPD
[10] Considerando 11 del RGPD
[11] A diferencia de lo constatado en la aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos

circulación de datos personales en la Unión[12]. Si entre los Estados Miembros hay divergencias en cuanto al nivel de garantía del derecho a la protección de datos, o en su forma de supervisión, se impediría la libre circulación y el buen funcionamiento del mercado interior. Por lo tanto, la exigencia[13] de un mismo nivel de cumplimiento del RGPD es básica para la libre circulación de personas[14], bienes y servicios, y del desarrollo del mercado digital europeo[15]. El marco jurídico de la UE en el ámbito de la protección de los datos personales es un elemento facilitador, y no un obstáculo, para el desarrollo de una economía de los datos que corresponda a los valores y principios de la Unión, y es la base sobre la que construir un modelo europeo de gobernanza de datos[16].

El presente documento analiza desde la perspectiva de protección de datos un modelo tecnológico para la implementación eficiente del "mercado interior de datos[17]" denominado Espacios de Datos, en cuanto supone tratamientos de datos personales[18]. Un Espacio de Datos no tiene una definición única, aunque es posible definirlo como una infraestructura federada y abierta para permitir el acceso soberano de datos, basada en una gobernanza, políticas, reglas y estándares que definen un marco de confianza para todos los intervinientes[19]. Normativamente se plantean diferencias jurídicas con relación a la definición de los intervinientes, los límites de los tratamientos y las garantías necesarias, en función de si se trata de la reutilización de datos en poder de organismos del sector público[20], servicios para establecer relaciones comerciales entre los intervinientes[21] o, por ejemplo, Espacios de Datos en sectores específicos[22]. Un Espacio de Datos es distinto a los almacenamientos centralizados de información, los *datalakes*[23], *data warehouses*[24], el intercambio bilateral de datos o puntos neutros, aunque las tecnologías subyacentes para la creación de un Espacio de Datos pueden ser en muchos casos coincidentes con las tecnologías con las que se implementan las soluciones anteriores.

Las iniciativas europeas y nacionales de Espacios de Datos, y sus desarrollos normativos, plantean modelos de tratamientos de gran complejidad organizativa, jurídica y tecnológica, así como de una gran escala en el número de sujetos afectados, en la diversidad de categorías de datos tratados, en los estamentos sociales involucrados, en la

[12] Considerando 13 del RGPD
[13] Considerando 13 del RGPD
[14] Schengen Acquis EUR-Lex - I33020 - EN - EUR-Lex (europa.eu)
[15] Un alto nivel de protección equivalente en todos los Estados es lo que garantiza la libre circulación de datos y no solo desde el punto de vista de protección de datos, sino como también establecen en otros ámbitos la DGA, la DMA, la DSA y las propuestas de DA y de AIA. La aplicación laxa y limitada de los niveles de protección establecidos en normativa sería el factor que impida de forma efectiva el mercado único.
[16] Párrafo 20 del documento "Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]".
[17] Considerando 2 de la DGA
[18] En aquellos Espacios de Datos donde no haya tratamientos de datos personales, p.ej. solo datos de entornos industriales, no aplicaría este documento.
[19] "What is a Data Space? Definition of the concept Data Space. White Paper 1/2022. (gaia-x – Hub Germany) [September 2022]" Whitepaper Definition Datenraum (gaia-x-hub.de)
[20] Capítulo II de la DGA, con las limitaciones desarrolladas en el Considerando 12, y la Directiva 2019/1024.
[21] Capítulo III de la DGA
[22] Como podría ser la propuesta de EHDS en el sector de datos sanitarios.
[23] Un único almacén de datos heterogéneos (estructurados, no estructurados u otros) que permite su catalogación y transformación para utilizarlos para tareas como informes, visualización, análisis avanzados y aprendizaje automático.
[24] Bases de datos internas operacionales o de analítica que las organizaciones necesitan/utilizan para su funcionamiento

amplitud geográfica, en los periodos de conservación, en la extensión en el tiempo del tratamiento, en el número de intervinientes y otros. Los Espacios de Datos abren un horizonte de grandes oportunidades, y para garantizarlas, así como para garantizar la sostenibilidad con relación al modelo europeo de derechos y libertades, obligan a realizar un análisis objetivo y crítico de su implementación desde el diseño que sea acorde al impacto del tratamiento.

Estas iniciativas no se plantean como una reducción o un compromiso de los derechos y libertades de las personas físicas con relación a la protección de sus datos personales. Con relación a esto, se ha de tener en cuenta que el acceso a los datos que se plantea en un Espacio de Datos se define como toda utilización de datos de conformidad con unos requisitos específicos, pero, y es de gran importancia matizarlo, sin que ello implique necesariamente la transmisión o la descarga de los datos, ni desplazando los principios y derechos del RGPD. A este respecto, existen distintos recursos tecnológicos que permiten el acceso a datos personales con garantías de protección de datos, ofreciendo más opciones que únicamente la anonimización o recurrir a la comunicación de datos personales.

El presente documento constituye una primera aproximación para el cumplimiento RGPD de los Espacios de Datos. No podría ser de otra forma cuando, a la complejidad intrínseca de las soluciones organizativas y técnicas planteadas, hay que añadir la complejidad de un paquete normativo que, además, está en pleno desarrollo. Aunque en el RGPD está claramente recogida la obligación de aplicar los principios de responsabilidad proactiva y protección de datos desde el diseño, no sería la primera vez que tratamientos innovadores se despliegan sin tener estos principios en cuenta. Por ello, aunque el RGPD es aplicable para todo tratamiento de datos personales independientemente de los medios técnicos que se utilizan para implementarlo, y que los responsables deben recabar el asesoramiento desde la concepción de los tratamientos de los Delegados de Protección de Datos (DPD) y expertos en protección de datos desde el concepto de los tratamientos, es imprescindible la acción temprana de la Autoridad de Control para garantizar que algunos aspectos se definan correctamente. Sin buscar trasladar el texto del RGPD a este documento, ni de ser exhaustivos, se realizará una asociación de los conceptos y términos empleados, se proporcionarán orientaciones para aplicar medidas y garantías de protección de datos desde el diseño en los tratamientos en el marco de un Espacio de Datos, tanto en la definición de su arquitectura como en sus mecanismos de gobernanza y se abordarán aspectos específicos sobre los principios, derechos y obligaciones con relación a los Espacios de Datos.

Este documento no supone una guía de obligado cumplimiento y su interpretación deberá hacerse sin perjuicio de la normativa sectorial aplicable[25]. Está dirigido a los responsables y encargados de tratamiento que intervengan en los Espacio de Datos, así como a los DPDs, a los asesores en protección de datos y a todos los intervinientes que en el marco de un modelo de compartición de datos realicen tratamientos de datos

[25] Si no existen tratamientos de datos personales se le aplicaría, por ejemplo, el Reglamento (UE) 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea

personales, o que autoricen, supervisen o faciliten, técnica u organizativamente, su tratamiento.

En su elaboración se ha tenido especialmente en cuenta las opiniones que sobre este tema han emitido el Comité Europeo de Protección de Datos (CEPD), el Supervisor Europeo de Protección de datos (SEPD) y las guías de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) sobre ingeniería de la privacidad[26].

El documento se estructura en los siguientes capítulos

- En primer lugar, un capítulo de definiciones, en el que se agrupan y relacionan definiciones procedentes del RGPD, de las distintas normas del paquete digital europeo, de normas específicas y vocabulario del ámbito de los Espacios de Datos.
- Un capítulo sobre el marco normativo básico que afecta a los Espacios de Datos cuando implican el tratamiento de datos personales.
- Una primera aproximación a los tratamientos de datos personales en el marco de los Espacios de Datos.
- La aplicabilidad de la protección de datos desde el diseño en los Espacios de Datos.
- Y finalmente un capítulo con cuestiones relativas a la protección de datos en Espacios de Datos, que no pretende ser exhaustivo, sino una primera aproximación.

[26] En el capítulo de referencias al final del texto se pueden encontrar las menciones a dichos documentos.

II. DEFINICIONES

En este capítulo se recogen las definiciones de los términos más relevantes que se emplean tanto en este documento como en la normativa y las referencias técnicas con relación a los Espacios de Datos.

- Acceso: toda utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.[27]
- Agregador de datos: servicio que permite aunar en un solo lugar datos existentes en distintas fuentes.
- Anonimización: Tratamiento sobre un conjunto de datos personales que genera un nuevo conjunto de datos que inhabilita la capacidad de relacionar estos datos con ninguna persona identificada o identificable.[28]
- Aprendizaje federado: técnica de aprendizaje automático que entrena un algoritmo a través de una arquitectura descentralizada de dispositivos que contienen sus propios datos locales y privados. Creado por Google en el año 2017, este enfoque contrasta con las técnicas en las que todos los datos se cargan en un servidor de forma centralizada. Gracias a ello se conserva la integridad de la información que está siendo utilizada para el aprendizaje sin poner en peligro la privacidad y seguridad.
- Calidad del dato: desde el punto de vista de un Espacio de Datos[29], la calidad del dato es un atributo subjetivo[30] asociado a un conjunto de datos sobre su utilidad para un tratamiento específico[31]. Este concepto es distinto del de calidad del datos del principio de exactitud[32] del RGPD.
- Catálogo de datos: una colección de descripciones de conjuntos de datos, organizada de manera sistemática y que contiene una parte pública orientada al usuario, en la que se puede acceder a la información relativa a los parámetros individuales de los conjuntos de datos por medios electrónicos a través de un portal en línea[33].
- Catalogación de datos: tratamiento que se realiza sobre datos o conjunto de datos que permite asociar a los mismos los metadatos necesarios para su explotación posterior. Generalmente implica la generación de Catálogos de recursos (datos) que se pueden poner a disposición de múltiples intervinientes.[34]

[27] Artículo 2.13) del DGA
[28] Apartado 2.2 del documento "WP 216 Dictamen 05/2014 sobre técnicas de anonimización (Grupo de Trabajo del Artículo 29) [10 de abril de 2014]"
[29] Se puede consultar los estándares UNE 0079 e ISO 25012.
[30] Data on the Web Best Practices: Data Quality Vocabulary (w3.org)
[31] En el artículo 2.ad) de la propuesta EHDS se define como: el grado en que las características de los datos sanitarios electrónicos son adecuadas para un uso secundario.
[32] Artículo 5.1.d) del RGPD
[33] Artículo 2.2.ac) de la propuesta EHDS
[34] Adaptado de la publicación de 28/12/2020 de la Oficina del Dato

- Cesión altruista de datos: todo intercambio voluntario de datos basado en el consentimiento de los interesados para que se traten sus datos personales, o en el permiso de los titulares de datos para que se usen sus datos no personales, sin ánimo de obtener o recibir una gratificación que exceda de una compensación relativa a los costes en que incurran a la hora de facilitar sus datos, con objetivos de interés general tal como se disponga en el Derecho nacional, en su caso, como, por ejemplo, la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, elaboración y difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica de interés general.[35]
- Ciclo de vida del dato: desde la perspectiva del Espacio de Datos, el ciclo de vida remite a las diferentes etapas por las que pasa un dato desde su nacimiento hasta el fin. El dato no es un activo estático durante su ciclo de vida, sino que pasa por distintas fases. Sin ser exhaustivos, ni por el orden expresado, podrían ser fases: extracción, carga, transformación, mantenimiento, síntesis, uso, publicación, almacenamiento o eliminación. No hay que confundir el concepto de ciclo de vida del dato en el marco de un Espacio de Datos, con el ciclo de vida del dato en un tratamiento.[36]
- Compute-to-data: estrategia que consiste en que, en vez de enviar los datos hacia los recursos de computación, los recursos de computación se llevan al origen de los datos. De esta forma se preserva la privacidad de los datos y el responsable (Titular de Datos) mantiene un mayor control sobre su tratamiento. Una forma de implementar "compute-to-data" es el aprendizaje federado, pero no la única.
- Conjunto de datos mixtos: conjunto de datos mixtos consta de datos personales y no personales. Los conjuntos de datos mixtos representan la mayoría de los conjuntos de datos utilizados en la economía de datos y son comunes debido a desarrollos tecnológicos como el Internet de las cosas (objetos que se conectan digitalmente), la inteligencia artificial y las tecnologías que permiten el análisis de macrodatos[37].
- Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.[38]
- Cooperativas de datos: los servicios de intermediación de datos ofrecidos por una estructura organizativa constituida por interesados, empresas unipersonales o pymes pertenecientes a dicha estructura, cuyos objetivos

[35] Artículo 2.16) de la DGA
[36] Apartado "V.C DESCRIPCIÓN DEL CICLO DE VIDA DE LOS DATOS" de la Guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales" de AEPD y de la publicación de 28/12/2020 de la Oficina del Dato sobre la importancia de la catalogación de datos.
[37] Apartado 2.2 de la Comunicación "Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea (COM(2019) 250 final) [29 de mayo de 2019]".
[38] Artículos 4, 6 y 7, considerandos 32, 42 y 43 del RGPD

principales sean prestar asistencia a sus miembros en el ejercicio de los derechos de estos con respecto a determinados datos, incluida la asistencia por lo que respecta a la adopción de decisiones informadas antes de consentir el tratamiento de datos, intercambiar opiniones sobre los fines del tratamiento de datos y las condiciones que mejor representen los intereses de sus miembros en relación con los datos de estos, y negociar las condiciones contractuales para el tratamiento de datos en nombre de sus miembros antes de conceder permiso para el tratamiento de datos no personales o antes de dar su consentimiento para el tratamiento de datos personales.[39]

- Datos: en el marco de los espacios de datos, toda representación de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual.[40]
- Datos de alto valor o HVDS: documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y del número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales conjuntos de datos[41].
- Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Los datos cifrados o seudonimizados son datos personales.[42]
- Datos no personales: aquellos que no entran en el ámbito de la definición anterior.
- Datos personales dinámicos y estáticos: los espacios de datos podrían contener datos personales estáticos, como el nombre, la dirección o la fecha de nacimiento, así como datos dinámicos que genera una persona, por ejemplo, a través del uso de un servicio en línea o un objeto conectado al Internet de las cosas. También podrían utilizarse para almacenar información de identidad verificada, como, por ejemplo, el número de pasaporte o la información sobre seguridad social, y credenciales (por ejemplo, permiso de conducir, diplomas o información sobre cuentas bancarias).[43]
- Datos protegidos: Aquellos que obren en poder de organismos del sector público que estén protegidos por motivos de confidencialidad comercial, protección de los derechos de propiedad intelectual de terceros, o protección

[39] Artículo 2.15) y Considerando 31 de la DGA.
[40] Adaptada del artículo 2.1) del DGA
[41] Definidos en la Directiva 2019/1024 traspuesta en la Ley 37/2007 sobre reutilización de la información en el sector público.
[42] Ampliada del artículo 4 del RGPD y su Considerando 24
[43] Considerando 30 del DGA

de los datos personales, en la medida en que estos últimos queden excluidos del ámbito de aplicación de la Directiva (UE) 2019/1024[44].

- ELT, ETL, EtLT: acrónimos que hacen referencia a los procesos de Extracción, Carga (Load) y Transformación de datos. La letra "t" minúscula hace referencia a procesos previos a la carga y a la transformación de los datos para su adaptación a formatos adecuados para un tratamiento concreto. Por ejemplo, la "t" podría hacer referencia a tratamientos de anonimización o seudonimización.
- Encargado del tratamiento (Encargado): la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, con una vinculación establecida con el responsable mediante un contrato u otro acto jurídico y que cumple con lo establecido en el artículo 28 del RGPD. En un mismo tratamiento puede haber varios encargados de tratamiento, y estos a su vez recurrir a subencargados (encargados de encargados).[45] Un encargado de tratamiento nunca es una persona o departamento del propio responsable de tratamiento, sino externa al propio responsable.
- Entorno de ejecución confiable: es un entorno de tratamiento inviolable que tiene lugar en el procesador principal de un dispositivo con un hardware y un software diseñados de tal manera que se garantiza la integridad y confidencialidad de los datos y del tratamiento realizado en dicho procesador frente a cualquier tipo de ataque. No debe confundirse con Entorno de Tratamiento Seguro donde además de los aspectos de confidencialidad, integridad y disponibilidad de los datos, se garantizan las obligaciones legales recogidas en el Derecho nacional y de la Unión[46].
- Entorno de Tratamiento Seguro: el entorno físico o virtual y los medios organizativos para garantizar el cumplimiento del Derecho de la Unión, como, por ejemplo, el RGPD, en particular, por lo que respecta a los derechos de los interesados, los derechos de propiedad intelectual y la confidencialidad comercial y estadística, la integridad y la accesibilidad, así como para garantizar el cumplimiento del Derecho nacional aplicable y permitir que la entidad encargada de proporcionar el Entorno de Tratamiento Seguro determine y supervise todas las acciones de tratamiento, incluida la presentación, el almacenamiento, la descarga y la exportación de datos, así como el cálculo de datos derivados mediante algoritmos computacionales.[47]
- Espacio de datos: infraestructura basada en mecanismos comunes de gobernanza, organizativos, normativos y técnicos, que facilita el acceso a los datos y, con ello, el desarrollo de modelos de negocio basados en su exploración y explotación.

[44] Definición adaptada del artículo 3.1 de la DGA
[45] Artículo 4.1 del RGPD
[46] Apartado 4.3 del documento "INGENIERÍA DE LA PROTECCIÓN DE DATOS, De la teoría a la práctica. European Union Agency for Cybersecurity (ENISA) [Enero de 2022]"
[47] Artículo 2.20) del DGA

- Extracción de datos: tratamiento que se realiza sobre un conjunto de datos para generar un nuevo conjunto de datos más acorde con las necesidades de un caso de uso. En el nuevo conjunto puede que se limite la extensión de los datos en sus categorías de datos (p.ej. no todos sus atributos), su granularidad (p.ej. no extraer la dirección completa pero sí el código postal), su frecuencia (p.ej. tan solo una posición de localización por día), precisión (p.ej. en vez de la edad del interesado, indicar únicamente la calificación en menores o adultos), etc.
- Guardián de acceso: se define en la DMA como una empresa prestadora de servicios básicos de plataforma, para el objeto de este documento un servicio de computación en la nube, con gran influencia en el mercado interior y con una posición afianzada y duradera.
- Habilitador: actor(es) que proporciona servicios o herramientas que permiten compartir o explotar conjuntos de datos e implementar medidas de gobernanza.[48]
- Hiperescalar: es un servicio básico de plataforma[49] que específicamente presta servicio de almacenamiento y procesado masivo en la nube que puede escalar un entorno de computación distribuido a miles de servidores.
- Intercambio de datos: la facilitación de datos por un interesado o Titular de Datos a un Usuario de Datos, directamente o a través de un intermediario y en virtud de un acuerdo voluntario o del Derecho de la Unión o nacional, con el fin de hacer un uso en común o individual de tales datos, por ejemplo, mediante licencias abiertas o mediante licencias comerciales de pago o gratuitas.[50]
- Interesado, Sujeto de los datos, Afectado[51]: persona física identificada o identificable. A lo largo del documento se utilizará el término "sujeto de los datos", que es la traducción literal de la versión en inglés del RGPD, ya que el término "interesado" puede tener un significado ambiguo en el entorno de los Espacios de Datos y confundirse con el de parte interesada o "stakeholder".[52]
- Mediador del Espacio de Datos, Mediador de Datos: entidades que establecen las relaciones en el Espacio de Datos entre los Sujetos de los Datos y/o Titulares de los Datos, por una parte, y los Usuarios de los Datos, por otra. En el marco de la DGA se considerarán Mediadores a los "organismos competentes"[53], los "servicios de intermediación de datos" (y su subtipo las "cooperativas de datos") y las "organizaciones de gestión de datos con fines altruistas". En el marco de la propuesta de EHDS será, entre otros, la plataforma central para el uso secundario de datos sanitarios electrónicos. En otros ámbitos se denominan "proveedor de datos", "operador del espacio de datos", etc.
- Metadatos: en el marco de los Espacios de Datos, son los datos acerca de los datos y sirven para suministrar información sobre los datos que queremos usar.

[48] Herramienta para elaborar casos de uso en espacios de datos de la Oficina del Dato
[49] Artículo.2.2) de la DMA
[50] Artículo 2.10) del DGA
[51] En el sentido de la LOPDGDD
[52] Artículo 4 del RGPD
[53] Artículo 7 de la DGA

Los metadatos consisten en información que caracteriza datos, describe su contenido y estructura, las condiciones de uso, su calidad para un contexto, su origen y transformación, entre otra información relevante. Pueden tener carácter técnico, operacional o de negocio.[54]

- Organismo competente: organismo del sector público que presta asistencia a otros organismos del sector público para la reutilización de datos mediante técnicas punteras, proporciona las mejores prácticas sobre tratamientos y sobre entornos seguros de tratamiento que permitan preservar la privacidad de la información. Entre sus tareas puede figurar la concesión de acceso a los datos, cuando así lo exija la normativa sectorial de la Unión o nacional.[55]
- Órgano supervisor: será la entidad con la obligación de evaluar cada una de las solicitudes presentadas por parte de un Usuario de Datos y conceder, o no, a la demanda de tratamiento solicitada, en particular, teniendo en cuenta el cumplimiento de las previsiones del RGPD.
- Responsable del tratamiento (Responsable): la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos igualmente el Derecho de la Unión o de los Estados miembros.[56] No hay que confundir el concepto Responsable RGPD con el concepto de responsable funcional de un proceso o departamento en la atribución orgánica de obligaciones en una entidad. Este será sólo será un usuario autorizado dentro de la organización.
- Reutilizador: aunque no está definido explícitamente[57], se infiere de la definición de reutilización, que es la persona física o jurídica que reutiliza los datos que obran en poder de organismos del sector público, con fines comerciales o no comerciales distintos del propósito inicial englobado en la misión de servicio público para el que se hayan producido tales datos, excepto en el caso del intercambio de datos entre organismos del sector público con la única finalidad de desempeñar sus actividades de servicio público[58].
- Servicio básico de plataforma[59]: se puede aplicar a cualquiera de los siguientes elementos: servicios de intermediación en línea; motores de búsqueda en línea; servicios de redes sociales en línea; servicios de plataforma de intercambio de vídeos; servicios de comunicaciones interpersonales independientes de la numeración; sistemas operativos; navegadores web; asistentes virtuales; servicios de computación en nube; servicios de publicidad en línea.

[54] Adaptado de la publicación de 28/12/2020 de la Oficina del Dato sobre la importancia de la catalogación de datos.
[55] Artículo 7 y Considerando 26 de la DGA
[56] Artículo 4 del RGPD
[57] Borradores de la DGA definían Reutilizador como la persona física o jurídica que reutiliza los datos que obren en poder de organismos del sector público, con fines comerciales o no comerciales distintos del propósito inicial englobado en la misión de servicio público para el que se hayan producido tales datos. Esta definición no se encuentra en la actual redacción.
[58] Artículo 2.2) de la DGA
[59] Artículo 2.2) de la DMA

- Servicio de intermediación de datos[60]: tal como se define en la DGA, todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por una parte, y usuarios de datos, por otra, a través de medios técnicos, jurídicos o de otro tipo, incluidos los servicios destinados al ejercicio de los derechos de los interesados en relación con los datos personales[61]. En esta definición quedan excluidos, al menos, los servicios que obtengan datos de Titulares y que los traten con el fin de añadirles un valor sustancial y concedan licencias a los Usuarios de Datos, sin establecer una relación comercial entre Titulares y Usuarios; los servicios dedicados a la intermediación de contenido protegido por derechos de autor; los servicios utilizados exclusivamente por un único Titular de Datos para permitir la utilización de sus los datos; los utilizados por múltiples personas jurídicas en un grupo cerrado, incluyendo también los utilizados en las relaciones con proveedores o con clientes o las colaboraciones establecidas contractualmente, en particular, los que tienen como objetivo principal garantizar las funcionalidades de los objetos y dispositivos conectados al internet de las cosas[62]; los servicios de intercambio de datos ofrecidos por organismos del sector público sin la intención de establecer relaciones comerciales[63].
- Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.[64]
- Soberanía del dato: Concepto no definido en la norma europea y que se interpreta generalmente como la idea de que el lugar en el que se recogen los datos determina la regulación y la gobernanza que se aplican a los mismos, y también como la capacidad de los gobiernos y las empresas para disponer de los datos digitales de los usuarios y las empresas.
- Sujeto de los datos: ver definición de “Interesado”.
- Tratamiento de datos personales: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.[65]

[60] Artículo 2.11) de la DGA
[61] No hay que confundirlo con “servicio intermediario”, definido en el artículo 3.g) de la DSA, o “servicio de intermediación en línea”, definido en la P2B, Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.
[62] En esos casos abría que remitirse a la propuesta de la DA
[63] Por ejemplo, los organismos competentes establecidos en el Artículo 7 de la DGA
[64] Artículo 4 del RGPD
[65] Artículo 4 del RGPD

- Titular de Datos: toda persona jurídica, incluidos los organismos del sector público y organizaciones internacionales, o persona física que no sea el interesado con respecto a los datos específicos en cuestión, que, de conformidad con el Derecho de la Unión o nacional aplicable, tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos.[66]
- Trazabilidad del dato: es la capacidad de conocer todo el ciclo de vida del dato.[67]
- Usuario de datos: toda persona física o jurídica que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el RGPD en el caso de los datos personales, a usarlos con fines comerciales o no comerciales.[68]

[66] Artículo 2.8) del DGA
[67] Adaptado de la publicación de 28/12/2020 de la Oficina del Dato sobre la importancia de la catalogación de datos.
[68] Artículo 2.9) de la DGA

III. EL MARCO NORMATIVO PARA LOS ESPACIOS DE DATOS

En la medida en que se realicen tratamientos de datos personales en un Espacio de Datos el marco normativo comienza a definirse por Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

En relación con la utilización de datos en el mundo digital, se está desarrollando un paquete de normas europeas y nacionales que no modifican el régimen del tratamiento de los datos personales para cualquiera de las actividades reguladas o los requisitos de información dispuestos en el RGPD[69], y en caso de conflicto con el Derecho de la Unión en materia de protección de datos personales o el Derecho nacional adoptado en la materia de protección de datos personales, debe prevalecer este último[70].

A. MARCO EUROPEO DE DATOS

Sin ánimo de exhaustividad, a continuación, se indican las siguientes normas básicas:

- El Reglamento de Gobernanza de Datos (DGA)[71] que regula las condiciones para la reutilización de determinadas categorías de datos que obren en poder de organismos del sector público y también define unas categorías de intervinientes en un Espacios de Datos para el aprovechamiento de datos procedentes tanto del sector privado como público. La DGA define condiciones y garantías para nuevos modelos de negocio del dato, como los servicios de intermediación de datos, así como la cesión altruista de datos, entre otros[72]. La DGA complementa a la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público entre otros aspectos definiendo las condiciones de reutilización de determinadas categorías de datos en poder del sector público que estén protegidos por motivos de confidencialidad comercial o estadística, derechos de propiedad intelectual o datos personales.
- El Reglamento de Mercados Digitales (DMA)[73] en cuanto regula los servicios básicos de plataforma prestados u ofrecidos por Guardianes de Acceso, en particular, aquellos relativos a servicios de computación en la nube.
- El Reglamento de Servicios Digitales (DSA)[74] en cuanto establece normas armonizadas sobre la prestación de servicios intermediarios en el mercado interior.

[69] Artículo 1.3 y considerando 4 de la DGA, artículo 1.3 y considerando 7 y 24 de la propuesta de DA,
[70] Artículo 1.3 y considerando 4 de la DGA, artículo 2.4 de la DSA, considerando 24 y artículo 1.3 de la propuesta de DA.
[71] 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 o DGA),
[72] Se explica la Ley de Gobernanza de Datos | Configurar el futuro digital de Europa
[73] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales o DMA)
[74] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales o DSA)

- El Reglamento de Libre Circulación de Datos no Personales[75] y las Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, con relación al tratamiento de conjuntos de datos mixtos.
- El Reglamento de Ejecución (UE) 2023/138 de la Comisión de 21 de diciembre de 2022 por el que se establecen una lista de conjuntos de datos específicos de alto valor y modalidades de publicación y reutilización.

B. PROPUESTAS DE REGULACIÓN EUROPEA

El paquete de regulación digital se completa con las propuestas de la Comisión Europea todavía en tramitación, de las que, igualmente sin ánimo de ser exhaustivos, cabe destacar las siguientes:

- La propuesta del Reglamento de Datos (DA) que, entre otros aspectos, amplia los derechos de acceso a datos no personales y dedica en el Capítulo VIII a las obligaciones de interoperabilidad en los Espacios de Datos.
- La propuesta de Reglamento de Espacio Europeo de Datos Sanitarios (EHDS).
- La propuesta de Reglamento de Inteligencia Artificial (AIA).

También se considera importante destacar todas las iniciativas existentes a día de hoy sobre de espacios europeos de datos dentro del marco de la European Strategy for Data así como del Mercado Único Digital, publicadas en el documento de trabajo sobre espacios comunes de datos europeos "Staff working document on data spaces" de la Comisión el 23 de febrero de 2022, en el marco de su línea de trabajo sobre Espacios de Datos, donde, entre otras cosas, se fijan las áreas sobre las que crear estos espacios de datos. Los Espacios Europeos de Datos, además de en el ámbito de la salud, incluyen los sectores de "*Manufacturing, Green Deal, Mobility, Financial, Energy, Agriculture, Legal, Procurement, Security, Skills, Open Science, Media, Cultural heritage, Tourism, Construction* y *Smart communities*".

C. REGULACIÓN NACIONAL

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

[75] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea

D. PROPUESTAS DE REGULACIÓN NACIONAL

En el ámbito nacional, a la hora de redactar estas orientaciones, se ha previsto la creación de un Espacio de Datos Integrado de Movilidad (EDIM) en la futura Ley de Movilidad Sostenible (anteproyecto de ley aprobado en Consejo de Ministros de 12 de diciembre 2022).

En la norma se establecerá su creación, definición y gobernanza[76]. En particular, en su artículo 104 sobre infracciones graves identifica en lo referente a suministro de datos al EDIM: "*la utilización para finalidades distintas de suministro de datos al EDIM de los datos personales obtenidos directamente por parte de los operadores de transporte, gestores de infraestructura y centros de actividad. En este caso, el procedimiento sancionador será el establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales por el órgano competente en materia de protección de datos personales*."

Por otro lado, también cabe mencionar a nivel nacional algunas líneas de trabajo en Espacios de Datos impulsadas por la Administración General del Estado:

- Desarrollo del Hub nacional de Gaia-X para el desarrollo de una infraestructura de datos abierta y segura, para lo que se están creando diversos grupos de trabajo centrados en sectores específicos: salud, industria 4.0, turismo, movilidad, agroalimentario, ingeniería y construcción, tecnologías habilitadoras, finanzas y administración pública, así como otros cuatro grupos de trabajo transversales orientados a aspectos legales, técnicos, proyectos y ética.
- Proyecto llevado a cabo por la Oficina del Dato en el sector del turismo para la realización de sesiones de trabajo orientadas al levantamiento de casos de uso y la complementariedad de los espacios de datos con la Plataforma Inteligente de Destinos de SEGITTUR del Ministerio de Industria, Comercio y Turismo.
- Creación de un "*data lake* sanitario" en el marco de la Estrategia de Salud Digital a través de la Comisión de salud digital del Consejo Interterritorial del Sistema Nacional de Salud, según el componente 18.I6 del Plan de Recuperación, Transformación y Resiliencia.
- Creación de la Plataforma del dato de la AGE alrededor de la cual se desplegarán los futuros espacios de datos del sector público.
- Desarrollo de las iniciativas Redes Territoriales de Especialización Tecnológica (RETECH) con componentes de espacios de datos, financiadas desde la Secretaría de Estado de Digitalización e Inteligencia Artificial y desarrolladas por diferentes CCAA coordinadamente.
- El futuro "Plan estratégico para la transformación y digitalización del sistema agroalimentario y la cadena logística para la promoción de grandes espacios de datos de alto valor que soporten la transformación digital de los sectores productivos", a través del componente 11.I2 del Plan de Recuperación,

[76] Artículos 6, 14 y 8 del Anteproyecto de Ley de Movilidad Sostenible.

Transformación y Resiliencia, como parte de una de las iniciativas de la "Lanzadera de proyectos tractores".

- Además, existen proyectos como el de Digitalización del Ciclo del Agua, dentro del objetivo de mejora de la eficiencia del ciclo urbano del agua, que ya contemplan la necesidad de realizar un desarrollo digital en el sector para poder cumplir los requisitos que se están estableciendo a nivel europeo para el Espacio de Datos del sector: "*Los diferentes sistemas de información mencionados, deberán garantizar una compartición fluida de datos entre ellos y con los oportunos sistemas externos, siguiendo para ello las recomendaciones y directrices fijadas por la Oficina del dato del Gobierno de España, garantizando así el cumplimiento allí donde sea necesario con el Esquema Nacional de Interoperabilidad (RD 4/2010) y las condiciones y requisitos derivados del espacio de datos sectorial europeo de medioambiente (Common European GreenDeal dataspace).*"

IV. TRATAMIENTOS SOBRE LOS ESPACIOS DE DATOS

El ámbito material del RGPD son tratamientos de datos personales[77]. En conjuntos de datos mixtos, cuando el tratamiento de datos no personales esté indisolublemente vinculados a datos personales, el tratamiento estará sujeto también al RGPD[78].

El RGPD no tiene como ámbito material las tecnologías o infraestructuras tecnológicas, ya que éstas son medios para implementar tratamientos de datos. Un Espacio de Datos es una infraestructura que permite implementar múltiples tratamientos. En la medida que un Espacio de Datos implique tratamientos de datos personales, estará sujeto a la normativa de protección de datos, sin perjuicio de la normativa sectorial aplicable[79].

Toda reutilización de datos personales debe respetar siempre los principios de licitud, lealtad y transparencia, así como la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del plazo de conservación, la integridad y la confidencialidad, de conformidad con el artículo 5 del RGPD[80]. Para el pleno cumplimiento RGPD han de estar bien definidos los tratamientos, y para ello se empezará por determinar con precisión sus finalidades, sus responsables y su legitimación.

A. CATEGORÍAS DE INTERVINIENTES EN UN ESPACIO DE DATOS DESDE LA PERSPECTIVA RGPD

Desde el punto de vista de la protección de datos se podrían identificar los siguientes intervinientes o roles en el Espacio de Datos:

1. Interesados o Sujetos de los datos
2. Titular de Datos
3. Usuario de Datos
4. Mediadores del Espacio de Datos
5. Habilitadores técnicos y legales
6. Supervisor de las solicitudes de acceso
7. Otros, como las autoridades de control.

Esta división de intervinientes tiene un carácter didáctico. En la aplicación práctica será posible encontrar entidades que ejecuten varios roles con mayor o menor extensión. Ya en la DGA se define un tipo de Espacio de Datos, las Cooperativas de datos, en la que una persona física podría actuar como Sujeto de los Datos, Titular de Datos, Mediador y Usuario de Datos[81]. Por otro lado, la DGA también limita en el caso de los Servicios de Intermediación de Datos los roles que puede adoptar[82].

---

[77] Artículo 2 del RGPD

[78] Apartado 2.2 de la Comunicación "Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea (COM(2019) 250 final) [29 de mayo de 2019]" y el Considerando 30 de la propuesta de DA.

[79] Si no existen tratamientos de datos personales se le aplicaría, por ejemplo, el Reglamento (UE) 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea

[80] Párrafo 73 del documento "Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]".

[81] Considerando 31 de la DGA

[82] Artículo 12.1 de la DGA "*los proveedores de servicios de intermediación de datos no podrán utilizar los datos en relación con los que presten sus servicios para fines diferentes de su puesta a disposición de los usuarios de datos y prestarán los servicios de intermediación de datos a través de una persona jurídica distinta*"

A modo ilustrativo se incluye un esquema donde se muestran las diferentes relaciones entre los diferentes intervinientes para que sirva de apoyo en la descripción del proceso que se recoge a continuación.

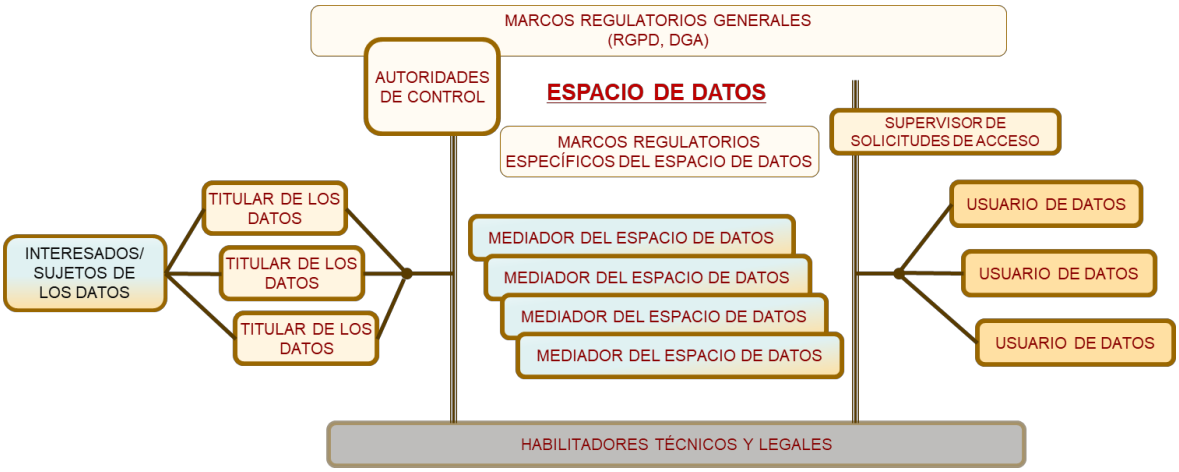

Figura 1: Esquema de relaciones de los intervinientes desde la perspectiva del RGPD

En este apartado se realizará una breve descripción de los intervinientes, y en el último apartado de este capítulo, se tratará sobre la determinación de los roles responsable/encargado.

Interesado o Sujeto de los Datos

En marcos generales de espacios de datos, el Interesado o Sujeto de los Datos, es decir, la persona física identificada o identificable cuyos datos personales son los que se plantea tratar, podría asociarse a la definición de "productor de los datos" utilizada en algunos esquemas de Espacios de Datos. Cuando se asocia la figura de "productor de los datos" a sistemas o servicios que recogen o generan datos personales de personas físicas (p.ej. sistemas IoT), en la medida en que dichos datos estén vinculados a personas identificadas o identificables, seguiremos hablando de datos de un interesado.

Sin embargo, cuando hablamos de datos personales, un interesado no es un mero "productor de los datos" sino una persona física cuyos datos solo pueden ser tratados de acuerdo con el cumplimiento de los principios, legitimación, respeto a los derechos y resto de obligaciones establecidas en el RGPD.

Titular de Datos

En el Capítulo "Definiciones" de este documento se ha transcrito la definición de Titular de Datos trasladando la establecida en la DGA, como aquella persona que tenga derecho a conceder acceso a determinados datos personales o no personales. Los Titulares de Datos, en el marco de un Espacio de Datos, podrían ejecutar operaciones de comunicación de datos, de aplicación de mecanismos para permitir el tratamiento *on-premises*, realizar tratamientos de seudonimización y anonimización, otros tratamientos como extraer datos sintéticos, proporcionar acceso con implementación de privacidad diferencial, realizar comunicaciones de datos a otros responsables u otros.

En marcos generales de Espacios de Datos se puede encontrar esta figura etiquetada como el "dueño de los datos" o "custodio de los datos". Esta denominación es engañosa cuando se refiere a datos personales, porque un responsable de tratamiento no posee los datos de los Interesados o Sujetos de los Datos, sino que dispone de una base jurídica que lo legitima para su tratamiento conforme a las obligaciones que se establecen en la normativa de protección de datos.

La definición de Titular de Datos podrá cambiar para determinados Espacios de Datos específicos establecidos normativamente, definiendo entidades de un sector determinado o matizando su definición[83].

Usuario de datos

El Usuario de Datos es toda persona física o jurídica que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el RGPD en el caso de los datos personales, a usarlos con fines comerciales o no comerciales[84]. En otros ámbitos puede recibir otros nombres, como "consumidor de datos". En la Directiva 2019/1024[85] utiliza el término "usuario final" para aquellos reutilizadores de datos de los organismos del sector público que actúan como Usuarios de Datos[86].

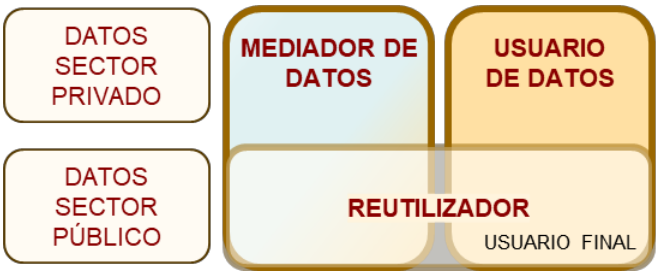

Figura 2: Correspondencia entre los términos Reutilizador, Usuario de Datos (empleados en la DGA) y Mediador (por ejemplo, los "servicios de intermediación de datos" o las "organizaciones que gestionan datos con fines altruistas" de la DGA)

En el marco de un tratamiento específico en el marco de un Espacio de Datos, una entidad podría actuar como Usuario de Datos, en otro tratamiento podría actuar como Titular de Datos, mientras que se podrán encontrar tratamientos donde una misma entidad será Usuaria de unos datos y Titular de otros.

[83] En el caso de la propuesta de EHDS, se define «titular de datos»: toda persona física o jurídica que sea una entidad o un organismo del sector sanitario o asistencial, o que lleve a cabo investigaciones en relación con estos sectores, así como instituciones, órganos y organismos de la Unión que tengan el derecho o la obligación, de conformidad con el presente Reglamento, con el Derecho de la Unión aplicable o con la legislación nacional por la que se aplique el Derecho de la Unión, o, en el caso de los datos no personales, mediante el control del diseño técnico de un producto y de los servicios conexos, de poner a disposición, así como de registrar o entregar determinados datos, restringir el acceso a ellos o intercambiarlos.

[84] Artículo 2.9) de la DGA

[85] Directiva (UE) 2019/1024 del Parlamento europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida)

[86] Hay que tener en cuenta que no todos los Usuarios de Datos serán reutilizadores de datos de organismos del sector público, ni todos los reutilizadores serán Usuarios de Datos.

Mediador del Espacio de Datos

Los Mediadores del Espacio de Datos son las entidades que establecen las relaciones en el Espacio de Datos entre los Sujetos de los Datos y/o Titulares de los Datos, por una parte, y los Usuarios de los Datos, por otra. Son aquellos que implementan los medios técnicos, jurídicos, organizativos, o de otro tipo que permiten la operación del Espacio de Datos entre múltiples Titulares y múltiples Usuarios de Datos. Dependiendo del contexto en el que opere el Mediador podrá tender una definición jurídica distinta como, por ejemplo, "servicio de intermediación de datos", "organismo competente", "organizaciones de gestión de datos con fines altruistas", "cooperativas de datos", etc. Igualmente, en las referencias técnicas a Espacios de Datos se podrán encontrar nombres como "proveedor de datos", "operador del espacio de datos", u otros.

Los Mediadores también podrán denominarse como "reutilizadores" con relación a la DGA cuando traten datos de organismos del sector público[87]. Mediadores también pueden ser organismos del sector público.

En el marco de un Espacio de Datos genérico, una o varias entidades Mediadoras podrían realizar tratamientos para la creación de catálogos de datos, creación de bases de datos centralizadas, transformación de los datos, creación de plataformas de intercambio o explotación de datos, gestión de consentimientos, etc. Además, el Mediador realizaría un seguimiento de todas las fuentes de datos y tratamientos, evaluaría y actualizaría las políticas de uso de datos a lo largo del ciclo de vida del tratamiento de datos. El Mediador de Datos registraría las comunicaciones de datos para cada Usuario de Datos con el que interactúa, y también para la mayoría de los Sujetos de los Datos, además de otras funciones[88]. De ahí cabe inferir que estas entidades son claves para la implementación de medidas de protección de datos desde el diseño y por defecto.

En el caso de que el Mediador se defina como un servicio de intermediación de datos de la DGA, estas entidades tendrán que cumplir las condiciones para la prestación de servicios de intermediación de datos recogidas en la DGA. El Mediador podrá incluir la oferta de herramientas y servicios específicos adicionales a los Titulares de Datos o a los Sujetos de los Datos con el objetivo específico de facilitar el intercambio de los datos (p.ej. el almacenamiento temporal, la organización, la conversión, la anonimización y la seudonimización), siempre que tales herramientas y servicios solo se utilicen previa solicitud o aprobación expresas del Titular de Datos o del Sujeto de los Datos, y que las herramientas de terceros ofrecidas en ese contexto no se utilicen para otros fines[89]. La DGA[90] proporciona ejemplos de "servicios de intermediación de datos" como mercados de datos en los que las empresas podrían poner datos a disposición de terceros, facilitadores de ecosistemas de intercambio de datos abiertos a todas las partes interesadas, por ejemplo, en el contexto de espacios comunes europeos de datos, así como conjuntos de datos creados en común por varias personas físicas o jurídicas con la intención de conceder licencias para la utilización de dichos conjuntos de datos, de manera que todos

[87] Ver definición de reutilizador.
[88] Apartado 4.3 del documento *"ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA) [January 2023]"*.
[89] Artículo 12.e) de la DGA
[90] Considerando 28 de la DGA

los participantes que contribuyan a su puesta en común reciban una gratificación por su contribución.

En el caso de que los Mediadores gestionen datos cedidos con fines altruistas, en caso de que, voluntariamente, hayan decidido solicitar la inscripción en los registros nacionales de organizaciones de gestión de datos cedidos con fines altruistas reconocidos en la Unión, deberán cumplir con las condiciones y requisitos de la DGA.

En el marco de la propuesta del EHDS[91] se podrían considerar Mediadores a la plataforma central para la salud digital, MiSalud@EU (*MyHealth@EU*), el punto de contacto nacional para el uso secundario de datos sanitarios electrónicos, plataforma central para el uso secundario de datos sanitarios electrónicos y DatosSalud@UE (*HealthData@EU*).

Supervisor de las solicitudes de acceso

Las entidades supervisoras serán aquellas encargadas de evaluar las solicitudes presentadas por parte de un Usuario de Datos para el tratamiento de datos personales.

Dependiendo de la finalidad del Espacio de Datos, la concesión de la solicitud puede estar sujeta a distintas normativas y principios éticos. Una de las normativas a tener en cuenta será la específica y sectorial con relación a la protección de datos. Estas normativas pueden exigir que dicha función la realice un organismo independiente, o al menos ajeno a cualquier otra función en el Espacio de Datos.

En el caso de que las solicitudes incluyan acceso a los datos personales, este Supervisor deberá establecer las condiciones en la que se le dará acceso a los datos en función, entre otras, de la base jurídica en la que se basa la petición y las medidas que se presentan para garantizar y poder demostrar el cumplimiento. También debería establecer en ciertas ocasiones las condiciones de acceso a los datos personales, independientemente de las medidas para la gestión del riesgo, donde figurarán, entre otras cosas, los mecanismos de seudonimización y/o anonimización previstos, el Entorno de Tratamiento Seguro habilitado para el tratamiento de datos personales y la limitación temporal de acceso a estos datos. Las Evaluaciones de Impacto en la Protección de Datos (EIPDs) con relación al tratamiento solicitado deberían ser parte de los elementos a incluir en las solicitudes.

Las entidades supervisoras no pueden eximir a los responsables del tratamiento de cumplir con sus obligaciones en virtud de la legislación de la UE en materia de protección de datos, cuya observancia queda atribuida a las autoridades de control independientes creadas a tal efecto[92].

El Supervisor podría ser parte de la entidad de un Mediador del Espacio de Datos y ejercer ciertas funciones del Habilitador de protección de datos. Por ejemplo, pudiera darse ese caso con los Organismos Competentes definidos en la DGA cuando así lo exija la normativa sectorial de la Unión o nacional[93]. Si no fuera así, para ejercer apropiadamente sus funciones es recomendable que se coordine con los Mediadores del Espacio de Datos

[91] Artículo 2 de la propuesta EHDS.
[92] Párrafo 29 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*
[93] Considerando 26 de la DGA

necesarios y con el propio Usuario de Datos para conocer como alcanzar la protección de datos desde el diseño, con el apoyo del Habilitador de protección de datos quien orientará al Usuario de Datos sobre las acciones que debe llevar a cabo para dar cumplimiento al RGPD.

Habilitador

Los Habilitadores en el entorno de un Espacio de Datos serían aquellos que darán apoyo a todos los intervinientes anteriormente descritos para poder garantizar que la implementación se realiza un proceso eficiente, coherente, implementando los mecanismos de gobernanza y gestión entre múltiples intervinientes, evitando duplicidades y repeticiones de tareas, facilitando los trámites y solicitudes.

Las funciones de los Habilitadores podrían incluir[94] el proveer de componentes para el acceso al Espacio de Datos, para la intermediación, para la gestión de identidad y la comunicación segura de datos o para la gestión del espacio de datos. También el proveer aplicaciones que permitan trabajar con los datos, como pueden ser modelos de aprendizaje automático, visualizadores, herramientas de limpieza o análisis de la calidad de los datos, etc., proveer vocabularios y ontologías y servicios de orquestación que permitan automatizar diversas actividades, entre otros.

El Punto Único de Información[95] definido en la DGA, en su función de puesta a disposición de una lista de activos consultable que contenga un resumen de todos los recursos de datos disponibles, actuaría como un Habilitador. También, como ejemplo, un proveedor de servicios de almacenamiento en la nube podría ser un Habilitador tecnológico que contribuya a la creación de esa infraestructura.

Un Habilitador no tendría exclusivamente carácter técnico, sino que también implementaría medidas organizativas (de gobernanza o de control, por ejemplo, de la trazabilidad o la monetización), y también de asistencia jurídica. Se considera conveniente recalcar la posición de este interviniente en el modelo del Espacio de Datos desde el punto de vista del RGPD.

En el caso de tratamiento de datos personales tiene especial significancia la posible figura del Habilitador en protección de datos que dé soporte al Titular de Datos, a los Mediadores del Espacio de Datos y al Usuario de Datos para garantizar el cumplimiento del RGPD[96]. Hay que tener en cuenta que a la hora de diseñar un tratamiento de datos personales sobre un Espacio de Datos habrá que determinar muchos aspectos que son transversales a los distintos intervinientes, que implican distintas arquitecturas posibles, diferentes herramientas tecnológicas y diferentes requisitos y garantías normativas, en particular, para la adecuada elaboración de una EIPD del tratamiento desde cada una de las perspectivas de los actores involucrados.

[94] Artículo publicado por la Oficina del Dato el 20/10/2022 sobre los principales elementos de un espacio de datos.
[95] Artículo 8 y Considerando 26 de la DGA
[96] Más adelante se trata la importancia de la figura del DPD en el Espacio de Datos.

Autoridades de Control

En materia de protección de datos, las autoridades competentes serán las indicadas en el RGPD, que en el caso de España será la AEPD, o las Autoridades Autonómicas de acuerdo con su competencia. Cuando otras autoridades actúen como autoridades competentes, por ejemplo, con arreglo a la DGA, lo deben hacer sin perjuicio de las facultades y competencias de supervisión de las autoridades responsables de la protección de datos con arreglo al RGPD[97].

El Capítulo III "Requisitos aplicables a los servicios de intermediación de datos" de la DGA se establecen los requisitos administrativos para la gestión de los servicios de intermediación de datos y su supervisión por una autoridad competente en materia de servicios de intermediación de datos con relación a los requisitos de notificación y supervisión establecidos en los Artículos 11 y 12 de la misma DGA. En principio, y como en cualquier otro sector regulado y sometido a supervisión de autoridades sectoriales, eso no implica que, en el caso de tratamientos de datos personales, suponga una falta de competencia de la Autoridad Supervisora de Protección de Datos. El Considerando 46 de la DGA manifiesta que "*cuando una cuestión requiera evaluar el cumplimiento del RGPD, la autoridad competente en materia de servicios de intermediación de datos debe solicitar un dictamen o una decisión, según proceda, a la autoridad de control competente establecida con arreglo a dicho Reglamento*", sin embargo, esto tampoco supone que la Autoridad Supervisora de Protección de Datos delegue el ejercicio de sus competencias.

En cualquier caso, desde la AEPD, se enfatiza la conveniencia de definir mecanismos de cooperación lo más eficaces posibles entre dichas autoridades sectoriales y las Autoridades Supervisoras de Protección de Datos.

B. TRATAMIENTOS Y FINALIDADES EN EL MARCO DE UN ESPACIO DE DATOS

Un tratamiento es cualquier operación o conjunto de operaciones[98] realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no[99]. El aspecto más importante que define a un tratamiento es su finalidad.

El principio de finalidad supone definir el motivo por el que se tratan determinados datos personales. Esto significa que hay que ser todo lo específico que sea posible sobre los fines para los que un tratamiento justifica la recopilación y el tratamiento de datos personales[100]. Para definir la finalidad no basta con una expresión de voluntad sobre la necesidad de los tratamientos, sobre todo cuando están basados en propósitos genéricos de beneficio social, sino que debe estar objetivamente fundamentada en que se van a conseguir dichos fines con los tratamientos planteados, es decir, el análisis de idoneidad de la implementación concreta del tratamiento.

[97] Considerando 4 y artículo 1.3 de la DGA

[98] Artículo 4.2 del RGPD "…recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

[99] Artículo 4.2 del RGPD

[100] Párrafo 5.7 del documento "WP 211 Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas (Grupo de Trabajo del Artículo 29) [27 de febrero de 2014]".

La finalidad es lo que diferencia una operación aislada del conjunto de operaciones que forman un tratamiento. Una operación en un tratamiento estará justificada en la medida que contribuye con otras operaciones a conseguir la finalidad del tratamiento. Una tecnología (p.ej. inteligencia artificial, biometría, uso de la nube, etc.) es un medio para implementar una o más operaciones en el tratamiento. La finalidad última es sobre la que se estudiará la legitimidad del tratamiento.

Por otro lado, en el marco del Espacio de Datos se define el ciclo de vida del dato como el conjunto de distintas operaciones que se podrían ejecutar sobre los datos desde su gestación hasta su eliminación, que sin ánimo de presentar una lista exhaustiva, podemos enumerar las siguientes:

- Recogida de datos.
- Extracción[101] de datos de los conjuntos de datos para la creación de nuevos conjuntos.
- Transformaciones de los datos con relación a la naturaleza del conjunto de datos como relativos a una persona identificada o identificable (anonimización o seudonimización).
- Acceso sin difusión de datos.
- Comunicación por transmisión o difusión.
- Registro y conservación de datos personales.
- Transformaciones sintácticas o semánticas del conjunto de datos mediante organización, estructuración, adaptación o modificación.
- Análisis de los datos para su catalogación y generación de metadatos.
- Anonimización y seudonimización de datos.
- Generación de datos sintéticos.
- Análisis de riesgos de reidentificación, de calidad de los datos resultantes, etc.
- Utilización o explotación de los datos.
- Establecimiento de limitaciones sobre los datos.
- Supresión o destrucción.
- Otras posibles operaciones.

Cada operación descrita anteriormente del dato no supone necesariamente un tratamiento. El conjunto de todas las posibles operaciones sobre un dato durante todo su ciclo de vida no será, generalmente, un único tratamiento. El ciclo de vida del dato puede involucrar distintos tratamientos y distintos responsables para cada tratamiento, lo que es el objeto de la infraestructura que supone un Espacio de Datos.

Independientemente de su legitimación, un tratamiento podría tener la finalidad de crear repositorios comunes de datos anónimos procedentes de datos personales de distintas fuentes. Este tratamiento podría implicar operaciones de extracción,

[101] La extracción se puede realizar una separación física entre un conjunto de datos y su copia, para realizar un tratamiento sin que afecte a los datos originales o por seguridad, o porque se genera un subconjunto de los datos originales reduciendo la extensión de campos, registros, extensión temporal de los datos registrados.

transformación de datos para anonimización, carga y almacenamiento bajo el control responsable que presta el servicio repositorio común.

Otro posible tratamiento resultaría del análisis por parte de un tercero de conjuntos de datos personales en manos de múltiples intervinientes con la finalidad de crear un catálogo de contenidos y localización de fuentes de datos[102].

También serían tratamientos el acceso por un Usuario de Datos a través de la infraestructura del Espacio de Datos a información de diversas fuentes de datos personales para la elaboración de una investigación de mercado o cualquier finalidad última que legítimamente defina un Usuario de Datos. El conjunto de operaciones implicadas e intervinientes podría variar mucho en función de las capacidades del Espacio de Datos.

En resumen, en un Espacio de Datos se pueden plantear distintos tratamientos, en los que podrían intervenir uno o varios responsables en función de cómo se implemente para cada caso de uso la arquitectura del Espacio de Datos y las garantías de privacidad desde el diseño.

C. LEGITIMACIÓN DE LOS TRATAMIENTOS

El tratamiento de datos personales en el marco de un Espacio de Datos carece de una legitimación per-sé, como establece la DGA[103], y necesita de una legitimación concreta basada en el artículo 6 del RGPD. Para la reutilización de datos que obren en poder de organismos del sector público, el Derecho de la Unión o de los Estados miembros debe prever un fundamento jurídico adecuado en virtud del RGPD, y los organismos del sector público definirlo de manera concienzuda[104].

La legitimación del tratamiento de datos personales en el marco de un Espacio de Datos puede basarse en cualquiera de las bases jurídicas del Artículo 6 del RGPD, incluyendo el cumplimiento de obligaciones legales[105] [106] [107], o el interés legítimo cuando no se trate de tratamientos realizados por las Administraciones Públicas en el ejercicio de sus funciones. La cuestión es que la legitimación esté clara y correctamente definida en el tratamiento.

Estrechamente vinculado a la legitimidad del tratamiento, está el principio de limitación de fines. Los límites de lo que constituye un tratamiento lícito y un tratamiento

[102] Podría ser el caso de el punto de información único debe contar con una lista de activos que contenga un resumen de todos los recursos de datos disponibles y que incluya, en su caso, aquellos recursos de datos que estén disponibles en los puntos de información sectoriales, regionales o locales, junto con información relevante que describa los datos disponibles. (Considerando 26 de la DGA) Este tratamiento se podría pretender implementarlo de forma activa por el punto de información único explorando los conjuntos de datos, o de forma pasiva solo recibiendo descripciones en cuyo caso no estaríamos en el marco de este ejemplo.

[103] Artículo 1.3 y considerando 4 de la DGA.

[104] Párrafo 83 del documento "Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]".

[105] Como podría ser el de anonimización para compartir datos de alto valor o HVDs, ver Considerando 8 del Reglamento de Ejecución (UE) 2023/138.

[106] En el caso de la propuesta de EHDS, en su Considerando 37 se manifiesta "En concreto, para el tratamiento de datos sanitarios electrónicos en poder del titular de los datos con arreglo al presente Reglamento, este crea la obligación jurídica, en el sentido del artículo 6, apartado 1, letra c), del Reglamento (UE) 2016/679, de que el titular de los datos revele dichos datos a los organismos de acceso a los datos sanitarios … El presente Reglamento también cumple las condiciones para dicho tratamiento de conformidad con el artículo 9, apartado 2, letras h), i) y j), del Reglamento (UE) 2016/679".

[107] También en la propuesta de EHDS se platea en el Artículo 33 "Categorías mínimas de datos electrónicos para uso secundario" la obligación de los titulares de datos de poner a disposición determinadas categorías de datos electrónicos para uso secundario.

posterior compatible de los datos deben ser muy claros para todas las partes interesadas. En el caso de un tratamiento compatible, el tratamiento en el contexto del Espacio de Datos debe cumplir los requisitos del artículo 5, apartado 1, letra b) del RGPD (limitación de la finalidad) y del artículo 6, apartado 4, del RGPD (prueba de compatibilidad). En caso de que vaya a realizarse un tratamiento ulterior, el responsable deberá asegurarse primero de que dicho tratamiento sea compatible con los fines originales y diseñarlo en consecuencia. La compatibilidad o incompatibilidad de un nuevo fin se evaluará con arreglo a los criterios establecidos en el artículo 6, apartado 4[108].

Además, en el caso de que los fines sean de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, debe estar de acuerdo con lo establecido en el artículo 89, apartado 1, del RGPD (salvaguardias y excepciones relativas al tratamiento con fines científicos), leído a la luz del artículo 50 del RGPD. La Opinión 3/2013 del Grupo de Trabajo del Artículo 29 proporciona una guía útil sobre la implementación del principio de limitación de la finalidad, así como sobre el uso apropiado de las diversas bases legales para el procesamiento de datos personales y sigue siendo relevante en gran medida también bajo el RGPD[109].

Cuando la legitimidad del tratamiento se haya basado en el consentimiento, si se considera que el tratamiento ulterior sobre la base de una prueba de compatibilidad con arreglo al artículo 6, apartado 4, del RGPD es posible, se eludiría el principio mismo de los requisitos de consentimiento[110]. Por lo tanto, en el caso de que el tratamiento se haya basado en el consentimiento, solo podrán seguir tratándose si el responsable del tratamiento solicita un consentimiento específico para ese otro fin distinto o si el responsable del tratamiento puede demostrar que se basa en una ley de la Unión o de un Estado miembro para salvaguardar los objetivos mencionados en el artículo 23 del RGPD.

El artículo 5.1.b del RGPD establece que el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. Esto no significa que dichos fines se consideren siempre compatibles, sino que el punto de partida del análisis es la posibilidad de compatibilidad. "*Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista*"[111]. Los responsables del tratamiento deben tener cuidado de

[108] Párrafo 71 del documento "Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (EDPB) [20 de octubre de 2020]".
[109] Párrafo 18 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*.
[110] Párrafo 53 documento "Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad (EDPB) [9 de marzo de 2021]"
[111] Considerando 50 del RGPD

no ampliar los límites de los «fines compatibles» del artículo 6, apartado 4, y tener presente qué tratamiento se corresponderá con las expectativas razonables de los Sujetos de los Datos[112].

La existencia de una legitimación no excusa que se haya de cumplir con todas los principios, derechos y obligaciones establecidas en el RGPD. En particular, el modelo de cumplimiento basado en la responsabilidad proactiva establecido en el RGPD exige algo más que la elección de una base jurídica para el tratamiento en base a las categorías del artículo 6:

- Por un lado, en caso de tratamiento de categorías especiales de datos, es necesario demostrar que se cumplen las condiciones de levantamiento de la prohibición de dicho tratamiento que se establecen en el artículo 9.2 del RGPD y lo establecido en el artículo 9 de la LOPDGDD[113].
- El artículo 8 de la LOPDGGD establece que el tratamiento de datos personales por obligación legal (artículo 6.1.c RGPD), interés público o ejercicio de poderes públicos (artículo 6.1.e RGPD), así como las especialidades de los tratamientos sometidos a la Ley Orgánica 7/2021, solo se podrá considerar fundado cuando así lo prevea o se derive de una competencia atribuida por una norma de Derecho de la Unión Europea o una norma con rango de ley y se establezcan las garantías adecuadas.
- El levantamiento de la prohibición[114] de tratar categorías especiales de datos contemplado en las letras g) (interés público esencial), h) (fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social) e i) (interés público en el ámbito de la salud pública) del artículo 9.2 del RGPD deberán estar amparados en una norma con rango de ley y se establezcan las garantías adecuadas.
- El RGPD exige la evaluación explícita de la necesidad, que implica también el análisis de la idoneidad, del tratamiento en aquellos legitimados en el artículo 6.1.b al f, y en el levantamiento de las prohibiciones basadas en el artículo 9.2.b, c, f y g.
- El RGPD exige una evaluación de la proporcionalidad del tratamiento en aquellos legitimados por una obligación legal (artículo 6.1.c RGPD), interés público o ejercicio de poderes públicos (artículo 6.1.e RGPD), para el levantamiento de las prohibiciones de tratar categorías especiales de datos por

[112] Párrafo 51 de las "Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (EDPB) [20 de octubre de 2020]"

[113] La propuesta de EHDS, en el Considerando 37 manifiesta "El presente Reglamento proporciona la base jurídica, de conformidad con el artículo 9, apartado 2, letras g), h), i) y j), del Reglamento (UE) 2016/679, para el uso secundario de los datos sanitarios, estableciendo las garantías para el tratamiento en cuanto a la licitud de los fines, la fiabilidad de la gobernanza para facilitar el acceso a los datos sanitarios (a través de los organismos de acceso a los datos sanitarios) y la seguridad del entorno de tratamiento, así como modalidades para el tratamiento de datos, establecidas en el permiso de datos."

[114] El levantamiento de la prohibición no implica la existencia de una base legitimadora, sino que será necesario abordar el análisis que exige el artículo 6 y, en su caso el 7, para determinar la base legitimadora.

los artículos 9.2.g (interés público esencial) y 9.2.j (fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos).

- Para cualquier tratamiento de alto riesgo, es necesario realizar una EIPD para gestionar dicho riesgo y superar la evaluación de idoneidad, necesidad y proporcionalidad estricta.
- En caso de que el tratamiento suponga decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, será necesario cumplir las condiciones que habilitan el tratamiento de acuerdo el artículo 22 del RGPD.

Con relación con la anonimización, hay que señalar que es un tratamiento de datos personales, y como todo tratamiento, debe cumplir con los mismos requisitos señalados anteriormente[115].

Finalmente, existen otras limitaciones al tratamiento de datos personales que no surgen del RGPD. Por ejemplo, un Servicio de Intermediación de Datos, para ser considerado como tal de acuerdo a la DGA[116], no podrá utilizar los datos en relación con los que presten sus servicios para fines diferentes de su puesta a disposición de los Usuarios de Datos y prestarán los servicios de intermediación a través de una persona jurídica que sea independiente de las demás actividades del proveedor de dichos servicios. Dichos servicios tampoco podrán realizar conversiones de formato de los datos personales[117] a menos que se cumplan una serie de condiciones y se ofrezca a los Sujetos de los Datos una posibilidad de exclusión[118]. La DGA limita también las posibilidades de tratamiento de datos por parte de las organizaciones de gestión de datos cedidos con fines altruistas que, voluntariamente, hayan decidido solicitar la inscripción en el registro nacional correspondiente, en el sentido de que no podrá utilizar los datos para objetivos distintos de los de interés general para los que el Sujeto de los Datos o el Titular de Datos permita el tratamiento.[119]

D. DETERMINACIÓN DE LA RESPONSABILIDAD DE LOS TRATAMIENTOS

Desde la perspectiva de protección de datos, la parte más importante de la estructura de gobernanza de un Espacio de Datos es el establecimiento con claridad de los roles de responsables y encargados/subencargados cuando se traten datos personales[120], y que debe estar definida desde el diseño. Además, estos roles han de ser establecidos de acuerdo con la normativa y a las directrices establecidas por las autoridades de control[121].

[115] WP 216 Dictamen 05/2014 sobre técnicas de anonimización (Grupo de Trabajo del Artículo 29) [10 de abril de 2014]
[116] Artículo 12.a) y Considerando 33 de la DGA
[117] La conversión del formato de los datos personales también es o puede formar parte de un tratamiento
[118] Artículo 12.d de la DGA
[119] Artículo 21.2 de la DGA
[120] Párrafo 39 del documento "Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]".
[121] WP 169 Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (Grupo de Trabajo del Artículo 29) [16 de febrero de 2010]

La condición de responsable o encargado se atribuirá a una entidad con relación a un tratamiento, en función de la toma de decisiones sobre los fines y los medios, de forma que una misma entidad podrá ser responsable para unos tratamientos y encargada para otros. Una entidad será encargada en un tratamiento cuando esté tratando los datos por cuenta de un responsable. Si está realizando el tratamiento sin que exista un responsable, o no haya sido elegido por el responsable de acuerdo con el artículo 28.1 del RGPD, o no haya contrato o un acto jurídico que lo vincule con el responsable, infringe el RGPD al fijar fines y medios[122], o quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los sujetos de los datos[123], o quien figurando como encargado utilizase los datos para sus propias finalidades[124] entonces será responsable del tratamiento.

Para un tratamiento podrá haber más de un responsable, y no hay que confundir la comunicación de datos entre dos responsables con la existencia de una relación responsable-encargado o una corresponsabilidad.

Cuando se tenga la condición de responsable, tendrá la obligación de garantizar y poder demostrar el cumplimiento de la normativa de protección de datos. Cuando tenga la condición de encargado/subencargado, tendrá que cumplir las obligaciones que para el encargado se establecen en la normativa de protección de datos, en particular, en el artículo 28.3 del RGPD. Por ejemplo, el responsable será el que tenga la obligación de garantizar que el interesado obtendrá el ejercicio de sus derechos, pero no el encargado, aunque este tenga la obligación de asistir al responsable de acuerdo con la naturaleza del tratamiento.

Cuando los roles se asignen normativamente, esta asignación también debería realizarse respetando lo establecido en el RGPD, en particular, que el responsable pueda ejercer sobre el encargado las obligaciones establecidas en el artículo 28 del RGPD, como el deber de diligencia del artículo 28.1, de control sobre los subencargados del artículo 28.2, y las estipulaciones el artículo 28.3[125]. En caso de que esto no sea posible, se recomienda conformar la relación como comunicaciones de datos entre responsables.

A continuación, se realizará un análisis de las responsabilidades sobre tratamientos en el Espacio de Datos sin perjuicio de la normativa especial aplicable y de la base jurídica para el tratamiento.

Titular de Datos

Cuando haya tratamiento de datos personales, aquellos que tengan la consideración de responsables de tratamiento podrán tener la consideración de Titular de Datos. Los encargados solo podrán actuar como Titulares de Datos cuando así se lo haya encomendado específicamente el responsable[126]. En este caso, el encargado se ha de

[122] Artículo 28.10 del RGPD.
[123] Artículo 33.2 de la LOPDGDD que no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.
[124] Artículo 33.2 párrafo segundo de la LOPDGDD.
[125] A este respecto, es destacable que en el artículo 12.7del borrador actual del EHDS, la Comisión se otorga el rol de encargado.
[126] En este sentido se expresa la Propuesta de DA en el considerando 21 "*Data processors as defined in Regulation (EU) 2016/679 are by default not considered to act as data holders, unless specifically tasked by the data controller*."

limitar al cumplimiento de las instrucciones documentadas por el responsable con relación al tratamiento de datos personales que se encuentre en el contrato o acto jurídico que les vinculan[127].

Los tratamientos ejecutados por los Titulares de los Datos en el marco del Espacio de Datos, ya sea para sus propios fines como, por ejemplo, pueden ser fines altruistas, para participar en alguna iniciativa, o por obligación legal serían considerados responsables de tratamiento.

Cabe destacar que no nos encontraremos en un supuesto de aplicación del RGPD si la información sobre los Interesados o Sujetos de los Datos que se comunica al Espacio de Datos son datos no personales. Sin embargo, si se han tenido que utilizar mecanismos para tratar datos personales, p.ej. para generar conjuntos de datos anonimizados, este hecho en sí constituye un tratamiento de datos personales de cara al Titular de Datos.

Además, los datos bajo la responsabilidad del Titular de Datos es probable que estén almacenados de forma que requiera la transformación de los datos tanto en su formato, contenido, metadatos e incluso formato de ficheros, y pueda ser encargada a un Medidador del Espacio de datos[128]. La transformación de los datos también supone una operación de tratamiento.

Mediador del Espacio de Datos

Los Mediadores del Espacio de Datos, cuando no actúen por cuenta de un responsable, sino que, definiendo fines y medios, realicen el tratamiento de datos personales, por ejemplo, para su almacenamiento, su transformación en información anónima, la generación de catálogos de datos que traten datos personales, proporcionar servicios de identidad a personas físicas, cedan datos responsables fuera del marco de una relación responsable-encargado u otros, serán responsables del tratamiento.

Los Mediadores podrán ser encargados en el marco de un tratamiento cuando actúen por cuenta de un responsable, por ejemplo, cuando un Usuario de Datos establezca con el Mediador un contrato, u otro acto jurídico, para tratar datos personales de los que sean responsables dichas entidades.

En el caso de reutilización de datos de organismos del sector público, en la DGA se expresa los Organismos Competentes deben actuar de conformidad con las instrucciones recibidas del organismo del sector público, de forma que el tratamiento que pueda realizar debe efectuarse bajo la responsabilidad del organismo del sector público a cargo del registro que contenga los datos, que sigue siendo el responsable del tratamiento según la definición del RGPD en la medida en que afecte a datos personales[129].

Usuario de Datos

En la medida que el Usuario de Datos defina los fines del tratamiento y los medios (que en este caso será utilizar infraestructura del Espacio de Datos) para el tratamiento de datos

[127] Artículo 28.3.a del RGPD
[128] Corresponde con el artículo 12.d) de la DGA en los casos en que se traten datos privados en una cesión no altruista.
[129] Considerando 26 de la DGA

personales, el Usuario de Datos será responsable de dicho tratamiento y por tanto deberá cumplir con todas las obligaciones que se derivan de la normativa de protección de datos.

En cuanto el Usuario de Datos determine implementar todo o parte del tratamiento a través del Espacio de Datos, las medidas adoptadas para garantizar el cumplimiento del RGPD deberán estar coordinadas, en su caso, con otros intervinientes como los Mediadores del Espacio Datos, los Titulares de los Datos o los Habilitadores.

Habilitadores

En el caso de que no traten datos personales, puede que no tengan un rol en el marco del RGPD.

Cuando traten datos personales para sus propios fines serán responsables del tratamiento. Serán encargados del tratamiento (o subencargados) cuando traten datos personales en nombre de responsables u otros encargados cumpliendo con los requisitos del artículo 28 del RGPD.

V. PRIVACIDAD DESDE EL DISEÑO EN UN ESPACIO DE DATOS

La implementación de los principios, derechos y obligaciones del RGPD exige a los responsables han de adoptar las medidas que sean adecuadas para conseguirlo[130]. Estas medidas podrían ser herramientas jurídicas, organizativas y también técnicas. Con relación a estas últimas, y respecto a la libre circulación de datos personales, el RGPD expone en sus considerandos iniciales que la tecnología ha de facilitar soluciones que implementen un elevado nivel de protección de los datos personales[131]. En cualquier caso, la adecuación de las medidas se establecerá según el contexto, la naturaleza, el ámbito, los fines y riesgos para los derechos de los Sujetos de los Datos que impliquen los tratamientos.

Los principios de minimización y protección de datos desde el diseño y por defecto son esenciales cuando el tratamiento implica riesgos significativos para los derechos fundamentales de las personas. Teniendo en cuenta los últimos avances técnicos, todas las partes involucradas en el intercambio de datos deben aplicar medidas técnicas y organizativas para proteger estos derechos. Dichas medidas incluyen no solo la anonimización, la seudonimización y el cifrado. Estas técnicas ni son las únicas, ni en muchas ocasiones pueden resultar las más adecuadas. Existen otras tecnologías cada vez más utilizadas que permiten introducir algoritmos en los datos y obtener información valiosa sin que sea necesaria la transmisión entre las partes ni la copia superflua de los datos brutos o estructurados[132]. Ejemplos de estas técnicas son la privacidad diferencial, la generalización, la supresión y la aleatorización[133], el uso de datos sintéticos, el aprendizaje federado, los Entornos de Tratamiento Seguro y otras herramientas y tecnologías para mejora de la protección de la privacidad (PET[134]). Los Estados miembros deben prestar apoyo a los organismos del sector público con el fin de hacer un uso óptimo de dichas técnicas y, de este modo, facilitar el mayor número posible de datos para su intercambio[135].

En la introducción hemos puesto de relieve que los Espacios de Datos, como infraestructura técnica y de gobernanza, se han de caracterizar por permitir que se adopten las medidas antes enumeradas, entre otras, para así implementar las necesarias garantías de protección de datos que permitan libre circulación de datos personales en la Unión.

A. POSIBLES CONFIGURACIONES DE UN ESPACIO DE DATOS

Un Espacio de Datos podrá tener distintas configuraciones[136]. En este apartado se despliegan un conjunto de ejemplos de configuraciones de un Espacio de Datos, sin ánimo de exhaustividad. Estas configuraciones podrían combinarse entre sí y, además, con el propósito de ser didácticos, se identifican Titulares y Usuarios de Datos como entidades

[130] Artículo 24 del RGPD
[131] Considerando 6 del RGPD
[132] Considerando 8 de la propuesta de DA
[133] Considerando 7 de la DGA
[134] *Privacy Enhancing Technologies*
[135] Considerando 7 de la DGA
[136] Escenarios de compartición de datos. Francisco Javier Esteve Pradera, junio 2022 – Boletic nº 91

distintas, aunque como se ha señalado en el apartado IV.A, se podrían compartir ambos roles.

Por un lado, un Espacio de Datos podría configurarse de forma que una sola entidad establezca todas las funciones de mediación y supervisión del Espacio de Datos, con el posible recurso a encargados/subencargados del tratamiento. Este Mediador podría centralizar todas las operaciones de acceso a los metadas, sus datos y los recursos para la explotación de los mismos entre Titulares y Usuarios:

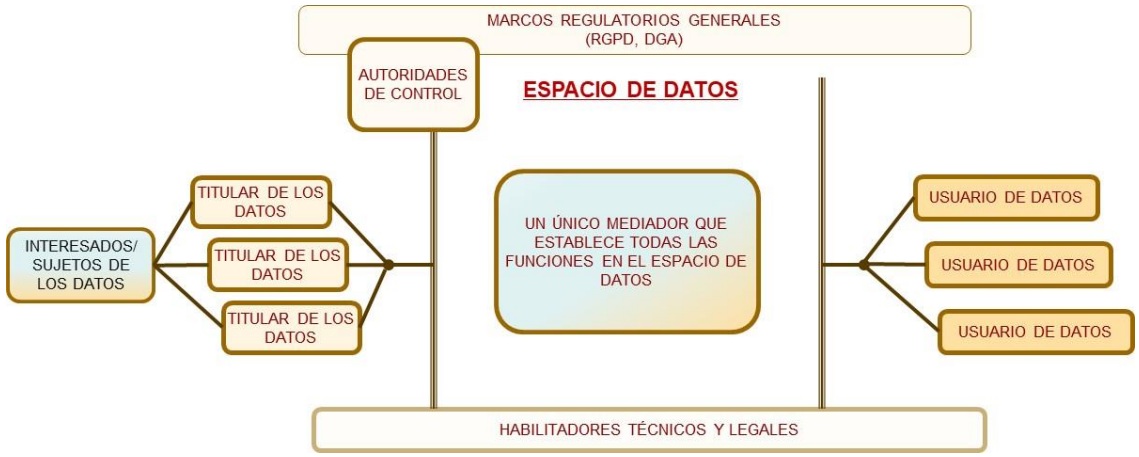

Figura 3: Configuración de un Espacio de Datos basado en el intercambio mediante un nodo central

En un Espacio de Datos dicho Mediador central podría limitarse a gestionar los participantes, el catálogo de datos y los mecanismos de seguridad, entre otros servicios, mientras que Titulares y Usuarios pueden hacer acceso a datos *peer-to-peer*:

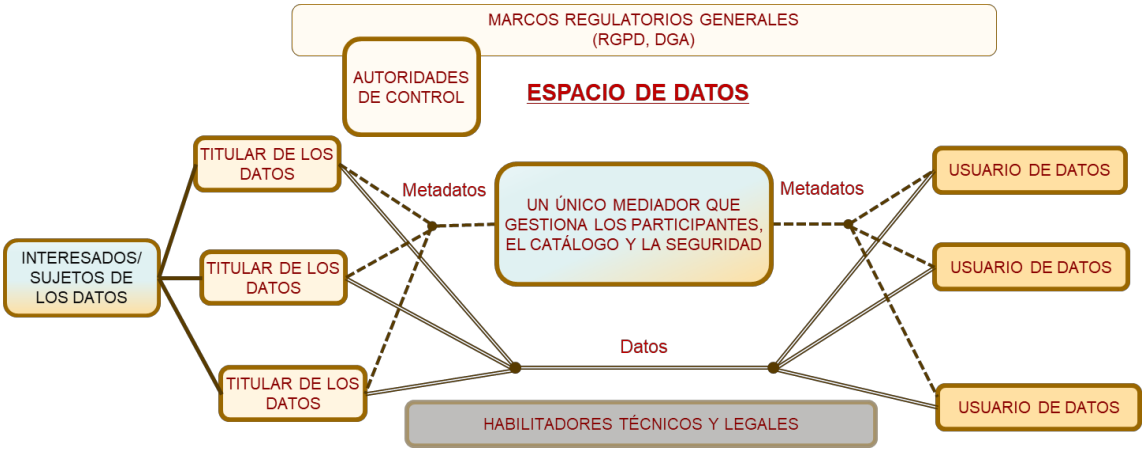

Figura 4: Configuración en base a un Mediador que actúa como hub central o data marketplace

Un Espacio de Datos podría tener una configuración más compleja, en la que intervengan múltiples entidades que establecerán las distintas funciones, algunas de ellas de forma repetida, implementado diferentes ofertas de un mismo servicio:

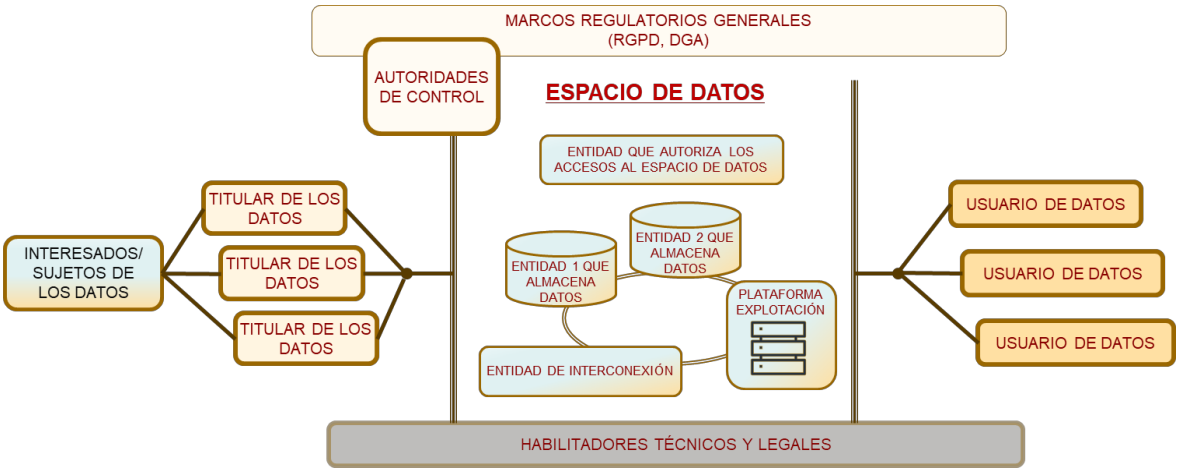

Figura 5: Configuración compleja en la definición de intervinientes en un Espacio de Datos

Por otro lado, el Espacio de Datos se podría establecer para dar soporte a la interacción directa entre los Sujetos de los Datos y los Usuarios de los Datos[137], como podrían ser las organizaciones de gestión de datos con fines altruistas[138]:

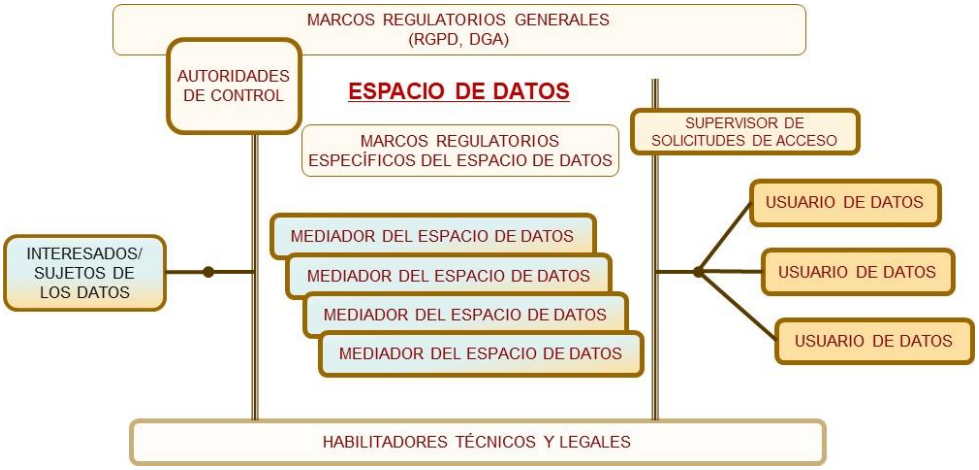

Figura 6: Configuración compleja en la definición de intervinientes en un Espacio de Datos

También, podría configurarse el Espacio de Datos para permitir el acceso a los datos de los Titulares de Datos por el o los Usuarios de los Datos, sin hacer uso de Mediadores.

[137] Artículo 10.b) de la DGA
[138] Capítulo IV de la DGA

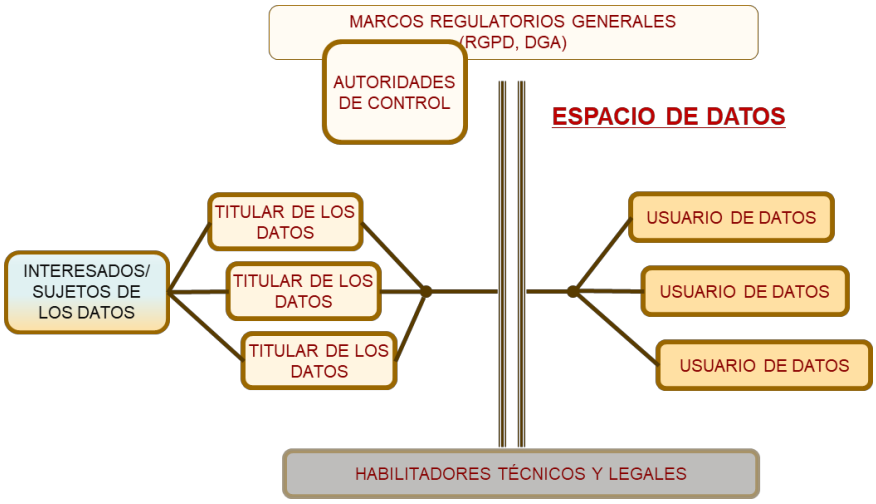

Figura 7: Configuración del Espacio de Datos sin el uso de servicios de intermediación

Finalmente, un Espacio de Datos podría también establecerse como una infraestructura para facilitar acuerdos de acceso a datos entre Sujetos y Titulares de Datos como la que sigue:

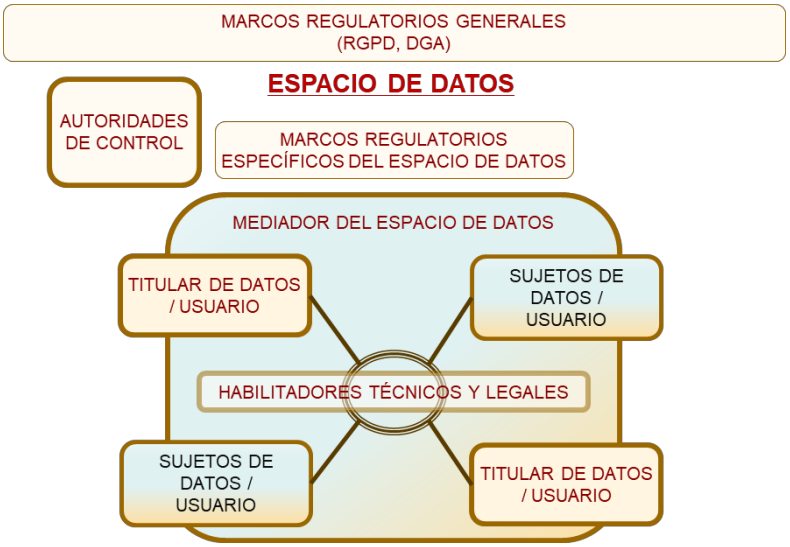

Figura 8: Configuración de un Espacio de Datos con acuerdos de acceso a datos entre Sujetos y Titulares de Datos

Si la aproximación anterior no se limita a un grupo cerrado de intervinientes, sino a un grupo abierto podría entrar dentro de la definición jurídica de “cooperativas de datos” [139].

Finalmente, estaría la participación de cualquiera de las opciones anteriores en federaciones de Espacios de Espacios de Datos. En la federación, un Titular/Usuario podría consultar los catálogos de su Espacio de Datos, así como del resto de Espacios conectados que sean interoperables, y acceder u ofrecer recursos a todo el resto de los intervinientes:

[139] Considerando 31 de la DGA

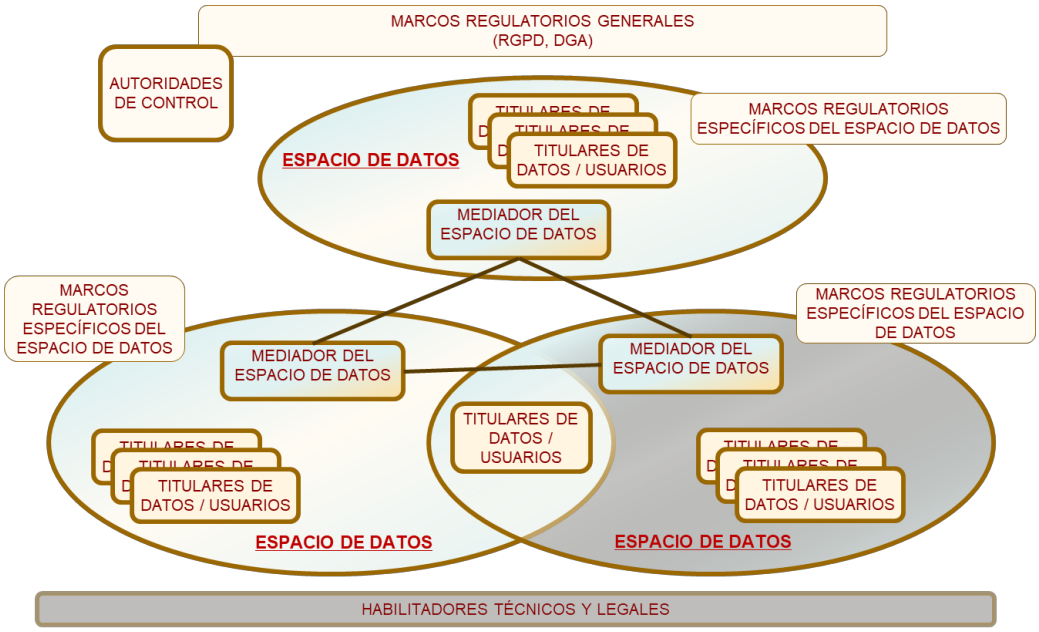

Figura 9: Federación de Espacios de Datos

En los siguientes apartados analizaremos una serie de aspectos a tener en cuenta para poder llegar al subapartado "V.E Casos de uso" donde incluiremos un análisis de arquitecturas y consideraciones en protección de datos.

B. ACCESO A DATOS E INFORMACIÓN

En la DGA se define "acceso" como toda utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.[140] Es decir, en el marco de los Espacios de Datos se hace la distinción entre dos conceptos que pueden parecer similares pero que son muy distintos:

- Acceso a los datos mediante la transmisión o la descarga.
- Acceso a la información generada por el tratamiento de los datos mediante un acceso que no implique ni transmisión o descarga de los datos. Información es aquello que incrementa el conocimiento en un contexto determinado y es necesario y relevante para cumplir los objetivos del Usuario de Datos.

Los datos pueden no contener la información necesaria para un contexto determinado y, en cualquier caso, será necesario un tratamiento previo de los datos para obtener la información requerida. Un Espacio de Datos ha de permitir al Usuario de Datos conseguir la información necesaria para cada uno de los tratamientos, y eso no implica necesariamente la comunicación o difusión de datos personales. Por lo tanto, un Espacio de Datos podría (y desde el punto de vista de protección de datos es lo más recomendable) conceder acceso a los datos personales, pero sin difundirlos, es decir, no necesariamente comunicación a terceros de los datos. De hecho, una arquitectura de Espacio de Datos, que se construya aplicando los principios de protección de datos desde el diseño,

[140] Artículo 2.13) de la DGA

minimizará la exposición de datos personales (principio de minimización) y preservará la capacidad de disponer de la información necesaria para cumplir las finalidades de los Espacios de Datos.

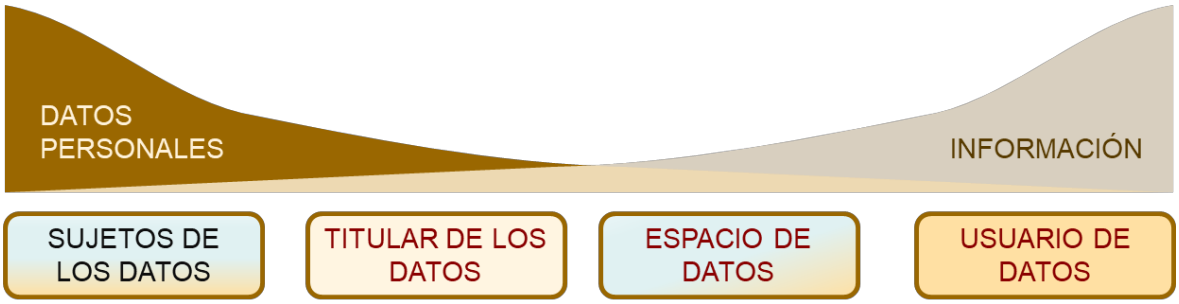

Figura 10: Evolución del tratamiento de datos en un Espacio de Datos

La infraestructura de un Espacio de Datos debe dar acceso a los datos entendido como la posibilidad de realizar una explotación de los mismos para obtener valor (información) sin que eso implique necesariamente la comunicación de datos, en este caso personales, entre intervinientes.

Los Espacios de Datos que permitan disponer de la información, pero sin comunicación o difusión de los datos personales, p.ej. dejando el control real de los datos y de las finalidades en manos de los Titulares de los Datos aumentarán la confianza[141] de dichos Titulares para participar en el Espacio de Datos y, además, la predisposición de los Titulares a implicarse en el desarrollo de la economía digital.

Como nota adicional, el desarrollo europeo de sistemas, soluciones y mantenimiento de los servicios que implementan protección de datos desde el diseño es impulso de la economía digital, que son los fines generales que justifican la creación de un Espacio de Datos. Además, si la falta de confianza entre los intervinientes no permite que los tratamientos planteados en el marco del Espacio de Datos cumplan con las finalidades declaradas, dichos tratamientos no cumplirían con criterios de idoneidad y necesidad.

La aproximación al acceso a datos planteada en este apartado puede ser en algunos casos deseable, y en otros obligada, bien por el resultado de la gestión del riesgo para los derechos y libertades, o bien porque así lo exija la norma. Por ejemplo, en la propuesta EHDS cada uno de los mediadores tendrá que establecer un servicio para evitar[142] que el Usuario de Datos realice una copia local o se comuniquen los datos personales fuera de un Entorno de Tratamiento Seguro habilitado en el mismo, salvo que se encuentre fundamentado con una base jurídica y sea valorada y autorizada por parte del Órgano Supervisor de las solitudes en base a una gestión de riesgos.

[141] Hay que tener en cuenta la reticencia de las entidades a compartir información que puede dañar sus intereses comerciales o desvelar su estrategia de negocio, aparte de otra regulación para la protección de propiedad intelectual e industrial.
[142] En línea con lo establecido en el artículo 5 y considerando 15 de la DGA para datos en poder de organismos del sector público y en el artículo 50 y el considerando 54 del EHDS.

C. TIPOS DE CONJUNTOS DE DATOS

Por otro lado, hay que tener en cuenta que los distintos casos de uso que se plantean a la hora de dar acceso a datos, y por tanto en un Espacio de Datos, pueden precisar tratar distintos tipos de datos:

- Estructurados (base de datos y otros) y/o no estructurados (documentos, voz, imagen, etc.).
- En tiempo real (IoT y similares en transporte, sanidad, suministros, ciudades inteligentes, etc.) o en tiempo diferido (bases de datos consolidadas que posteriormente son procesadas en *batch*).

Y en función del modo de tratamiento:

- Tratamientos automatizados.
- Tratamientos manuales. Hay que tener en cuenta que en muchos tratamientos de desarrollo y evolución de sistemas de aprendizaje automático es necesario utilizar equipos masivos de procesado manual para el etiquetado de muestras, sobre todo en el tratamiento de datos no estructurados[143].

A su vez, en función del flujo de información y conocimiento, se podrían dar dos casos:

- En sentido solo de los Titulares de los Datos a los Usuarios de los Datos.
- Además, en sentido contrario: de los Usuarios de los Datos a los Interesados o Sujetos de los Datos.

Este último caso podría ser el de la investigación clínica[144], cuando un resultado deba ser comunicado a un paciente concreto. No sería el caso cuando se pudiera hacer una realimentación generalista a un colectivo.

D. ARQUITECTURAS DE ESPACIOS DE DATOS Y CASOS DE USO

La arquitectura básica y más inmediata de un Espacio de Datos implica la recogida de datos de múltiples Titulares de los Datos, concentrar los mismos en un único punto y dar acceso a los Usuarios de los Datos a los mismos.

[143] Caso del Mechanical Turk en Amazon, o el etiquetado de voz en Sigma.
[144] Considerando 44 del EHDS.

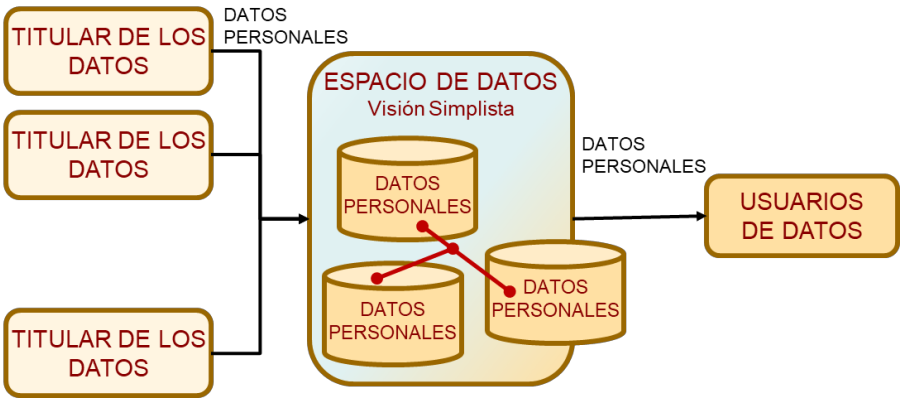

Figura 11: Esquema de arquitectura básica de un Espacio de Datos

En la medida que la implementación de tratamientos en un Espacio de Datos supone la necesidad de acceder a recursos de almacenamiento y proceso masivos, Usuarios de Datos que podrían carecer de los mismos (como pueden ser PYMEs y algunos grupos de investigadores), tendrían que hacer uso, en muchos casos, de servicios de computación en la nube.

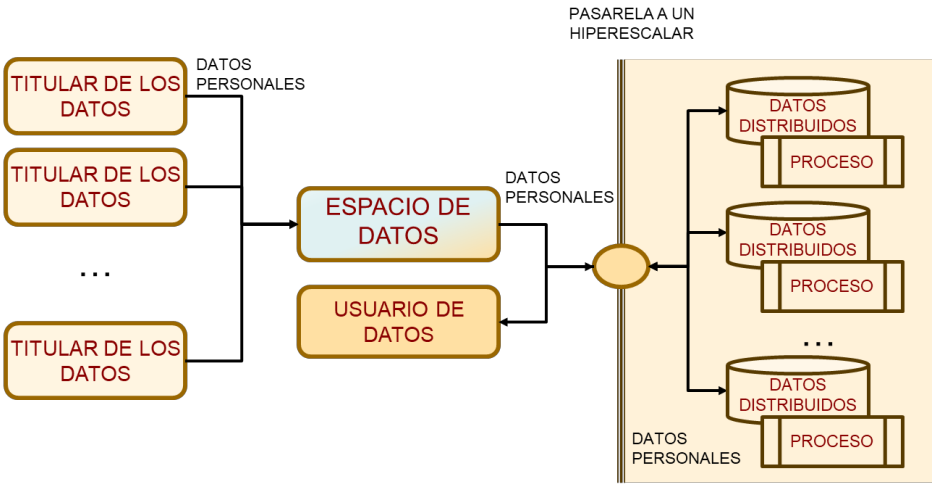

Figura 12: Esquema de arquitectura básica de un Espacio de Datos haciendo uso de un hiperescalar

Estas arquitecturas podrían implicar el desplazar a dichos Usuarios de Datos, con menos recursos, las cuestiones de cumplimiento normativo, de preservación de principios sobre los derechos y libertades y otros efectos colaterales. Esta circunstancia podría dificultar la consecución de los fines del tratamiento, como pueden ser la falta de confianza de los Interesados o Sujetos de los Datos, reticencia a compartir datos por los propios Titulares de los Datos para proteger intereses o secretos comerciales, etc.

Existen distintas aproximaciones a un Espacio de Datos que podrían resolver estas cuestiones en avance. Una de estas posibles soluciones se podría conseguir empleando las mismas tecnologías que utilizan los hiperescalares para tratamiento distribuido pero,

en este caso, para implementar técnicas de "*compute-to-data*"[145], es decir, el proceso de los datos de forma distribuida se ejecutaría en el origen de los datos. De esta manera se evitaría la comunicación de datos a terceros, el proceso se realizaría en el origen de los datos, y se reduciría la exposición de datos personales en redes de comunicaciones y la acumulación de datos en grandes repositorios.

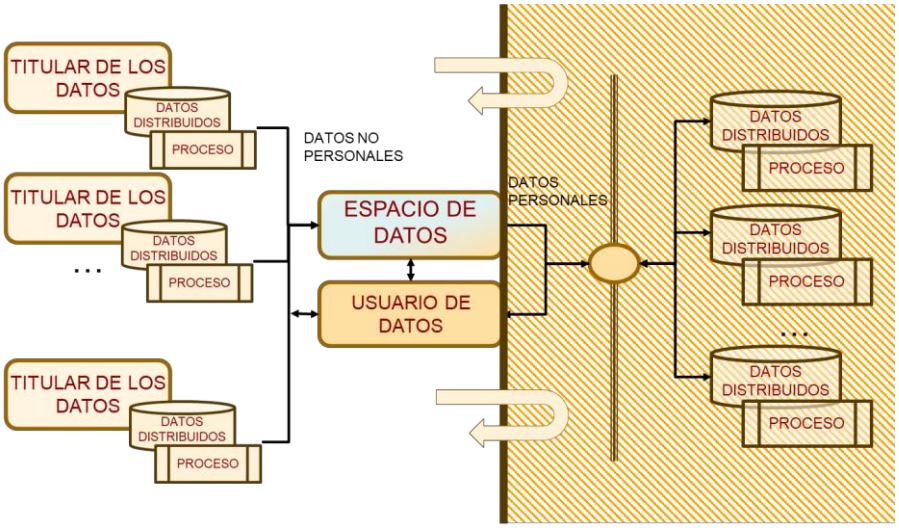

Figura 13: Esquema de arquitectura básica de un Espacio de Datos haciendo uso de la estrategia "*compute-to-data*"

Como cualquier estrategia de protección de datos desde el diseño, como la anonimización o la privacidad diferencial entre otros, esta no sería la única solución para el cumplimiento normativo y de finalidades de un Espacio de Datos en caso de tratamiento de datos personales. Tampoco la más adecuada para todos los posibles casos de uso, ni se adapta a todos los escenarios de tratamientos de datos. Siempre hay que valorar distintas estrategias en función del caso de uso específico y el diseño del Espacio de Datos ha de permitirlas. Para que esto sea posible, es necesario tener en cuenta desde el diseño de los Espacios de Datos la protección de datos.

E. CASOS DE USO Y ARQUITECTURAS PARA DAR RESPUESTA A LA PRIVACIDAD

En el marco de un Espacio de Datos se pueden plantear distintos tipos de tratamiento de datos personales, es decir, diferentes casos de uso[146] en los que se podrán adoptar estrategias específicas para implementar la protección de datos desde el diseño para los accesos entre Titulares de Datos y Mediadores de Datos:

1. El caso de uso que requiere tratar información no personal en supuestos distintos a la anonimización de datos personales.

[145] Como aparece en las definiciones, supone que el proceso se realiza en la fuente origen de los datos, en vez de que los datos se comuniquen a una "nube" donde se realice dicho proceso. Está relacionado también con las estrategias Edge-Computing, que es una de las características de 5G, y que supone acercar el proceso de los datos a los propios sistemas de los usuarios finales, con la ventaja de que se descarga la red de tráfico y por otro lado los proveedores de servicios necesitan menos servidores, pues usan la capacidad de los terminales de los usuarios.

[146] En aquellos Espacios de Datos donde no haya tratamientos de datos personales, p.ej. solo datos de entornos industriales, no aplicaría este desarrollo de casos de uso.

2. El caso de uso donde se puede ejecutar el tratamiento sin ceder datos personales por el Titular de Datos, sino tratándolos en sus propios sistemas y proporcionando información que no constituyan datos de carácter personal al Mediador de Datos (agregada, procesada u otros). Es decir, implementando estrategias "*compute-to-data*".
3. El caso de uso que se puede cumplir comunicando el Titular de Datos información anonimizada al Mediador de Datos.
4. El caso de uso que se puede cumplir comunicando el Titular de Datos información seudonimizada al Mediador de Datos.
5. El caso de uso que solo se puede cumplir realizando una comunicación de datos personales de los Titulares de los Datos a un Mediador de Datos.

Los casos anteriores describen la relación entre los Titulares de los Datos y los Mediadores de Datos. También se podrían aplicar cuando un Usuario de Datos quiera acceder a la información de múltiples Titulares de Datos[147].

Solo en los casos 4 y 5 se comunica información personal al Mediador, en el caso 4 seudonimizada y en el caso 5 sin seudonimizar. Cabría plantearse que, en estos dos últimos casos, entre el Mediador de Datos y el Usuario de Datos se podrían desplegar los siguientes subcasos:

1. El subcaso de uso donde se puede ejecutar el tratamiento sin ceder datos personales por el Mediador de Datos, sino tratándolos en sus propios sistemas y proporcionando información que no constituyan datos de carácter personal al Usuario de Datos (agregada, procesada u otros). Es decir, implementando entornos de tratamientos seguros de datos.
2. El subcaso de uso donde se puede cumplir comunicando el Mediador de Datos información anonimizada al Usuario de Datos.
3. El subcaso de uso donde se puede cumplir comunicando el Mediador de Datos información seudonimizada al Usuario de Datos.
4. El subcaso de uso donde solo se puede cumplir realizando una comunicación de datos personales de Mediador de Datos a un Usuario de Datos.

Para implementar los casos/subcasos de uso enumerados se pueden plantear distintas arquitecturas de tratamiento de datos en el Espacio de Datos. En este punto, el factor que se quiere subrayar es que el Espacio de Datos ha de estar definido desde el diseño para poder implementar aquellas arquitecturas que se planteen tengan un riesgo aceptable para los derechos y libertades de los sujetos de los datos y la sociedad de acuerdo con los distintos tratamientos concretos.

A continuación, se van a desarrollar arquitecturas que se podrían emplear para dar respuesta a los casos de uso desde el punto de vista de protección de datos. El propósito de este apartado no es hacer una relación completa y exhaustiva, ni hacer un análisis completo de las obligaciones e implicaciones que conllevan, sino que se tratará de recoger

[147] Como aclaración, y haciendo referencia a lo dispuesto en el Considerando 28 y el artículo 2 de DGA, se destaca que una solicitud directa por un Usuario de Datos a un único Titular de Datos no forma parte de lo considerado aquí como Espacio de Datos y no se contemplará como un caso de uso.

una serie de ejemplos. El ánimo de los ejemplos que se desarrollan a continuación es el de ejemplificar algunas de las posibilidades que existen para implementar el acceso, tal como se define en la DGA, minimizando la transmisión o difusión de datos personales.

Tratamientos de datos no personales

Cuando el tratamiento en el Espacio de Datos no implique ningún tratamiento de datos personales ya sea por el Titular de Datos, por los Mediadores de Datos, por el Usuario de Datos o en cualquier otro, estás orientaciones sobre la arquitectura no serían aplicables.

Existirán dos fuentes de datos no personales: los conjuntos de datos procedentes de procesos de anonimización y aquellos conjuntos de datos que son no personales en el origen, como, por ejemplo, es en principio la base de datos de geolocalización de antenas de telefonía móvil. Sin embargo, sí se requeriría diligencia en el Mediador de Datos, o en su caso en el Usuario de Datos y Titulares de Datos, para realizar una evaluación de si es posible una reidentificación de personas físicas por la acumulación masiva de datos de diversas fuentes y el uso de tecnologías novedosas.

Con relación a los datos anonimizados, se deberá tener en cuenta que, a mayor volumen de datos recibido, aumentan las posibilidades de reidentificación a pesar de ser datos no personales, especialmente cuando se reciben datos de diversas fuentes[148]. Estas fuentes incluyen datos anonimizados como datos originalmente no personales. Por ello, entre las funciones de los Mediadores del Espacio de Datos cobra especial relevancia la realización de una primera revisión de la fortaleza del tratamiento de anonimización de un conjunto de datos previamente a ponerlo a disposición del Usuario de Datos.

[148] Considerando 15 del DGA y Considerando 64 de la propuesta de EDHS

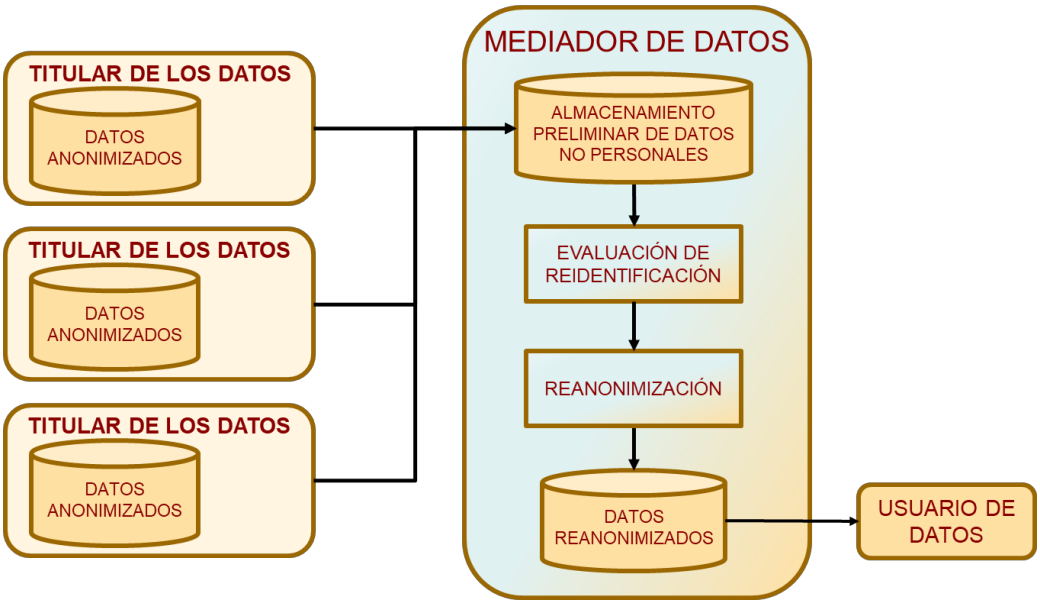

Figura 14: Esquema de la arquitectura para el caso de uso para la consolidación de datos no personales de distintos Titulares de Datos

En los casos en los que se detecte la posibilidad de reidentificación, se tendrán que volver a aplicar mecanismos de anonimización (o reanonimización) ya en el Mediador de Datos, en un entorno seguro, donde se procederá a eliminar todos los datos que permitían la reidentificación.

En el caso de conjuntos de datos no personales, el DPD del Mediador de Datos debería conocer qué conjuntos de datos se encuentran disponibles en cada momento.

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser jurídicas, organizativas y técnicas. Por ejemplo, entre las jurídicas se podría incluir en los acuerdos de comunicación de datos la obligación del Mediador de realizar un tratamiento de reanonimización.

Entre las medidas organizativas, y sobre políticas de protección de datos, se podría incluir el que la evaluación de la anonimización se realizará de forma coordinada entre los Mediadores del Espacio de Datos y, especialmente, el Supervisor de las solicitudes. Otras medidas podrían ser que el DPD esté informado de los conjuntos de datos anónimos y no personales que recojan en sus sistemas, que exista una evaluación sobre el riesgo de reidentificación cuando se sume un nuevo conjunto de datos a la entidad, que exista un proceso interno para comprobar el estado del arte y los eventos y desarrollos de reidentificación y también que exista un proceso de eliminación de los datos que son reidentificables una vez se ha extinguido su necesidad, entre otras.

Entre las medidas técnicas se podría incluir, por ejemplo, una evaluación sistemática en un entorno controlado y seguro de la anonimidad de los resultados en su conjunto almacenados en el Espacio de Datos de manera temporal y previamente a su puesta a disposición del Usuario de Datos.

Estrategias "compute to data" y aprendizaje federado

Al inicio de este capítulo V se mostró un ejemplo de lo que son las estrategias "*compute-to-data*". Estas estrategias suponen llevar el proceso de los datos a la fuente original de los datos, en este caso el Titular de Datos, para extraer la información (ya no personal) del Titular de Datos. Por ejemplo, las estrategias "*compute-to-data*" se pueden emplear para la implementación de aprendizaje federado en el entrenamiento de inteligencia artificial basada en *machine learning*.

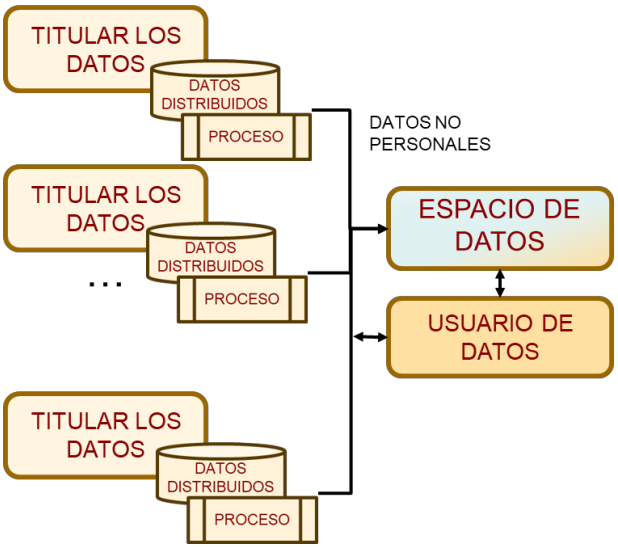

Figura 15: Esquema de la arquitectura utilizando estrategias "*compute-to-data*"

La aplicación de estas estrategias implica que el Espacio de Datos tenga definidas las obligaciones de gobernanza y gestión de la información en un entorno distribuido. En algunos casos, se tendrán que auditar o certificar los procesos que el Usuario de Datos pretende ejecutar en los locales de los Titulares de los Datos antes de ser distribuidos a estos últimos.

En estos casos, los Titulares de los Datos deberían disponer de espacios ad-hoc en sus infraestructuras, con completa separación de sus sistemas de explotación (al uso de un área DMZ[149]).

[149] DMZ hace referencia a zona desmilitarizada o zona segura no conectada con los sistemas de explotación de la entidad.

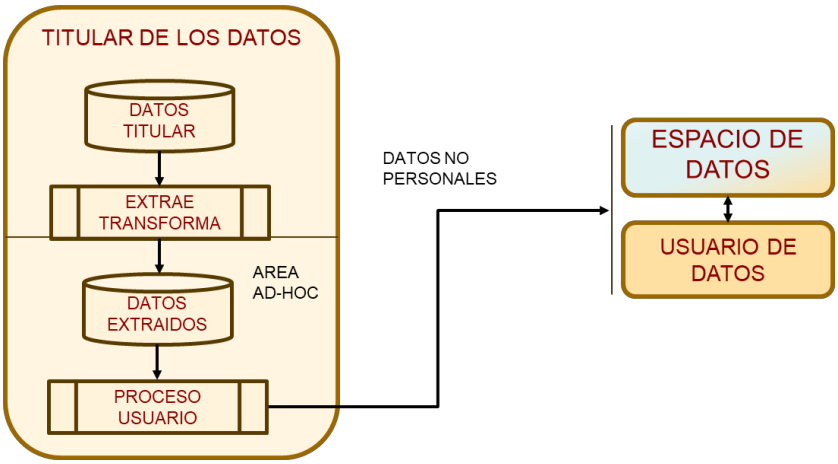

Figura 16: Esquema de espacios específicos en los Titulares de los Datos para habilitar la insfraestructura "*compute-to-data*"

Este caso de uso se podría desarrollar en múltiples casos dependiendo del tratamiento concreto del que se trate.

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser jurídicas, organizativas y técnicas. Por ejemplo, entre las jurídicas se podría incluir obligaciones de auditoría o certificación previa de los procesos de los Usuarios de los Datos.

Entre las organizativas, y sobre políticas de protección de datos, se podría incluir la supervisión humana en la descarga y ejecución de procesos en el Titular, la no ejecución de los procesos de Usuario sobre los datos y sistemas de explotación del Titular, la extracción de un conjunto de datos de trabajo que no contenga la totalidad del conjunto de datos, la evaluación de que el proceso del Usuario no genera y comunica datos personales o la evaluación de los resultados obtenidos, entre otras.

Entre las medidas técnicas se podría incluir, por ejemplo, el establecimiento de áreas ad-hoc para la ejecución de los procesos con aislamiento físico de los sistemas del Titular, áreas ad-hoc que conformen Entornos de Tratamiento Seguro, etc.

Un caso de "compute-to-data": Catalogación

La catalogación es un tratamiento que se realiza sobre datos o conjunto de datos que permite asociar a los mismos los metadatos necesarios para su explotación posterior. Los metadatos incluirán al menos descripciones sobre los tipos de datos y dónde se encuentran los datos, pero puede extenderse a evaluar la calidad de los datos, lo que implica un tratamiento profundo de los mismos, o incluso determinar si existen datos personales en dicho conjunto. De esta forma se podrían generar Catálogos de recursos (datos) que se pueden poner a disposición de múltiples intervinientes de forma virtual, intermediada o real.

La catalogación de los conjuntos de datos es la primera tarea que se ha de realizar en el marco de un Espacio de Datos. La catalogación podría realizarse de diversas formas: accediendo por parte de Mediadores y/o Usuarios a los sistemas de los Titulares, o

comunicando los datos a los Mediadores y/o Usuarios, o con un proceso en los propios Titulares, como un caso particular de "Compute-to-data".

En este último caso, la catalogación no precisa que los conjuntos de datos en poder del Titular de Datos se transfieran a terceros, sino solo es preciso comunicar los metadatos resultantes del análisis.

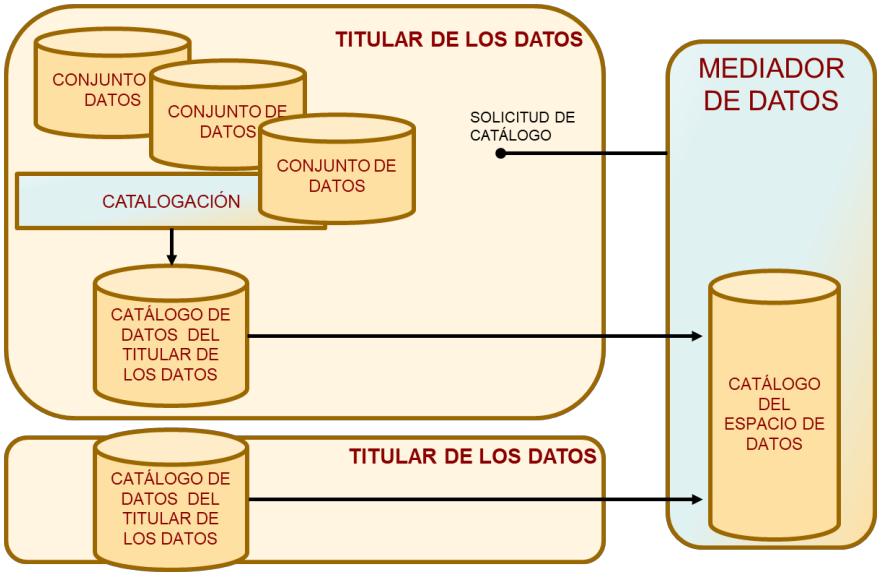

Figura 17: Esquema de la arquitectura para catalogación

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos serán del mismo orden que las estrategias "*compute-to-data*".

Los tratamientos de catalogación y generación de metadatos también pueden ser parte de la implementación de técnicas de protección de datos desde el diseño en un Espacio de Datos, como mediante el etiquetado y las jerarquías de etiquetas con el objeto ser utilizado para la gestión de privilegios de acceso.

Anonimización: Tratamientos que requieren datos agregados anónimos de los Titulares de los Datos con desvinculación de datos de distintos Titulares

En este caso, el Mediador o los Usuarios de Datos, bien por iniciativa propia o para dar respuesta a la solicitud de un Usuario, requiere de los Titulares de los Datos información anonimizada, o no personal, y de forma que la información que sea necesario extraer no tenga necesidad de vincular datos de un mismo sujeto que esté almacenada entre distintos Titulares.

Un ejemplo son los estudios de movilidad a partir de los datos de geolocalización de los operadores de telecomunicaciones, ya que normalmente se vincula un usuario a un único operador de telecomunicaciones, y el caso de usuarios cuyo perfil de movilidad dependa de la información procedente de dos operadores es residual para cumplir la finalidad del tratamiento.

En ese caso se propia diseñar la siguiente arquitectura:

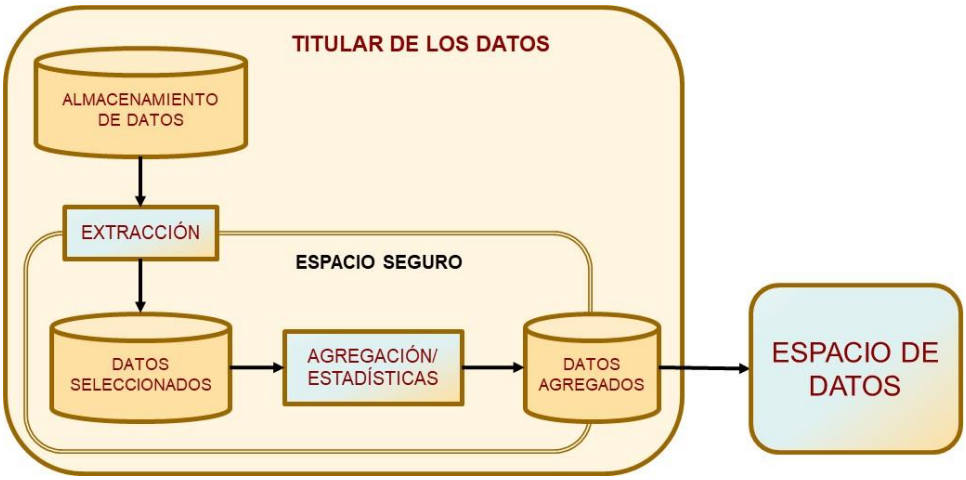

Figura 18: Esquema de la arquitectura para el caso de uso de datos anonimizados con desvinculación entre los datos de distintos Titulares de Datos

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser, por ejemplo, jurídicas como la de verificar que no es posible la reidentificación mediante un análisis de riesgo.

Entre las posibles medidas organizativas y sobre políticas de protección de datos se podría, con relación al proceso de agregación u otro tipo de análisis de datos, no realizarlo sobre el almacenamiento de datos de explotación sino sobre la extracción ya realizada de los mismos, siguiendo criterios de minimización, y realizarlo en un entorno ad-hoc, entre otras.

Entre las medidas técnicas que se podrían aplicar podría ser realizar una evaluación de la imposibilidad de reidentificación en los datos resultantes.

Anonimización: Tratamientos que suponen la consolidación de datos anonimizados de distintos Titulares de Datos

Este es un caso de uso que se puede producir de forma combinada con otros casos mostrados en esta guía, en particular con el caso de uso de tratamiento de datos no personales.

El Espacio de Datos deberá tener en cuenta que, a mayor volumen de datos recibido, aumentan las posibilidades de identificación a pesar de ser datos no personales, especialmente cuando se reciben datos de diversas fuentes. Por ello, entre las funciones de los Mediadores del Espacio de Datos cobra especial relevancia la realización de una primera revisión de la fortaleza del tratamiento de anonimización de un conjunto de datos previamente a ponerlo a disposición del Usuario de Datos.

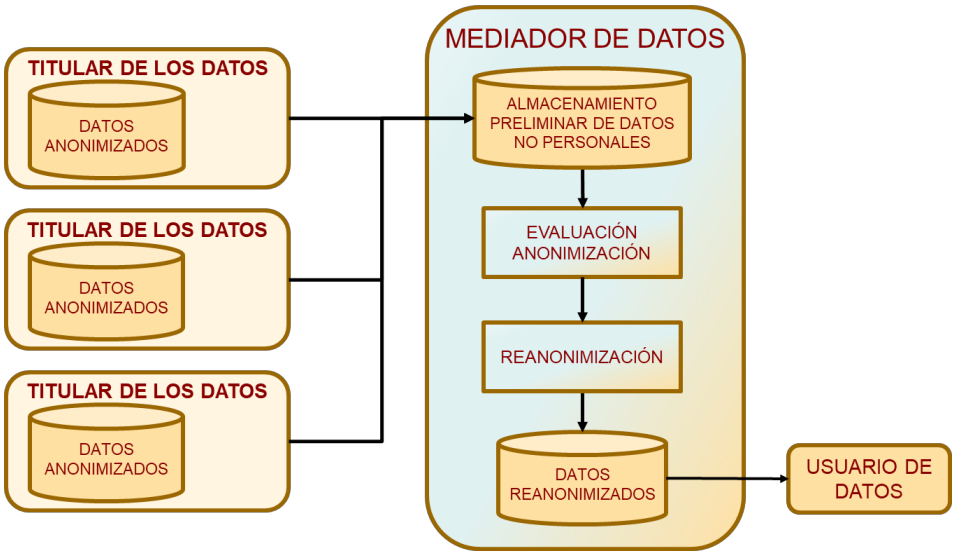

Figura 19: Esquema de la arquitectura para el caso de uso para la consolidación de datos anonimizados de distintos Titulares de Datos

En los casos en los que se detecte la posibilidad de reidentificación, se tendrán que volver a aplicar mecanismos de anonimización ya en el Espacio de Datos, en un entorno seguro, donde se procederá a eliminar cualquier clave de reidentificación, así como todos los datos de esta primera revisión.

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser, por ejemplo, jurídicas como aplicar garantías de limitación de la difusión de los datos anónimos hasta que estos hayan sido correctamente evaluados en su anonimidad o reanonimizados, y la limitación sobre la difusión o conservación de datos anonimizados por acuerdos jurídicos más allá de lo establecido en el RGPD, entre otros.

Entre las organizativas y sobre políticas de protección de datos se podría realizar una eliminación de los conjuntos de datos que conducen a una reidentificación e informar a los Titulares de Datos de esa posible vulnerabilidad, entre otras.

Entre las medidas técnicas se podría implementar un entorno controlado y seguro para el almacenamiento de forma temporal de los datos anonimizados procedentes de las diferentes fuentes sobre los que se realizará la vinculación y posterior anonimización.

Anonimización: Generación y uso de datos sintéticos

Otra estrategia de minimización de datos es la utilización de datos sintéticos. Los datos sintéticos no son datos aleatorios, sino son datos que cumplen con los mismos requisitos que los datos reales en el marco de una finalidad específica. Los requisitos dependerán del caso de uso concreto: una distribución estadística determinada, adecuarse a un determinado tipo de patrones, etc. Esos patrones deberán extraerse de los datos personales tratando dichos datos personales y generando información no personal[150]. En

[150] Un ejemplo de este caso de uso es el proyecto piloto para la compartición de datos que se realiza a nivel europeo con los datos de los bancos centrales de cada país, donde previamente a la puesta a disposición de los datos, se genera una base de datos sintéticos que

cuanto se estén empleando datos personales, el proceso de generar datos sintéticos será o formará parte de un tratamiento sometido al cumplimiento del RGPD.

El Titular de Datos podrá realizar un tratamiento de los datos personales en un entorno ad-hoc para el análisis de los mismos, a continuación, generar los patrones que se derivan de sus datos almacenados y, de esta forma, permitir al propio Titular desarrollar los datos sintéticos, o simplemente liberará los patrones para que un interviniente del ecosistema del Espacio de Datos (puede que el propio Usuario de Datos o a un Habilitador) sea el que genere los conjuntos de datos sintéticos.

Para este caso se propone la siguiente arquitectura:

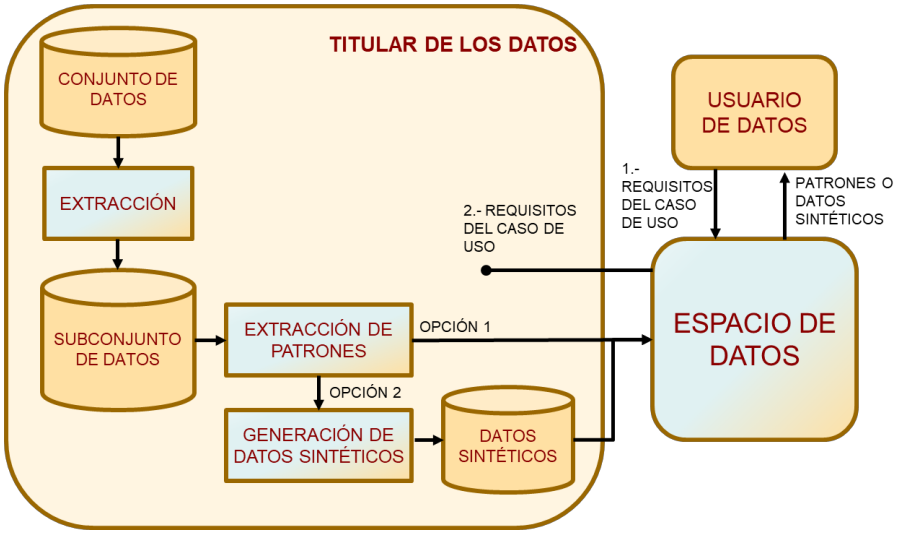

Figura 20: Esquema de la arquitectura para el caso de uso de puesta a disposición datos sintéticos

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser jurídicas, organizativas y técnicas. Por ejemplo, entre las jurídicas se podría incluir la obligación de crear el *data set* sintético en el Titular de Datos o la exigencia de auditorías o certificaciones de las herramientas de generación de datos sintéticos.

Entre las organizativas y sobre políticas de protección de datos se podría realizar el proceso de análisis de los datos en un entorno seguro, con extracción de un subconjunto de datos de los sistemas de explotación, entre otras.

Entre las medidas técnicas se podría incluir, por ejemplo, la evaluación de la anonimidad de los resultados sintéticos.

Anonimización: Computación segura multiparte

Computación Segura Multi-parte[151] o SMPC (por sus siglas en inglés, *Secure Multiparty Computation*). Este es un protocolo criptográfico que, mediante la Compartición Aditiva de Secretos, permite segmentar un dato secreto en distintas partes, de manera que, al

tenga las mismas características que el original. Es un proyecto liderado por *DG for Financial Stability, Financial Services and Capital Markets Union* de la Comisión Europea dentro de su proyecto de creación de un *Data Hub* en la *EU Digital Finance Platform.*

[151] Artículo del blog de AEPD titulado "Privacidad desde el diseño: Computación segura multi-parte, compartición aditiva de secretos | AEPD [mayo 2022]"

compartirse la información, no pueda ser revelado el dato original por ninguna de las fuentes. En el protocolo se obtiene el resultado deseado sin la necesidad de revelar ningún dato sensible, y el resultado obtenido no sufre ningún tipo de desviación.

Esta estrategia es útil en determinados escenarios y precisa de disponer de la ayuda tecnológica para poder implementarla.

Anonimización: Privacidad diferencial

La privacidad diferencial[152] permite garantizar, mediante la incorporación de ruido aleatorio a la información original, que en el resultado del proceso de análisis de los datos a los que se ha aplicado esta técnica no hay pérdida en la utilidad de los resultados obtenidos. Tiene su fundamento en la Ley de los Grandes Números, un principio estadístico que establece que cuando el tamaño de la muestra crece, los valores promedios que se derivan de la misma se aproximan al valor medio real de la información. De esa forma, la adición a todos los datos de un ruido aleatorio permite compensar estos efectos y producir un valor "esencialmente equivalente".

Un ejemplo de uso se puede encontrar en la oficina del Censo de los Estados Unidos[153], que aplica privacidad diferencial para garantizar la precisión de sus estadísticas e impedir que la información personal se revele incluso a través de las mismas, y así aumentar la confianza de los ciudadanos en la seguridad de los datos que proporcionan, aplica privacidad diferencial.

Anonimización: Documentos orientados a la anonimización

El Considerando 9 de la DGA, para el caso de reutilización de datos, manifiesta la necesidad de desarrollar tratamientos de datos en los que la anonimización se plantee desde el concepto de los mismos y en la que los formatos de datos permitan "desde el diseño" una anonimización eficiente: "*Con el fin de facilitar la protección de los datos personales y confidenciales, y de agilizar el proceso de proporcionar tales datos para su reutilización con arreglo al presente Reglamento, los Estados miembros deben animar a los organismos del sector público a crear y poner a disposición datos de conformidad con el principio de «documentos abiertos desde el diseño y por defecto» mencionado en el artículo 5, apartado 2, de la Directiva (UE) 2019/1024 y promover la creación y la adquisición de datos en formatos y con estructuras que faciliten una rápida anonimización en ese sentido.*"

Otras técnicas para salvaguardar la protección de datos

Sin querer ser exhaustivos, existen otras técnicas utilizadas para salvaguardar la protección de datos a la hora de compartirlos. Se identifican, por ejemplo, el cifrado homomórfico, la recuperación de información privada, o las técnicas de aprendizaje federado en *machine learning*. A continuación, se recogen unas breves pinceladas de cada una de estas técnicas.

[152] Artículo del blog de AEPD titulado "Anonimización y seudonimización (II): la privacidad diferencial | AEPD [octubre 2021]"
[153] La privacidad diferencial y el Censo del 2020 (census.gov)

El cifrado homomórfico[154] es una técnica de privacidad por defecto que es adecuada para aquellos casos en que un responsable subcontrata una parte de una actividad a un encargado, y quiere garantizar técnicamente que éste no va a acceder a los datos.

En un esquema tradicional el responsable transmite la información al encargado de forma cifrada, para proteger la confidencialidad durante el tránsito. Una vez que el encargado la ha recibido, la descifra y la trata. Sin embargo, este esquema presenta riesgos tanto legales como técnicos, por lo que lo ideal para minimizar los riesgos sería que el encargado no tuviera la posibilidad de descifrar la información, y que todo su tratamiento pudiera llevarse a cabo sobre los datos cifrados por el responsable. De esta forma, se evitaría que un encargado desleal o un tercero suyo pudiera acceder a los mismos y usarlos para finalidades diferentes. Una forma de conseguir esta protección es mediante el llamado cifrado homomórfico.

Por tanto, el cifrado homomórfico permite realizar operaciones sobre los datos cifrados y obtener resultados, también cifrados, equivalentes a las operaciones realizadas directamente sobre la información original

Por otro lado, la recuperación de información privada (PIR, por sus siglas en inglés de *Private Information Retrieval*[155]) es una técnica criptográfica que permite al usuario recuperar una entrada de una base de datos sin revelar al responsable de la custodia de los datos el elemento que se ha recuperado y desvincular la información que se pudiera inferir relativa a quién está realizando el acceso[156].

Se puede llevar al ejemplo de una empresa que desea que sus clientes puedan acceder a una base de datos. En un entorno predeterminado, cada vez que un cliente accede a la base de datos, el custodio de los datos sabe a qué entrada ha accedido. Con el tiempo, el responsable del tratamiento podrá saber cuáles son las entradas de la base de datos que interesan a los clientes. Al implementar la técnica de recuperación de información privada, el responsable del tratamiento minimiza la cantidad de información revelada sobre los datos a los que se ha accedido, ya que la técnica PIR impide que el responsable del tratamiento sepa cuáles son las entradas consultadas.

Por último, también se pueden destacar las técnicas de aprendizaje federado[157], tanto horizontal como vertical, para aplicaciones de inteligencia artificial basadas en aprendizaje automático (*Machine Learning*). Las técnicas de aprendizaje federado son una categoría de PET (*Privacy-Enhancing Technology*) que permiten el desarrollo de sistemas de aprendizaje automático sin necesidad de comunicar los datos personales entre los intervinientes. Estas técnicas pueden ser tanto de tipo horizontal como vertical y son clave en los nuevos escenarios que se plantean para mejora y desarrollo de la sociedad como, por ejemplo, los Espacios de Datos.

---

[154] Artículo del blog de AEPD titulado "Cifrado y Privacidad III: Cifrado Homomórfico [junio 2020]"
[155] INGENIERÍA DE LA PROTECCIÓN DE DATOS, De la teoría a la práctica. European Union Agency for Cybersecurity (ENISA) [Enero de 2022]
[156] Por ejemplo, en caso de investigación salud, financiera o policial, el Titular de Datos o el Mediador no recibirían información de que se consultan los datos de determinada persona.
[157] Artículo del blog de AEPD titulado "Federated Learning: Inteligencia Artificial sin comprometer la privacidad | AEPD [abril 2023]"

El aprendizaje federado habilita la creación de modelos de *Machine Learning* donde, en lugar de centralizar los datos en un gran repositorio para analizarlos, se envían modelos al lugar donde están ubicados los datos. Esta estrategia, del tipo "*compute-to data*" permite un tratamiento local de los datos para, posteriormente, agregar el resultado de los modelos parciales desarrollados y consolidar la información obtenida del aprendizaje en un modelo completo. De esta forma, habilita la creación de espacios federados de datos en los que cada participante mantiene el control, la soberanía y preserva la protección de los datos, eligiendo en todo momento quién puede hacer uso de los datos y para qué caso de uso en particular.

Seudonimización de datos

La seudonimización se implementan mediante un conjunto de operaciones dentro de un tratamiento (en algún caso muy específico podría ser un tratamiento en sí mismo) y tiene el objetivo de ser una medida de seguridad cuando no sea posible cumplir los fines del tratamiento mediante anonimización. Uno de esos fines podría ser la necesidad de vincular los datos de un mismo sujeto entre diferentes Titulares de Datos, otro cuando los datos no se reciben en modo *batch*, sino de forma continuada (p.ej. se reciben de dispositivos móviles o IoT), y otro es cuando se necesite informar a un Interesado o Sujeto de los Datos de forma específica sobre algún resultado del tratamiento de sus datos (caso de la investigación clínica) y que por, tanto, sean necesaria una reidentificación esporádica y selectiva a fin de garantizar los intereses vitales de los sujetos de los datos.

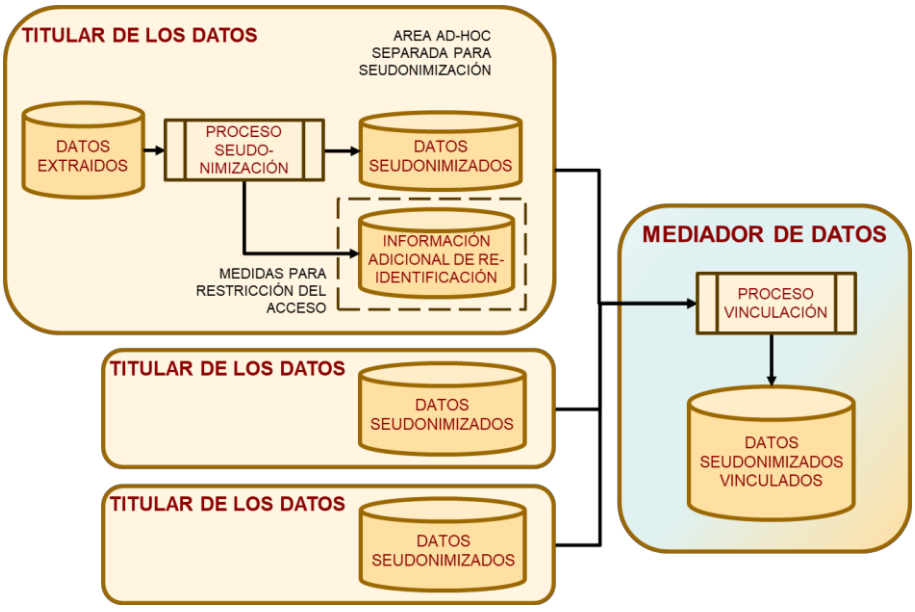

Figura 21: Esquema de la arquitectura para el caso de uso de seudonimización

Además, en determinados sectores, como el de la investigación clínica, existen requisitos y una normativa específica[158] por lo que lo aquí desarrollado será sin perjuicio de dicha normativa. En algunos sectores está regulada la figura de un Habilitador como entidad de confianza que va a ejecutar el proceso de seudonimización y que tiene la

[158] Disposición adicional 17 de la LOPDGDD, o el Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia

responsabilidad de la custodia de la información adicional de reidentificación, por ejemplo, el monitor en el caso de la investigación clínica.

En el proceso de seudonimización también se pueden emplear técnicas de cifrado polimórfico (*Polymorphic Encription and Pseudonimization* o PEP) [159]. A cada individuo se le asignan diferentes seudónimos para cada Usuario de Datos que solicita acceso a los datos del Sujeto, evitando así la vinculación de seudónimos a través de múltiples terceros.

En el caso concreto de Espacios de datos de salud, cada paciente podría tener un identificador único. Este identificador podría ser transformado por el Mediador en diferentes seudónimos dependiendo del destinatario y el contexto o propósito de compartir los datos. Cada seudónimo se comunica a cada destinatario junto con los datos cifrados polimórficos. Como para cada receptor se está generando un nuevo seudónimo, los seudónimos utilizados para el mismo paciente no se pueden vincular, por lo que se consideran no vinculables y preservan la confidencialidad de los datos del paciente.

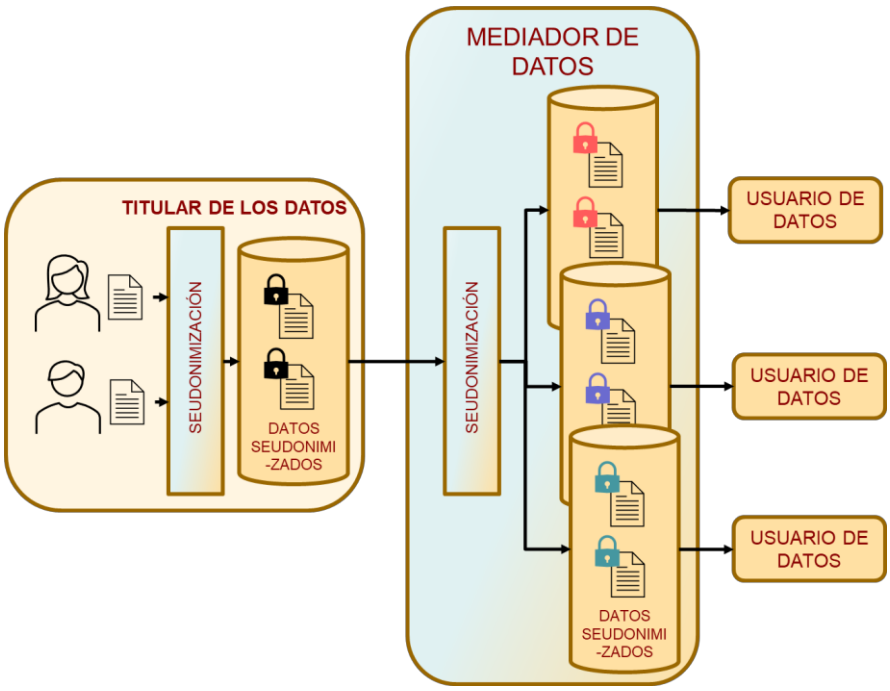

Figura 22: Esquema de la arquitectura para seudonimización de un mismo conjunto de datos para diferentes Usuarios de Datos

Tratamientos que requieren datos anonimizados cuando es relevante vincular la información personal tratada por distintos Titulares de Datos

Esto es un caso de uso que se podría plantear donde estrategias como Computación Segura Multiparte o Privacidad Diferencial no pueden dar resultado. Un ejemplo podría producirse cuando se desee realizar el análisis de productos o servicios que un mismo Sujeto esté llevando a cabo en distintos Titulares de Datos para lo que es necesario vincularlos inicialmente, pero que finalmente se mostrarán de manera anonimizada.

[159] Apartado 2.2.1 del documento "*ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023]*".

En ese caso, se podría realizar un proceso previo de sustitución de identificadores y seudoidentificadores por nuevos seudoidentificadores no vinculados con datos personales. Esto se debería llevar a cabo mediante un mecanismo previamente acordado por todos los Titulares en el marco de la gobernanza del Espacio de Datos, de forma que cuando los registros se comuniquen al Espacio de Datos sea posible vincular los correspondientes a un mismo usuario.

Una vez recibidos en el Espacio de Datos, se crearía un consolidado de los datos anónimos y se desecharían la información utilizada para vincular los registros.

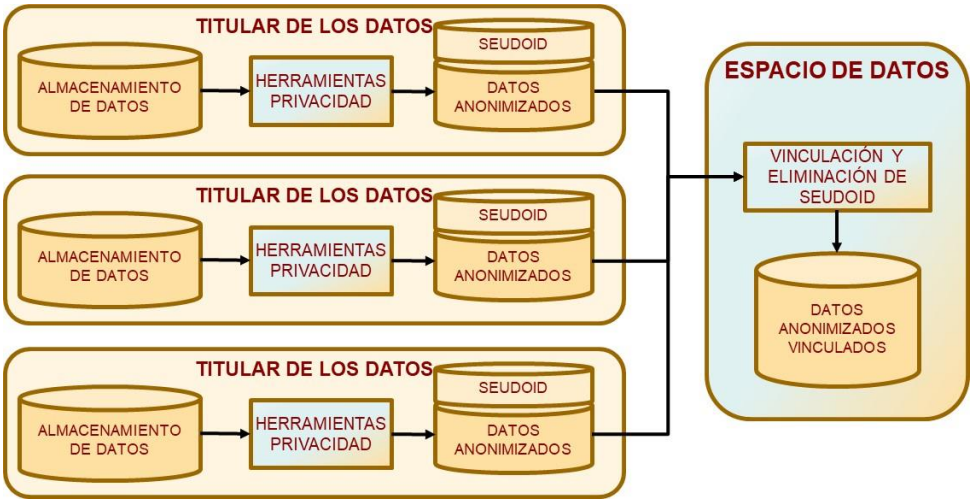

Figura 23: Esquema de la arquitectura para el caso de uso de datos anonimizados con vinculación entre los datos de distintos Titulares de Datos

Esta aproximación podría tener que hacer uso de espacios ad-hoc para implementar la extracción y los procesos de anonimización en los Titulares, y a su vez un análisis de reidentificación en el Espacio de Datos del conjunto de datos consolidado.

Las garantías que se podrían establecer se podrían derivar de las ya mencionadas para el tratamiento de datos personales, seudónimos y anónimos.

Tratamientos en los que no es posible anonimizar los datos

Pueden existir tratamientos que por su propia naturaleza no es posible conseguir un nivel de calidad adecuado con datos anonimizados. Esta circunstancia ha de estar correctamente evaluada en la EIPD y haber superado el análisis de idoneidad, necesidad y proporcionalidad estricta por los responsables de tratamiento.

En el marco de la evaluación del riesgo, en particular, de la evaluación de la proporcionalidad del tratamiento, existen tres opciones, ordenadas de menor a mayor riesgo, para el implementar el tratamiento:

1. Trasladar el tratamiento deseado por el Usuario de Datos a los Titulares de los Datos (p.ej. utilizando técnicas de aprendizaje federado).
2. Transferir o comunicar datos personales al Espacio de Datos, a un Mediador, y trasladar el tratamiento a un Entorno de Tratamiento Seguro proporcionado por

el mismo (aplicando en su caso seudonimización o anonimización en el Espacio de Datos u otras estrategias).

3. Transferir o comunicar datos personales al Espacio de Datos y de éste al Usuario de Datos.

Este último caso será el último en contemplar, tras descartar todos los anteriores basadas en un análisis de estricta necesidad. Además, será el que requiera una evaluación más restrictiva sobre la necesidad, ya citada, y proporcionalidad del tratamiento, es decir, contemplando unas garantías más estrictas de protección de datos.

Cualquier tratamiento que implique la extracción de datos personales del ámbito del Titular de Datos deberá aplicar un análisis previo de minimización de datos. En particular, se deberían aplicar uno o más métodos como los siguientes:

- Eliminación de campos innecesarios y metadatos (p.ej. en caso de imágenes).
- Disminuir la granularidad de la información de los campos transmitidos.
- Disminuir la frecuencia de los eventos recogidos.
- Ruido con características estadísticas que no degrade la calidad necesaria.
- Ofuscación.
- Agrupación (p.ej. entre 40 y 45 años).
- Scrambling.
- Tokenización.
- Aplicación de técnicas de cifrado.

Entre las técnicas de cifrado a emplear hay que plantear el empleo de modernas estrategias como cifrado homomórfico ante descritas, y también cifrado basado en atributos, recifrado proxy, cifrado polimórfico[160] y otros.

Además, en el marco de un Espacio de Datos, habrá que tener en cuenta que los datos personales recogidos por un Titular de Datos podrán estar sometidos a los siguientes tratamientos adicionales que habrá que registrar e incluir dentro de la EIPD:

1. Tratamientos en el propio Titular de Datos para cumplir los fines del Espacio de Datos o de los Usuarios de los Datos
2. Cesión de los datos personales al Espacio de datos.
3. Cesión de los datos personales por parte del Espacio de Datos al Usuario de Datos.

Entornos de tratamiento seguro

Como se ha señalado anteriormente, puede darse el caso que para implementar tratamientos específicos sea estrictamente necesario dar acceso a datos personales sin anonimizar de los Titulares de los Datos al Espacio de Datos, ya que de otra forma no se podrían cumplir con las finalidades del tratamiento.

[160] *ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023].*

En algunas de las arquitecturas anteriores se ha tratado de la utilización de un área ad-hoc para almacenar la extracción y tratamiento de datos personales para realizar preprocesos previos a la comunicación de información al Espacio de Datos. Un Entorno de Tratamiento Seguro está relacionado con dichas áreas ad-hoc, y se podría definir como áreas o servicios proporcionados por aquel que almacena físicamente los datos y que permiten a personal previamente autorizado acceder y analizar directamente datos cuyo libre acceso supondría un riesgo inasumible, incluso contando con garantías jurídicas[161]. En el caso de acceso de Usuarios de los Datos a datos personales almacenados en el Espacio de Datos, suponen una medida organizativa y técnica para minimizar el tratamiento de los datos y la conservación de estos (casi llevando la retención a cero) en manos de los Usuarios de Datos.

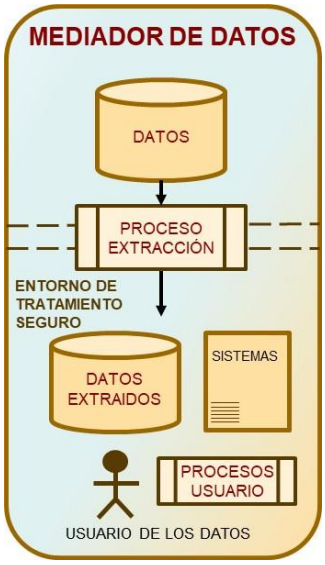

Figura 24: Esquema de un Espacio Seguro en el Mediador de Datos

El acceso y la reutilización de datos en un Entorno de Tratamiento Seguro no pueden considerarse una alternativa a las bases jurídicas enumeradas exhaustivamente en el artículo 6 del RGPD[162].

En el caso de datos protegidos que obren en poder de los organismos del sector público, el Considerando 15 de la DGA aclara que podría permitirse su reutilización presencial o remota en un Entorno de Tratamiento Seguro siempre que se hayan cumplido los posibles requisitos de realizar una EIPD y de consultar a la autoridad de control en virtud de los artículos 35 y 36 del RGPD, y se haya constatado que los riesgos para los derechos y los intereses de los interesados son mínimos. Los organismos del sector público impondrán condiciones que preserven la integridad del funcionamiento de los sistemas técnicos del entorno de tratamiento seguro utilizado, se reservarán el derecho a verificar el proceso, los medios y los resultados del tratamiento de datos efectuado por el Reutilizador para preservar la integridad de la protección de los datos, así como el derecho

[161] SOMA_D2.1.pdf Evaluating Safe space solution including data management and processing setups (disinfobservatory.org)
[162] Párrafo 81 del documento "Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]".

a prohibir la utilización de aquellos resultados que contengan información que ponga en peligro los derechos e intereses de terceros[163].

Por otro lado, la propuesta de EHDS establece en su artículo 50 "1. *Los organismos de acceso a los datos sanitarios facilitarán el acceso a los datos sanitarios electrónicos únicamente a través de un entorno de tratamiento seguro, con medidas técnicas y organizativas y requisitos de seguridad e interoperabilidad.*" y "2. *Los organismos de acceso a los datos sanitarios garantizarán que los titulares de los datos puedan cargar los datos sanitarios electrónicos y que el Usuario de Datos pueda acceder a ellos en un entorno de tratamiento seguro. Los usuarios de datos solo podrán descargar datos sanitarios electrónicos no personales desde el entorno de tratamiento seguro*".

En el mismo artículo de la propuesta de EHDS se enumeran las medidas de seguridad que han de tener dichos Entornos y que pueden servir de guía para otros Espacios de Datos:

a) *"restringir el acceso al entorno de tratamiento seguro a las personas autorizadas enumeradas en el correspondiente permiso de datos;*
b) *minimizar el riesgo de lectura, copia, modificación o supresión no autorizadas de los datos sanitarios electrónicos alojados en un entorno de tratamiento seguro a través de los medios tecnológicos más avanzados;*
c) *limitar la introducción de datos sanitarios electrónicos y la inspección, modificación o supresión de los datos sanitarios electrónicos alojados en el entorno de tratamiento seguro a un número limitado de personas identificables autorizadas;*
d) *garantizar que los usuarios de datos solo tengan acceso a los datos sanitarios electrónicos cubiertos por su permiso de datos, únicamente mediante identidades de usuario individuales y únicas y modos de acceso confidenciales;*
e) *conservar registros identificables de acceso al entorno de tratamiento seguro durante el período de tiempo necesario para verificar y auditar todas las operaciones de tratamiento en dicho entorno;*
f) *garantizar el cumplimiento y supervisar las medidas de seguridad a que se refiere el presente artículo para mitigar las posibles amenazas para la seguridad.*"

Los Entornos de Tratamiento Seguro se podrían definir a dos niveles:

- Entorno de Tratamiento Seguro presencial/físico, que implican que el tratamiento y el operador del Usuario de Datos se trasladan físicamente a los locales en donde se encuentran los datos, y allí son sometidos a controles de acceso y proceso. La información resultante sí es posible extraerla del espacio seguro.
- Entorno de Tratamiento Seguro remoto/virtual, en que si bien el tratamiento se ejecuta en los locales donde se almacenan los datos, el operador puede manipular el tratamiento de forma remota, de forma que el operador no tiene acceso a los

[163] Artículo 5.4 de la DGA

datos, pero sí a la información resultante. La manipulación se realizaría a través de redes virtuales seguras o incluso de redes privadas físicas.

En ambos casos, los datos originales no salen el lugar físico de almacenamiento de la información.

El segundo caso, el Entorno de Tratamiento Seguro con acceso virtual, ha demostrado en su aplicación efectiva su vulnerabilidad, incluso cuando los accesos se permiten únicamente a través de redes privadas físicas, derivando en brechas de datos de gran impacto social. Por ello, su uso ha de estar complementado por otras garantías.

Además, dichos Entornos de Tratamiento Seguro deberían implementarse sobre Entornos de Ejecución Confiables[164]. Aunque dichos entornos deberían implementarse para todo tratamiento de datos personales, en los Espacios Seguros es dónde sería más crítico. Un entorno de ejecución confiable (TEE), tal como lo define ENISA, es un entorno de tratamiento inviolable en el procesador principal de un dispositivo. Al funcionar en paralelo al sistema operativo y utilizar tanto hardware como software, los TEE están diseñados para ser más seguros que los entornos de tratamiento tradicionales. También recibe el nombre de entorno de ejecución de sistema operativo enriquecido (REE), en el que se ejecutan el SO y las aplicaciones del dispositivo.

F. ALMACENAMIENTO DE DATOS PERSONALES Y NO PERSONALES EN EL ESPACIO DE DATOS

En el caso de que en un Mediador se almacenen, aunque sea temporalmente, datos personales además de datos no personales (que no sean conjunto de datos mixtos), se deberá analizar si se incurre en un alto riesgo (ver apartado VI.B.Alto Riesgo).

Las medidas que se podrían aplicar para garantizar y poder demostrar la conformidad con la normativa de protección de datos en este caso de uso podrían ser, por ejemplo, jurídicas como acuerdos para la limitación del almacenamiento y del tratamiento más allá de las obligaciones del RGPD, compromisos de confidencialidad del personal, cláusulas sobre los periodos de cancelación o de limitación del tratamiento, entre otras.

Entre las organizativas y sobre políticas de protección de datos se podría incorporar supervisión humana a los accesos a los conjuntos de datos, tener una separación funcional entre datos personales y no personales, entre otras.

Entre las medidas técnicas se podría realizar una separación física entre ambos conjuntos de datos, impedir el acceso directamente desde Internet a los conjuntos de datos personales, incorporar trazabilidad del acceso de terceros mediante informe correspondiente (Informe de trazabilidad) que incluya persona (física, no jurídica), fecha de acceso y tiempo de sesión de acceso, auditorías automáticas, limitación técnica en cuanto a datos accedidos, entre otros[165].

[164] Apartado 4.3 del documento "INGENIERÍA DE LA PROTECCIÓN DE DATOS, De la teoría a la práctica. European Union Agency for Cybersecurity (ENISA) [Enero de 2022]"

[165] Con independencia de las medidas que serían recomendables u obligadas en la normativa para datos no personales. Por ejemplo, la DGA establece requisitos para la seguridad de datos no personales y en los servicios de intermediación de datos en al Artículo 12.l, o para las las organizaciones de altruismo reconocidas en la Unión en el Artículo 21.4.

VI. CUESTIONES SOBRE PROTECCIÓN DE LOS DATOS PERSONALES EN UN ESPACIO DE DATOS

Para reforzar e implementar el control de las personas físicas de sus propios datos personales[166], el RGPD establece un conjunto de principios y derechos, así como obligaciones para aquellos que tratan datos personales, que se extienden a lo largo de todo el texto de la norma.

Los principios[167] de licitud, lealtad, transparencia, finalidad, minimización, exactitud, conservación, seguridad y responsabilidad proactiva, son todos de obligatorio cumplimiento, autónomos y complementarios entre sí, no pudiendo reducirse unos en otros como, por ejemplo, considerar que la seguridad para la protección de datos personales subsume a cualquiera de los anteriores. Por lo tanto, los tratamientos sobre un Espacio de Datos han de cumplir todos ellos.

La falta de cumplimiento supondría impedir la libre circulación de los datos de carácter personal en la Unión Europea y constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas[168]. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la UE no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales[169] y, para que esto no suceda, los tratamientos han de implementarse con medidas apropiadas que garanticen y permitan demostrar que son conformes con el RGPD, además de que dichas medidas se revisen y actualicen cuando sea necesario[170].

Algunas de las cuestiones que se derivan de la normativa de protección de datos para el marco específico de los Espacios de Datos ya se han desarrollado en los apartados anteriores. En este capítulo se van a desarrollar algunas otras cuestiones de relevancia, todo ello sin pretender ser exhaustivos y sin perjuicio de la normativa sectorial aplicable.

A. DELEGADO DE PROTECCIÓN DE DATOS

Los Espacios de Datos están proponiendo tratamientos de una dimensión desconocida hasta ahora, por lo que no se puede plantear un cumplimiento de mínimos o formal, sino que será necesario aplicar un nivel de cumplimiento equivalente a la dimensión del tratamiento. Como establece el artículo 24.1 del RGPD, las medidas que desde la concepción y diseño de los Espacios de Datos garanticen y permitan demostrar el cumplimiento, han de estar dimensionadas en función de "la naturaleza, el ámbito, el contexto y los fines del tratamiento". De ahí la importancia de la implicación de los Delegados de Protección de Datos y asesores en protección de datos en las fases más tempranas de la definición de un Espacio de Datos y desde el diseño en sus tratamientos.

Los intervinientes en el Espacio de Datos deberán determinar si tienen la obligación de nombrar un Delegado de Protección de Datos (DPD), con relación a la escala del

[166] Considerando 7 del RGPD
[167] Artículo 5 del RGPD
[168] Considerando 9 del RGPD
[169] Considerando 13 del RGPD
[170] Artículo 24.1 del RGPD

tratamiento que realiza, pues se puede considerar dentro de los supuestos del artículo 37.1.b o c. Las AAPP, como establece el artículo 37.1.a, deberán tener un DPD.

En caso de no tener la obligación, se considera recomendable que todos los Mediadores dispongan de un DPD y/o de una asesoría de protección de datos. Esto es especialmente recomendable para las entidades que ejerza las funciones de supervisión y autorización de los accesos al Espacio de Datos. En este sentido, y en la medida es que si estas acciones de supervisión son realizadas por los comités éticos de investigación, el propio legislador exige a estos, en el ámbito de la salud, biomédico o del medicamento, que deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del RGPD cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados[171].

El DPD ha de participar en la definición de los modelos de gobernanza y políticas del Espacio de Datos, análisis y evaluación de los casos de uso, de la selección de las medidas de protección de datos desde el diseño, la gestión de las brechas de datos personales y en el asesoramiento y supervisión de las evaluaciones de impacto.

B. GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS

El responsable de un tratamiento de datos personales tiene la obligación, según los artículos 24 y 35 del RGPD, de realizar una gestión de los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas y, en su caso, la evaluación de impacto para la protección de datos (EIPD). Dicha obligación ha de ser ejercida por los responsables de tratamientos que se planteen sobre la infraestructura del Espacio de Datos, y también por el legislador cuando éste es quien establece normativamente un Espacio de Datos[172]. Por ello es de vital importancia identificar los diferentes responsables del tratamiento que pueda haber tras la autorización de acceso a los datos y el papel del Supervisor de Acceso apoyado, en su caso por un Habilitador de protección de datos, es fundamental.

La correcta gestión del riesgo para los derechos y libertades incluye la evaluación del riesgo y la selección, ejecución, revisión y actualización de las medidas apropiadas para garantizar el cumplimiento. Un modelo de tratamiento en el Espacio de Datos que no gestione el riesgo cumpliendo con los principios de protección de datos desde el diseño y por defecto podría suponer forzar al máximo todos los principios de protección de datos, en particular los de minimización, conservación y limitación del tratamiento.

La gestión del riesgo no es un requisito formal, sino que es una herramienta para la toma de decisiones sobre cómo se han de implementar desde el diseño los casos de uso de los tratamientos para garantizar el cumplimiento de la normativa de protección de datos y la minimización del impacto para los Sujetos de los Datos. Como ejemplo de una aproximación errónea a una gestión del riesgo para los derechos y libertades de los Sujetos de los Datos en el marco de los Espacios de Datos, en la "*EDPB-EDPS Joint Opinion*

[171] Disposición adicional 17 de la LOPDGDD.
[172] Consultar las Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo de la AEPD

03/2022 on the Proposal for a Regulation on the European Health Data Space", en el párrafo 49, se manifiesta que el borrador de EHDS no ha gestionado los riesgos para los derechos y libertades al no haber llevado a cabo una EIPD ya que, según la nota 18 que acompaña al párrafo, ambas instituciones interpretan que el documento que acompaña a la norma "*Commission Staff Working Document Impact Assessment Report*" no es una EIPD, a pesar de su título, al no realizar una evaluación del riesgo ni proporcionar las medidas necesarias para mitigarlo.

Riesgos para los derechos fundamentales

Resulta evidente la necesidad de gestionar desde el diseño los riesgos para los Sujetos de los Datos que se pueden originar por la materialización de brechas de datos personales en Espacios de Datos. Sin embargo, los riesgos para los derechos fundamentales van más allá que las brechas de datos personales, ya que el propio tratamiento de datos puede suponer un riesgo o una limitación a dichos derechos fundamentales. La directrices WP248[173] establecen que la protección se ha de extender a otros derechos fundamentales, como la libertad de expresión la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, la libertad de conciencia y de religión, la inviolabilidad del domicilio o las comunicaciones, o la tutela judicial efectiva.

Hay que tener en cuenta que muchos de los tratamientos de los Espacios de Datos involucrarán intervinientes tanto de las AAPP como de entidades privadas, y cuya base legal se podrá encontrar en la norma.

Tanto la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE)[174] así como las opiniones del SEPD[175] manifiestan que la evaluación de impacto de una normativa con relación a la protección de datos debe realizarse en los casos en que la medida legislativa propuesta implique el tratamiento de datos personales. Cualquier operación de tratamiento de datos prevista por la legislación supone una limitación del derecho a la protección de los datos personales, independientemente de que dicha limitación pueda estar justificada. A su vez, el Tribunal Europeo de Derechos Humanos (TEDH) ha sostenido que el almacenamiento por parte de una autoridad pública, de datos relativos a la vida privada de una persona equivale a una limitación del derecho al respeto de su vida privada[176].

La jurisprudencia reiterada del TJUE establece que «para determinar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia si la información tiene o no carácter sensible o si los afectados han sufrido algún tipo de inconveniente»[177]. La evaluación del respeto a la esencia del derecho puede, en algunos casos, necesitar un profundo análisis jurídico, de ahí la importancia de las evaluaciones de la idoneidad, necesidad y la proporcionalidad estricta de los tratamientos

[173] WP248 Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (Grupo de Trabajo del Artículo 29) [4 de octubre de 2017]
[174] TJUE, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, apartados 34 - 36; véase también los asuntos acumulados C-92/09 y C-93/09 Volker und Markus Schecke, apartado 58.
[175] Apartado II.5 del documento "Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos personales (EDPS) [11 de abril de 2017]".
[176] TEDH, Leander c. Suecia, apartado 48.
[177] TJUE, asuntos C-465/00, C-138/01 y C-139/01 Österreichischer Rundfunk y otros, apartado 75 y Digital Rights Ireland, apartado 33.

y la implementación de medidas, más allá de las de ciberseguridad, derivadas de las Evaluaciones de Impacto para la Protección de Datos.

Alto riesgo

Los tratamientos en el marco de un Espacio de Datos suponen, al menos, el acceso, que podría incluir comunicación y almacenamiento en terceros, de cantidades masivas de datos personales de distintas fuentes con una novedosa solución técnica/ organizativa, a gran escala, de una forma exhaustiva, sistemática, que incluye asociación y combinación de datos, automatizado, y orientado a la aplicación de tecnologías novedosas[178]. Hay que tener en cuenta, en particular para los Espacios de Datos Europeos, que se abre la posibilidad de tratamientos que afecten a la totalidad de los Interesados o Sujetos de los Datos, con recogida masiva de información en cuanto a categorías de datos, granularidad y frecuencia, correlación de fuentes distintas, acceso a los mismos por multiplicidad de intervinientes, etc., y para múltiples fines.

Aunque para todos los tratamientos se exige una gestión del riesgo para los derechos y libertades de los interesados según en el artículo 24.1, los tratamientos de alto riesgo [179] tienen como obligación realizar una evaluación de impacto para la protección de datos (EIPD). Para determinar si hay un alto riesgo hay que comenzar consultando los casos que ya están tasados, como:

- Los casos del artículo 35.3 del RGPD.
- La normativa especial que exige una EIPD para el tratamiento o identifica factores de riesgo.
- Los casos y ejemplos de las Directrices WP248.
- Los casos de la lista aprobada por la AEPD en base al artículo 35.4 del RGPD.
- Los casos del artículo 28.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Los casos del artículo 32.2 del RGPD.
- Los riesgos identificados en el Considerando 75[180].
- Los casos y condiciones específicas descritos en las directrices publicadas por el CEPD para tratamientos específicos.

[178] Apartado II.B.a. del documento "WP248 Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (Grupo de Trabajo del Artículo 29) [4 de octubre de 2017]".

[179] Artículo 35.1 del RGPD

[180] *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*

- Los casos y condiciones específicas descritos en los códigos de conducta de acuerdo con el artículo 40 y mecanismos de certificación de acuerdo con el artículo 42 del RGPD.

Aunque un tratamiento no esté en el conjunto de datos tasados como de alto riesgo, que es una lista de mínimos, hay que determinar para cada tratamiento que el impacto que tiene éste no conlleva un alto riesgo. Es importante destacar que la existencia de un alto riesgo para los derechos y libertades de los Sujetos de los Datos no está vinculado exclusivamente al tratamiento de categorías especiales de datos, aunque el tratamiento de este tipo de datos incrementará la posibilidad de un mayor impacto para los Sujetos de los Datos. Para facilitar el análisis de la existencia de un alto riesgo, la AEPD ha puesto a libre disposición guías y herramientas[181] que simplifican su determinación.

Si el proceso de gestionar un alto riesgo no consigue reducirlo hay que consultar a la autoridad de protección de datos. Si no se cumplen los criterios de idoneidad, necesidad y proporcionalidad, o no se ha podido mitigar el alto riesgo, el tratamiento no se podrá llevar a cabo.

Riesgo social

Las medidas de protección de datos, en particular las orientadas a minimización de datos o aquellas de seguridad para la gestión del control de acceso, están normalmente orientadas a minimizar el impacto individual en el derecho a la protección de datos por el tratamiento excesivo de datos personales por un responsable o por el compromiso de los mismos datos personales. Sin embargo, cuando nos encontramos en el marco de Espacios de Datos donde la extensión del tratamiento, tanto en las categorías de datos, en las categorías de Interesados o incluso en los periodos de conservación son muy extensos, es necesario establecer medidas específicas de protección de datos desde el diseño para disminuir un posible impacto tanto a nivel individual como a la sociedad en su conjunto.

Hay que tener en cuenta también la perspectiva del riesgo que supone para la sociedad el impacto de que una cantidad masiva de Interesados o Sujetos de los Datos sufran un compromiso en sus datos personales. La intrusión en el derecho a la protección de datos aparece por la mera acumulación de información personal en determinadas organizaciones. En estos casos, no solo han de considerarse cada uno de los impactos individuales en los derechos fundamentales como una suma de estos, sino que tiene un efecto multiplicador que afecta a los fundamentos de nuestra sociedad: la falta de confianza en las instituciones, la manipulación de grandes sectores de la población o de grupos especialmente vulnerables, la puesta en riesgo de sectores masivos de la población que hacen inviables medidas de mitigación, etc.

Accountability de los medios

El principio de responsabilidad proactiva o "*accountability*" de los tratamientos difícilmente podrá cumplirse si los medios técnicos que se emplean para implementarlo (su naturaleza) no son por sí mismos "*accountables*".

[181] Disponibles en el sitio web: Innovación y Tecnología

Por lo tanto, el responsable tendrá la obligación de exigir la información y colaboración necesaria para el cumplimiento de la norma a la hora de garantizarla y de poder demostrarla, tanto de encargados de tratamiento como de los Habilitadores que no tengan tal naturaleza, pero faciliten herramientas empleadas por responsables/encargados/subencargados para implementar los medios de los tratamientos. Los servicios y herramientas que proporcionan deben de tener auditadas, acreditadas o certificadas su calidad cuando puedan influir en el tratamiento de datos personales realizados por responsables o encargados, de forma que el responsable pueda cumplir con sus obligaciones.

Aplicación del principio de precaución desde el diseño

La Comisión Europea declaró en su Comunicación sobre el principio de precaución[182]: "*Aunque en el Tratado sólo se mencione explícitamente el principio de precaución en el terreno del medio ambiente, su ámbito de aplicación es mucho más amplio. Este principio abarca los casos específicos en los que los datos científicos son insuficientes, no concluyentes o inciertos, pero en los que una evaluación científica objetiva preliminar hace sospechar que existen motivos razonables para temer que los efectos potencialmente peligrosos para el medio ambiente y la salud humana, animal o vegetal pudieran ser incompatibles con el alto nivel de protección elegido.*".

A este respecto, el SEPD ha señalado la oportunidad de la aplicación del principio de precaución como medida preventiva ante tratamientos de gran impacto o en el que hay incertidumbre de cuál podría ser su impacto[183]. Es decir, como herramienta para la gestión del riesgo.

Con relación a los Espacios de Datos, la aplicación del principio de precaución puede adoptarse con varias estrategias: la realización de *sandboxes*[184], la adopción de un "enfoque incremental" en el despliegue del tratamiento (limitación geográfica, en categorías de interesados, en categorías de datos, número de intervinientes, encargados/subencargados, etc.) con hitos de evaluación supervisados por autoridades independientes, etc.

Garantías en las comunicaciones de datos

En el caso de comunicaciones de datos personales, en función de los riesgos para los Sujetos de los Datos se debería realizar una evaluación exhaustiva de la idoneidad y necesidad de dicha comunicación, y de la proporcionalidad de la misma con respecto al tratamiento en el marco de la gestión del riesgo. Además, se podrían obtener las siguientes garantías en compromisos bajo contrato, licencias[185] de uso que limiten su tratamiento, incluyendo cláusulas de penalización, independientemente de las responsabilidades en las que se incurran a nivel penal, civil o administrativo, con relación a:

[182] Comunicación sobre el principio de precaución (COM(2000)1 final) [2 de febrero de 2000]
[183] Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales [19 de diciembre de 2019].
[184] Entornos controlados de pruebas.
[185] En el considerando 28 y en la definición recogida en el artículo 2.10) de la DGA se hace referencia al uso de licencias en el intercambio de datos.

- No reutilización de la información.
- No transmisión a terceros.
- No anonimización de la información para puesta a disposición de terceros.
- No almacenamiento o tratamiento de la información en encargados del tratamiento, especialmente en la Nube.
- No almacenamiento o tratamiento de la información en sistemas del Usuario de Datos fuera del Espacio Económico Europeo.
- Implementación de soluciones de protección de datos desde el diseño y por defecto en el diseño del tratamiento.
- Disponibilidad de un sistema de gestión de brechas de datos personales efectivo.
- Implicación del Delegado de Protección de Datos en dicho tratamiento.
- Demostración, mediante certificación de un tercero independiente, del cumplimiento de la normativa de protección de datos para el tratamiento concreto que pretende hacer, la cualificación de los trabajadores con relación a dicho tratamiento y el cumplimiento de las condiciones antes enumeradas.
- Certificación, mediante petición a la Autoridad de Control, de la inexistencia de sanciones por incumplimiento de la normativa de protección de datos.

Medidas de seguridad

Los Espacios de Datos deben garantizar un alto nivel de ciberseguridad[186]. Las medidas de seguridad son de la mayor importancia, sin embargo, hay que recordar que gran parte de las limitaciones y riesgos a los derechos y libertades de las personas que en los tratamientos no se resuelven con medidas de seguridad. En particular, aquellos riesgos relacionados con los principios minimización, limitación del tratamiento y limitación de la conservación, entre otros, han de ser gestionados con medidas sobre el concepto de los tratamientos, gobernanza, políticas de protección de datos, medidas de protección de datos desde el diseño y por defecto (como las señaladas en el capítulo anterior), de gestión de brechas de datos personales, etc. No todas las medidas de seguridad están orientadas a proteger los derechos y libertades de los Sujetos de los Datos, algunos serán tratamientos con otras finalidades y sus propias legitimaciones[187].

Hay que recordar que las medidas de seguridad, según la experiencia y la doctrina del Tribunal Supremo[188], suponen una obligación de medios, pero no de fines. La realidad de las brechas de datos personales hace evidente que la materialización de las amenazas sobre los conjuntos de datos es cuestión de tiempo, y que la única incógnita es la dimensión que va a tener.

[186] Considerando 2 de la DGA
[187] Considerando 49 del RGPD
[188] C.G.P.J - Noticias Judiciales (poderjudicial.es)

En caso de AAPP, u otras entidades obligadas, han de implementar las medidas del ENS[189] correspondientes a la evaluación del nivel de riesgo para los derechos y libertades de las personas físicas del tratamiento. Estas medidas son catálogo de mínimos, y en función de las especificidades del tratamiento (ver art.32 del RGPD) y de la evaluación del riesgo desde otras perspectivas (p. ej. en el caso de infraestructuras críticas) se tendrán que ampliar. Además, en función del rol que tengan en el Espacio de Datos y el impacto que este pueda tener en la seguridad del conjunto del Espacio, será altamente recomendable que estén certificados.

Disponibilidad y resiliencia

El Artículo 32.1.b del RGPD exige, entre otros, el garantizar la disponibilidad y resiliencia permanente de los servicios y tratamientos de datos personales.

En ese sentido también se expresa la DGA, pero de forma general, cuando exige que los Mediadores de Datos actuando como servicios de intermediación de datos se asegurarán en caso de insolvencia, de la continuidad razonable de la prestación de sus servicios de intermediación de datos y, cuando esos servicios de intermediación de datos incluyan el almacenamiento de datos, dispondrán de los mecanismos de garantía necesarios para que los Titulares de Datos y los Sujetos de los Datos puedan acceder a sus datos, transferirlos o recuperarlos y, cuando presten esos servicios de intermediación entre Sujetos de los Datos y Usuarios de Datos, para permitir que los Sujetos de los Datos ejerzan sus derechos[190].

Escenarios de brechas de datos personales

Cuando se plantee un Espacio de Datos, aquellos que traten datos de carácter personal deben plantearse distintos escenarios de brechas de datos. Este ejercicio de análisis ha de buscar una respuesta al menos a las siguientes cuestiones:

- Qué impacto personal y social puede tener una brecha de datos personales.
- Qué medidas de protección de datos se han implementado o deberían estar implementadas para minimizar el impacto para los Sujetos de los Datos y la sociedad en caso de que se produzca una brecha de datos personales.
- Qué medidas de contingencia deberían estar preparadas para cuando se produzca la brecha para también minimizar dicho impacto, para hacer frente a las obligaciones de notificación a las Autoridades de Control y a la comunicación a los Sujetos de los Datos.

En dicho análisis hay que tener en cuenta que el Espacio de Datos supone, como mínimo, un tratamiento que puede ser no solo a nivel nacional, sino europeo, y con implicaciones más allá del marco de la UE. Esto supone que hay que, a la hora de plantear escenarios de brechas, tener en cuenta:

- Quiebras del Estado de Derecho.
- Situaciones de emergencia nacional o internacional.

[189] Esquema Nacional de Seguridad establecido mediante Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
[190] Artículo 12.h) de la DGA

- Crisis en la relaciones y acuerdo internacionales.

Por la relación con tiene con los Espacios de Datos, se recomienda consultar las Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales.

Reidentificación

Para finalizar, y aunque se trata en el apartado de anonimización, hay que destacar que la reidentificación se considera una brecha de datos personales.

En particular, el Reutilizador de Datos Protegidos del sector público deberá notificar al organismo del sector público que le dio acceso sobre toda brecha que permita la reidentificación de Sujetos de los Datos en conjuntos de datos no personales[191].

Cooperación entre intervinientes

El responsable del tratamiento puede recibir asistencia de terceros para ejecutar sus obligaciones. Ya el artículo 28.3.f del RGPD establece la obligación de los encargados de realizar esa asistencia cuando proceda. En concreto, el RGPD establece que el encargado "*ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado*". Además, en el Considerando 78 del RGPD se expone que "*Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos*".

La complejidad del entorno de los Espacios de Datos, en el que puede haber varios ámbitos de responsabilidad, hacen imprescindible una colaboración entre todos los intervinientes a la hora de gestionar los riesgos que supone un tratamiento de datos personales, ya sean responsables, corresponsables, encargados, subencargados o suministradores de tecnologías. Una eficaz y eficiente protección de datos va a exigir un esfuerzo coordinado para plantear y seleccionar los escenarios de implementación de casos de uso orientados a la protección de datos desde el diseño y una aproximación combinada a la solución que dé cumplimiento al RGPD. La EIDP y las soluciones que gestionen las limitaciones y los riesgos a los derechos y libertades han de surgir de un trabajo común y el resultado ha de ser único.

Dicha cooperación ha de producirse en la implementación y gestión de las medidas de gobernanza, políticas, estrategias de protección de datos desde el diseño y por defecto, medidas de seguridad, gestión de brechas, etc., destinadas a la gestión del riesgo para los derechos y libertades.

[191] Artículo 5.5 de la DGA

Como se ha señalado anteriormente, es fundamental que existan Habilitadores de protección de datos (labor que podría realizar un mismo Mediador de Datos) para coordinar y dar soporte jurídico, organizativo y técnico a los intervinientes en un tratamiento que se platee en el marco del Espacio de Datos. Esta figura será vital para cumplir el propósito que justifica la finalidad de un tratamiento de datos personales en el marco de un Espacio de Datos, como es el que el aprovechamiento de los mismos esté a disposición de la sociedad, prestando especial atención a la posición que tienen las PYMES, emprendedores y pequeños grupos de investigación.

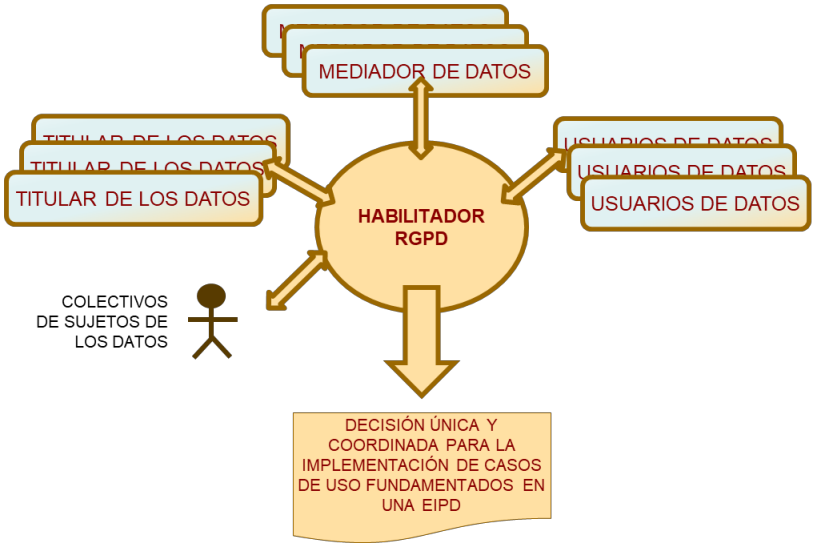

Figura 25: Papel de un Habilitador de protección de datos para la coordinación y soporte jurídico, organizativo y técnico a los diferentes intervinientes en un tratamiento que se platee en el marco del Espacio de Datos

Escenarios con relación a la ejecución de la EIPD

El conjunto de escenarios en los que se puede plantear la realización de una EIPD con una colaboración entre los intervinientes podrá ser tan amplia como los escenarios de tratamientos de datos que se planteen en el marco del Espacio de Datos y tendrán que tener en cuenta de forma específica los roles de responsable, o corresponsable, o encargado, o subencargado o proveedor tecnológico sin acceso a datos que adopte cada uno de los intervinientes en el tratamiento.

Por lo tanto, no se plantea realizar una relación exhaustiva de los mismos, ni valoración de otros requisitos como la legitimación para realizar el tratamiento, sino mostrar algunos ejemplos de cómo se podría plantear dicha colaboración a la hora de realizar la EIPD:

> Ejemplo 1
>
> Un Mediador de Datos se plantea para construir un repositorio con información anonimizada recogida de múltiples Titulares de Datos. En ese caso, cada Titular de Datos deberá hacer un análisis de riesgos del tratamiento de anonimización, y, en su caso, una EIPD. El Mediador, a su vez, deberá hacer un análisis de riesgos de la consolidación de varias fuentes anonimizadas en función de las características de los datos anónimos, su diversidad, su volumen, y el posible tratamiento de

reidentificación, y, en su caso, una EIPD. En la ejecución de dicha EIPD, de la que deberían concluirse recomendaciones de como ejecutar la anonimización, y concluir que hay una estrategia que permita realizarla con garantías y calidad suficiente, el Mediador y los Titulares deberán trabajar en coordinadamente para extraer las conclusiones.

Ejemplo 2

Un Usuario de Datos desea realizar un tratamiento sobre datos en posesión de un Mediador de Datos que actúa como responsable del tratamiento y que se puede llevar a cabo mediante anonimización. Este Mediador va a realizar un tratamiento de anonimización previamente antes de cederlos al Usuario de Datos. En ese caso, el Mediador de Datos ha de realizar la gestión del riesgo, y en su caso, de la EIPD del tratamiento de anonimización. Esta evaluación ha de realizarse en coordinación con el Usuario de Datos, tanto para determinar sus requisitos de calidad de datos o que de la posibilidad de reidentificación que podría existir por otras fuentes de datos a las que accede el Usuario.

Ejemplo 3

El Usuario de Datos solicita realizar un tratamiento sobre datos no anonimizados que un Mediador ya tiene disponibles, para los que el Mediador actúa como responsable del tratamiento y sobre los que el éste va a habilitar la ejecución en un Entorno de Tratamiento Seguro para que el Usuario de Datos extraiga únicamente información que no es de carácter personal.

El Mediador de Datos ha de realizar la gestión del riesgo, y en su caso, de la EIPD del tratamiento en el ámbito de sus obligaciones en el tratamiento de habilitar un conjunto de datos no anonimizados. El Usuario de Datos también ha de realizar la gestión del riesgo y la EIPD del tratamiento en su área de responsabilidad ya que, aunque se realice el proceso en un Entorno de Tratamiento Seguro del Mediador, el Usuario tiene su parte de responsabilidad en el mismo. Ambas han de estar coordinadas con relación a las garantías que se establecen en el Entorno de Tratamiento Seguro, la posibilidad de acceso remoto a dicho entrono de tratamiento seguro, los tratamientos realizados en el mismo y el procedimiento de extracción de resultados.

Ejemplo 4

El Usuario de Datos solicita realizar un tratamiento sobre datos no anonimizados que el Mediador no tiene físicamente en sus sistemas, pero catalogado que están en manos de varios Titulares de los Datos. El Mediador puede gestionar el acceso a Entornos de Tratamiento Seguro en los Titulares de los Datos para poder implementar el tratamiento solicitado utilizando estrategias de protección de datos desde el diseño y que permita extraer información anonimizada.

Los Titulares de Datos, como responsables, han de realizar la gestión del riesgo, y en su caso, de la EIPD del tratamiento en el ámbito de sus obligaciones en el tratamiento. El Mediador de Datos tomaría el rol de Habilitador, al menos en la tarea de servir de puente entre Titulares de Datos y Usuarios de Datos, y el Usuario de Datos ha de realizar la gestión del riesgo y la EIPD del tratamiento en su área de responsabilidad. La evaluación del riesgo y las medidas adoptadas no pueden llevarse a cabo de forma eficiente sin una colaboración entre Titulares, Mediador y Usuario, por lo tanto, en la ejecución de la gestión del riesgo han de actuar de forma coordinada, posiblemente ayudados por un tercero o con el liderazgo del Mediador en su papel de Habilitador.

Revisión y actualización de las medidas

El artículo 24 del RGPD establece la necesidad de la revisión y actualización de las medidas[192] cuando estas condiciones cambien, pues las medidas adoptadas han de ser las adecuadas para garantizar y poder demostrar el cumplimiento. En un Espacio de Datos los elementos que conforman los tratamientos ejecutados (naturaleza, extensión, contexto y fines) van a cambiar de forma muy dinámica, de igual forma que los riesgos para los derechos y libertades que se derivan de ellos. Por lo tanto, en la gobernanza del Espacio de Datos han de establecerse los mecanismos para ejecutar la revisión y actualización de medidas, en particular, con relación a los riesgos de reidentificación y la necesidad de reanonimización de conjuntos de datos.

El artículo 32.1.d del RGPD va más allá de esa obligación de revisión de las medidas de seguridad, exige revisiones regulares. Debido al riesgo de estos entornos, se recomienda realizar las revisiones con una periodicidad anual, pudiendo aumentarse la frecuencia de las revisiones tras la realización de la EIPD para los distintos casos de uso en el Espacio de Datos, si con ello se reduce el riesgo.

Recursos y transparencia

La AEPD ha publicado números recursos para la gestión del riesgo para los derechos y libertades, así como para la ejecución de proceso de evaluación de impacto para la protección de datos que se pueden encontrar en el portal web de la AEPD.

Hacer públicos los resultados de la EIPD es una buena medida de transparencia para aumentar la confianza en los tratamientos efectuados en el marco de los Espacios de Datos[193].

C. RELACIONES ENTRE LOS INTERVINIENTES EN EL ESPACIO DE DATOS

En el Capítulo IV de este documento se trató sobre las categorías de intervinientes en el Espacio de Datos, así como sobre las responsabilidades en los tratamientos. En este apartado se desarrollarán otros aspectos sobre las relaciones entre los intervinientes en el Espacio de datos.

[192] Artículo del blog de AEPD titulado "Cuándo hay que revisar las medidas de protección de datos [febrero 2023]"
[193] Párrafo 27 de la "*Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]*"

Formalización de los tratamientos entre intervinientes

Además de las obligaciones establecidas en el RGPD para la formalización mediante un contrato u otro acto jurídico de las relaciones responsable-encargado-subencargado cumpliendo todos los requisitos del artículo 28 del RGPD, hay que formalizar también las relaciones de comunicación de datos entre responsables y, en su caso, las situaciones de corresponsabilidad[194].

Esta formalización debería formar parte de los recursos de gobernanza en el Espacio de Datos y en dichos acuerdos es recomendable establecer:

- La facilitación de herramientas de anonimización/ seudonimización a los Titulares de los Datos, ya sea a través de Habilitadores, o con recursos propios.
- La facilitación de herramientas de trazabilidad y registro en el uso de los datos.
- La facilitación de herramientas de notificación a los Sujetos de los Datos o Interesados en los casos en los que se usen sus datos personales ya sea a través de Habilitadores, o con recursos propios de Mediadores o Usuarios de los Datos.
- Cláusulas para establecer de manera coordinada diligentes medidas de seguridad para el acceso y la transferencia de datos.
- Y otros aspectos que implementen políticas comunes de protección de datos[195].

Por su importancia, hay que destacar la importancia de las medidas jurídicas que van más allá de los mínimos obligados en la normativa de protección de datos para la gestión de riesgos en la difusión de datos personales y anonimizados y que pueden formar parte de la formalización de las relaciones entre intervinientes. Entre ellas, limitar por contrato el ámbito de difusión de los datos anonimizados (por ejemplo, sólo entre un grupo de investigadores) o establecer requisitos y limitaciones de conservación, que son el tipo de garantías comunes para reducir otra clase de riesgos en datos no personales.

Estas garantías se pueden plasmar en las licencias de uso en los Espacios de Datos.

Procedimiento de acceso al Espacio de Datos cuando se traten datos personales

El tratamiento de datos personales en el marco de un Espacio de Datos tiene que estar autorizado, procedimentado y supervisado por aquellos que son responsables RGPD de los datos que se pretenden tratar. La responsabilidad en sí no se puede delegar, pero sí puede estar apoyada en un juicio competente, que en este caso podría ser el del Supervisor de las solicitudes de acceso al Espacio de Datos.

El procedimiento que se plantee tendría que estar reflejado en la gobernanza del Espacio de Datos y debería tener las garantías suficientes como, por ejemplo, estar apropiadamente documentado, motivado, con referencias a la base jurídica, la información que precisa conseguir que justifique el acceso a determinados datos y todos los requisitos de cumplimiento del RGPD. El procedimiento debería incluir los pasos necesarios para definir, en cooperación entre el Usuario con Mediadores y Titulares de los Datos si fuera el caso, las medidas de protección de datos desde el diseño, las limitaciones

[194] Artículo 26 del RGPD
[195] Artículo 24.2 del RGPD, no confundir con políticas de privacidad.

en el tratamiento, la gestión del riesgo, la probabilidad de reidentificación de datos personales, la gestión de posibles brechas, los controles y auditorías de cumplimiento, la formalización de las relaciones entre los intervinientes, etc., hasta obtener una definición precisa del tratamiento. Todo ello también daría soporte a la elaboración de una eventual EIPD.

Supervisión humana en la decisión de acceso a datos personales

En la propuesta de la DA se contempla la posibilidad de dar acceso a datos en Espacios de Datos mediante el empleo de "*Smart contracts*" o contratos establecidos en algoritmos y de ejecución automática[196] con ciertas garantías: mecanismos de control de acceso rigurosos, limitación del periodo de validez del contrato y capacidad de interrupción, transparencia y la misma tutela judicial efectiva que cualquier otro contrato.

Por otro lado, la DGA, para el caso de los puntos de información único que permitan la reutilización de categorías específicas de datos que obren en poder de organismos del sector público, aun cuando debe poder contar con medios automatizados cuando transmita consultas o solicitudes de reutilización, debe garantizarse una supervisión humana suficiente en el proceso de transmisión[197].

Con relación a protección de datos, la decisión de dar acceso de forma genérica, o comunicar, datos personales a terceros podría tener consecuencias jurídicas para los Interesados o afectarles de forma similar. En ese caso, habría que estudiar si una decisión totalmente automatizada podría estar contraviniendo el establecido en el artículo 22 del RGPD. Por otro lado, en determinados casos y para determinados tipos de Usuarios de Datos deberían existir procedimientos para conceder acceso automático una vez evaluados inicialmente, con el condicionante de establecer un monitoreo y control periódico de los accesos realizados, por ejemplo, para el uso primario de datos en el marco de los Espacios de Datos Sanitarios.

Independientemente de lo anterior, también sería necesario determinar el riesgo que para los derechos y libertades podría tener el dar acceso a datos personales a terceros de forma automática, entre otros aspectos, por los posibles errores en los "*Smart contracts*"[198].

Interoperabilidad

El Capítulo VIII de la propuesta de DA está orientado a definir los requisitos mínimos de interoperabilidad en los Espacios de Datos. La obligación de interoperabilidad también se establece en la DGA en los Mediadores de su competencia[199].

La interoperabilidad tiene un papel fundamental en la implementación correcta de medidas para el cumplimiento del RGPD. Una interoperabilidad mal definida o que no

[196] Artículo 30 de la propuesta de DA.
[197] Considerando 26 de la DGA
[198] Como todo algoritmo, tiene una probabilidad de error o simplemente sufrir un diseño defectuoso: AkuDreams dev team locks up $33M due to smart contract bug (cointelegraph.com)
[199] Si se trata de servicios de intermediación de datos, se aplica el artículo 12.i) de la DGA y para las organizaciones reconocidas de gestión de datos cedidos con fines altruistas el 21.1.d.

contemple los requisitos de protección de datos no podría implementar apropiadamente las soluciones de protección de datos desde el diseño o por defecto ni los principios de protección de datos, en particular, la gestión del consentimiento, el ejercicio de derechos, la trazabilidad de conjuntos de datos y de datos personales, la implementación de estrategias "*compute-to-data*", la aplicación eficiente de Entornos de Tratamiento Seguro, etc.

La falta de interoperabilidad en la implementación de un Espacios de Datos afectará al cumplimiento de las finalidades de los tratamientos planteados en el marco de dicho Espacio. En ese caso, sería necesario replantearse si se siguen cumpliendo los requisitos de idoneidad y de necesidad de los tratamientos.

Interacción entre Mediadores

En algunos casos puede haber más de un Mediador de Datos involucrado en el tratamiento que desea plantear un Usuario de Datos. Incluso que dichos Mediadores estén actuando en el marco de distintos Espacios de Datos. La interacción entre Mediadores, o entre varios Mediadores y un Usuario de Datos tiene que contemplar otros aspectos más allá de los de interoperabilidad técnica.

Los mecanismos de gobernanza, partiendo desde la figura del Supervisor de las solicitudes de acceso, deben contemplar la implementación de medidas de privacidad desde el diseño y también de gestión del riesgo para los derechos y libertades, así como en su caso la realización de la EIPD, en particular con relación a la probabilidad de reidentificación.

Por ejemplo, la decisión de incluir un determinado conjunto de datos en una respuesta puede ser tomada por un Mediador de datos, pero los datos en sí pueden ser controlados por un Mediador diferente. En tales casos, los Mediadores de Datos tienen que cooperar en el marco de sus responsabilidades para dar respuesta a la solicitud de datos, lo que implica mecanismos de gobernanza, de gestión (en particular del riesgo para los derechos y libertades de los Sujetos de los Datos) y técnicos[200].

Selección de encargados/subencargados en el Espacio de Datos

La selección de encargados/subencargados del tratamiento forma parte de la naturaleza del tratamiento, es decir, la forma en la que éste se implementará. El responsable tendrá la obligación de que se sigan los principios de responsabilidad proactiva o "*accountability*", de protección de datos desde el diseño y de gestión del riesgo para los derechos y libertades en el proceso de selección de encargados y subencargados de tratamiento. En la selección de encargados/subencargados en el Espacio de Datos se precisa de un análisis en el contexto de las especiales características del mismo.

Hay que tener en cuenta que el recurso a un encargado de tratamiento no supone un desvío de obligaciones del responsable del tratamiento a un tercero. Más bien al contrario, se añaden obligaciones muy concretas para el responsable, como la obligación a recurrir

[200] Apartado 4.3.2 del documento "*ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023]*".

únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento[201], la necesaria diligencia en su selección y, como forma parte de la naturaleza del tratamiento, y la de gestionar el riesgo específico que puede suponer la selección de distintos encargados. Hay que recordar que la documentación de dicha diligencia forma parte de las obligaciones de responsabilidad proactiva.

En particular, se exige un cumplimiento de las condiciones enumeradas en el artículo 28.3 del RGPD y, entre ellas, la de la letra 28.3.h: "*pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*". Además del requisito del artículo 28, el encargado ha de permitir de forma efectiva el ejercicio de los poderes que el artículo 58.1 otorga a las Autoridades de Control en cuanto a sus poderes de investigación, que no pueden quedar vacíos de contenido de forma efectiva.

La selección de encargados/subencargados ha de estar orientada a cumplir las finalidades del Espacio de Datos y no debería ser una forma de circunvalar las garantías y medidas que se exigirán al Mediador de Datos y a los Usuarios de los Datos para garantizar un cumplimiento real de los principios de protección de datos.

Guardianes de Acceso

La normativa de la Unión Europea, en particular en la DMA y la propuesta de DA, ha identificado una figura que denomina Guardianes de Acceso[202]. Los Guardianes de Acceso, con relación a los Espacios de Datos, son, entre otros, aquellos que dan servicio de computación en la nube[203] empleando economías de escala extremas, con efectos de red muy potentes, gran capacidad de conectividad entre usuarios, creando un importante grado de dependencia que pueden socavar la disputabilidad de los servicios y por tanto la equidad de la relación comercial[204]. Algunas de las empresas consideradas Guardianes de Acceso controlan ecosistemas completos de plataformas en la economía digital y aumentan la posibilidad de que los mercados subyacentes puedan no funcionar bien[205]. Los Guardines de Acceso tienen costes marginales nulos a la hora de añadir usuarios y proporcionan soluciones integradas para la implementación y explotación de *data lakes* que incluyen desde herramientas para la carga de datos en tiempo real de sistemas IoT[206], pasando por múltiples soluciones de extracción, transformación, catalogación, presentación, etc., y llegando al procesado con herramientas de inteligencia artificial y biométricas predefinidas.

[201] Considerando 81 del RGPD.
[202] Definición en el artículo 2.1) de la DMA
[203] La DMA aplica la definición de Guardián de Acceso a otros servicios más allá de la computación en la nube, pero en este texto nos centraremos en estos últimos.
[204] Considerando 2 de la DMA
[205] Considerando 3 de la DMA
[206] *Internet of Things*

La DMA regula la actuación de los Guardianes de Acceso desde el punto de vista de cómo pueden afectar en el detrimento de los precios, la calidad, la competencia leal, las opciones y la innovación en el sector digital[207], estableciendo normas para garantizar la disputabilidad y la equidad de los mercados en el sector digital[208]. En la propuesta de DA se manifiesta en el Considerando 36 que "*la inclusión de dichas empresas guardianas de acceso como beneficiarias del derecho de acceso a los datos no sería necesaria para alcanzar el objetivo del presente Reglamento y, por tanto, sería desproporcionada en relación con los titulares de datos sujetos a dichas obligaciones. Esto significa que una empresa que presta servicios básicos de plataforma que ha sido designada como guardián de acceso no puede solicitar ni obtener acceso a los datos de los usuarios generados por el uso de un producto o servicio relacionado o por un asistente virtual sobre la base de las disposiciones del capítulo II del presente Reglamento. Debe entenderse que una empresa que presta servicios básicos de plataforma designada como guardián de acceso con arreglo a la Ley de Mercados Digitales incluye a todas las entidades jurídicas de un grupo de empresas en el que una entidad jurídica presta un servicio básico de plataforma. Además, los terceros a los que se faciliten datos a petición del usuario no podrán poner los datos a disposición de un guardián de acceso designado. Por ejemplo, el tercero no puede subcontratar la prestación de servicios a un guardián de acceso. Sin embargo, esto no impide que terceros utilicen servicios de tratamiento de datos ofrecidos por un guardián de acceso designado. Esta exclusión de los guardianes de acceso designados del ámbito de aplicación del derecho de acceso en virtud del presente Reglamento no impide a estas empresas obtener datos por otros medios legales.*"

Con relación al desarrollo de una normativa digital que regula el equilibrio del mercado entre las PYMES y los Guardianes de Acceso, también habría que preguntarse el efecto que pueden tener dichos Guardianes de Acceso en el marco de los Espacios de Datos con relación al cumplimiento de los principios, derechos y obligaciones del RGPD. En ese sentido el SEPD ha manifestado que *"el tratamiento de datos para el bien público no debe crear ni reforzar situaciones de oligopolio de datos (dependencia del sector público, PYME, etc., en unas pocas empresas poderosas de TI, las llamadas Big Tech). Esto también es relevante desde una perspectiva de protección de datos, ya que los monopolios y oligopolios crean situaciones de bloqueo de los usuarios y, en última instancia, restringen la posibilidad de que las personas ejerzan efectivamente sus derechos."*[209]

Impacto de los Guardianes de Acceso en las medidas de protección de datos

Por ejemplo, sea un caso de que se quieren implementar garantías tanto jurídicas, como organizativas y técnicas para el tratamiento de datos de alto impacto (p.ej. sanitarios[210]) en un Espacio de Datos que incluya seudonimización. Para ello se podría exigir a los Titulares de los Datos que se dispusiera de un espacio ad-hoc para extraer la información a compartir, distinto de donde se almacena la información para explotación. En ese espacio ad-hoc, la información seleccionada sería accesible a un Mediador que

[207] Considerando 4 de la DMA
[208] Considerando 7 de la DMA
[209] Párrafo 26 de la "*Opinion 3/2020 on the European strategy for data (EDPS) [16 June 2020]*"
[210] Sea el caso de la implementación del Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia

realizaría la seudonimización y que guardaría la información adicional de reidentificación. Cuando un Usuario de Datos necesite la información para un caso de uso concreto, el Mediador hará una extracción del conjunto de datos, los cederá al Usuario de Datos en un Entorno de Tratamiento Seguro, conforme a lo establecido en el considerando 54 del EHDS en el marco de un uso secundario de los datos, para su tratamiento.

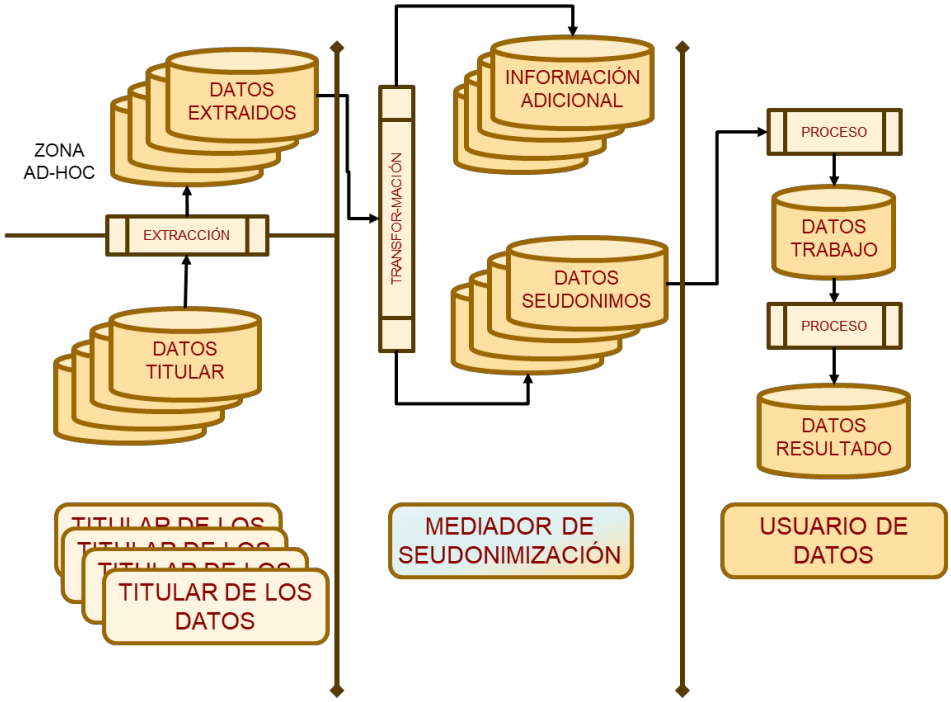

Figura 26: Esquema de implementación de garantías de seudonimización por separación física de los intervinientes.

En el esquema anterior, se establece la separación física entre Titular y Mediador, y la independencia con los sistemas de los Usuarios de los Datos como una garantía adicional para la implementación de las garantías del RGPD.

Sin embargo, supongamos que todos los intervinientes seleccionan el mismo Guardián de Acceso como encargado de tratamiento (o subencargado dependiendo del rol de los intervinientes). En ese caso, gran parte de las medidas organizativas y técnicas podrían encontrarse comprometidas, y las jurídicas que obligan a los intervinientes perderían parte de su eficacia. Por ejemplo, las separaciones de datos entre intervinientes se diluirían pues de forma efectiva residirían en el mismo encargado, independientemente de las medidas de seguridad empleadas.

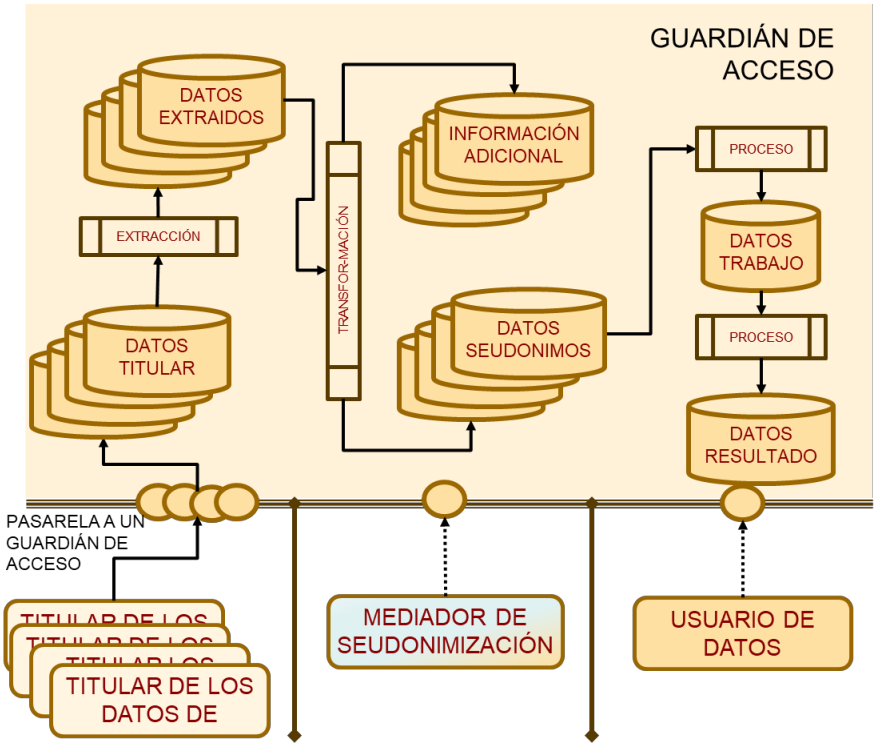

Figura 27: Esquema de implementación de garantías de seudonimización por separación física de los intervinientes cuando comparten el mismo Guardián de Acceso.

En la figura anterior, las garantías basadas en la separación física de la información de reidentificación, se podrían ver comprometidas cuando se implementen sobre Guardianes de Acceso. Por supuestos, estos estarán sujetos por garantías jurídicas[211], pero esas mismas son las que en el ejemplo inicial no se han considerado suficientes para los Mediadores o a los Usuarios de los Datos.

Esta situación puede generarse incluso cuando se distribuyen varios Espacios de Datos sobre los servicios de pocos Guardianes de Acceso.

[211] Establecidas en el Artículo 5.2.b de la DMA "combinar datos personales procedentes de los servicios básicos de plataforma pertinentes con datos personales procedentes de cualesquiera servicios básicos de plataforma adicionales o de cualquier otro servicio que proporcione el guardián de acceso o con datos personales procedentes de servicios de terceros"

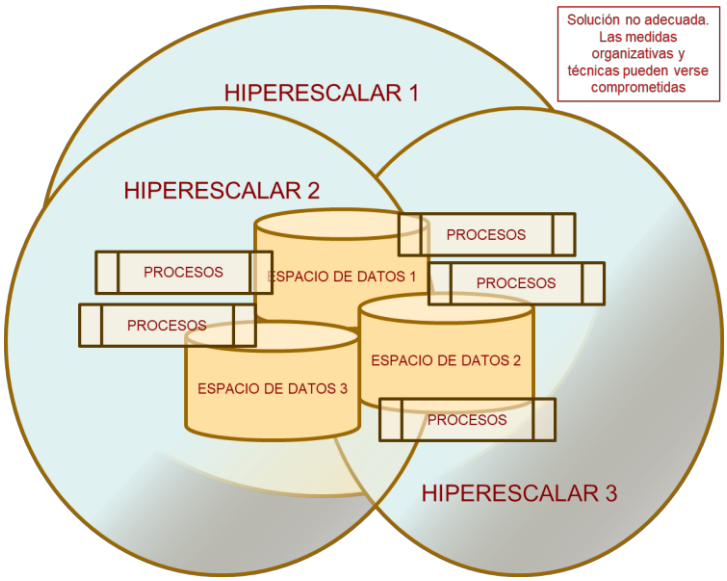

Figura 28: Distribución de varios Espacios de Datos sobre los servicios de pocos Guardianes de Acceso

Por otro lado, una implementación como la señalada podría conducir a una federación de *datalakes* antes que a un Espacio de Datos.

La gestión del riesgo en la selección de encargados/subencargados

Una de las principales virtudes del RGPD es su flexibilidad a la hora de adaptarse a nuevos contextos tecnológicos, pues el principio de responsabilidad proactiva exige a los responsables ir más allá del cumplimiento de los mínimos directamente exigibles en el texto de la norma y condicionar el tratamiento a una adecuada gestión de los riesgos para los derechos y libertades de los Sujetos de los Datos.

Con relación a la selección de encargados/subencargados, y en particular los Guardianes de Acceso, además de la posible pérdida de la efectividad de ciertas garantías, podríamos encontrarnos ante nuevos riesgos. Dichos riesgos pueden surgir por una mayor concentración de datos, por el impacto masivo de las potenciales brechas de datos personales, el sometimiento a regulaciones de terceros países y a una menor capacidad de exigencia y de capacidad de control por parte de responsables y de las Autoridad de Control (p. ej. a la hora de acceder a la información de trazabilidad o la imposibilidad de aceptar o rechazar a subencargados de tratamiento). A esto hay que añadir los riesgos a la disponibilidad y resiliencia que pueden suponer los cambios unilaterales en las condiciones de servicio, la oferta *best-effort*[212] en las condiciones de calidad de servicio, la modificación y discontinuidad de servicios siguiendo políticas que no se adecuan a las necesidades de los responsables, la actuación ejecutiva de autoridades de terceros países[213], la retirada de servicio por eventos geopolíticos[214], etc.

Todos estos riesgos han de evaluarse y, como recomendación general para disminuir el riesgo, se aconseja que se límite al máximo posible el recurso a encargados de tratamiento

[212] La no existencia de garantías reales de niveles de disponibilidad.
[213] Recordamos el caso Megaupload
[214] Companies pulling back from Russia over the war in Ukraine | CNN Business

para el almacenamiento o tráfico masivo de los datos personales no anonimizados (ver también la recomendación de realizar un análisis de reidentificación cuando se acumulen en un mediador muchos conjuntos de datos anonimizados). El nivel de riesgo del empleo de encargados de tratamientos probablemente irá *in crescendo* cuando:

- Se recurra a un encargado que preste servicios exclusivamente para dicho Espacio de Datos.
- Se recurra a un encargado que preste servicios a varios Espacio de Datos, pero de forma exclusiva para Espacios de Datos.
- Se recurra a un encargado que preste servicios a un único Espacio de Datos y proporcione otros servicios TIC a su cuenta o como encargado de terceros.
- Se recurra a un encargado que preste servicios a múltiples Espacio de Datos y proporcione otros servicios TIC a su cuenta o como encargado de terceros.

En estos tres últimos casos, en los que el impacto de los riesgos anteriormente citados serían mayores, y que son comunes a las nubes públicas o Guardianes de Acceso, se consideran de un alto nivel de riesgo (ver apartado "VI.B. Gestión del riesgo y evaluación de impacto para la protección de datos - Alto riesgo") que es muy difícil de mitigar. En estos casos hay que plantearse que es muy probable que se requerirá una consulta previa a la autoridad de protección de datos[215].

D. TRAZABILIDAD, TRANSPARENCIA Y EJERCICIO DE DERECHOS

La trazabilidad del dato es la capacidad de conocer todo el ciclo de vida del dato: la fecha y hora exacta de extracción, cuándo, dónde y por quién se produjo su transformación, y cuándo, dónde, por quién y con qué finalidad y legitimidad se cargó, se usó o se descargó desde un entorno a otro destino. A este proceso también se conoce como "*Data Linage*".

La trazabilidad puede cumplir propósitos ajenos a protección de datos, como implementar la monetización inherente a los Espacios de Datos, también para soportar el principio de soberanía de los Titulares de los Datos, u otros requisitos de control de la propiedad intelectual, industrial, perfeccionamiento de contratos, información al Interesado o Sujeto de los Datos de los resultados del tratamiento de los mismos[216], etc.

Trazabilidad para la protección de datos

Trasladando las conclusiones de ENISA, "*En la era del Big Data, los mecanismos "tradicionales" de información y consentimiento no proporcionan la transparencia y el control adecuados*"[217] para los Usuarios de los Datos. Hay que recordar que uno de los cuatro pilares de la Estrategia Europea de Datos[218] es apoyar "*a las personas en el ejercicio de sus derechos en relación con el uso de los datos que ellas mismas generan. Se les puede*

[215] Artículo 36.1 del RGPD

[216] El Considerando 44 de la propuesta de EHDS cita "*Las personas físicas deben poder acceder a los resultados de los distintos proyectos de investigación en el sitio web del organismo de acceso a los datos sanitarios, idealmente mediante una búsqueda fácil de realizar*""

[217] Conclusiones del documento de ENISA "*Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics European Union Agency for Cybersecurity (ENISA) [17 December 2015]*".

[218] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos (COM(2020) 66 final) [19 de febrero de 2020]

empoderar para que tengan el control sobre sus datos a través de herramientas y medios que les permitan decidir a un nivel más detallado sobre lo que se hace con sus datos («espacios de datos personales»)".

Con el propósito de adecuar los mecanismos de control a la realidad de los tratamientos en el marco de los Espacios de datos, la trazabilidad de los datos podría cumplir con los siguientes objetivos desde el punto de vista del RGPD:

- Cumplir con los requisitos de transparencia a los interesados del RGPD.
- Permitir el ejercicio efectivo de los derechos de los interesados, en particular, la gestión del consentimiento.
- Permitir ejercer las obligaciones del responsable del tratamiento (p.ej. para que garantice los principios de limitación de tratamiento, las finalidades ajustadas a las bases jurídicas o el control de encargados/subencargados de tratamiento).
- Permitir a las Autoridades de Control ejercer sus poderes de acuerdo con el artículo 58.1 del RGPD.

Estos objetivos son complementarios pero distintos, y la información que es necesario recoger para habilitar el pleno ejercicio de estas funciones variará, por ejemplo, entre la que es necesario poner a disposición del Interesado o Sujeto de los Datos, de aquella que se ha de poner a disposición de las Autoridades de Control.

La trazabilidad de los datos exige identificar roles e implementar políticas de control de acceso y de registro de acceso. En el caso de los Espacios de Datos, por su especial naturaleza, la habilitación de acceso ha de establecer políticas de control y registro de acceso que permitan la trazabilidad a nivel de persona usuario individual, y no solo a nivel de organizaciones o departamentos[219]. El mantenimiento de un registro de los accesos, así como de las acciones realizadas durante el acceso al Espacio de Datos se recomienda tanto para poder cumplir los objetivos anteriores como para implementar las obligaciones del artículo 32 del RGPD , cumplir las obligaciones de los servicios de intermediación de datos[220] o las obligaciones de transparencia las organizaciones reconocidas de gestión de datos con fines altruistas[221]. Por ejemplo, estas últimas estarán obligadas a llevar un registro completo y exacto de:

- todas las personas físicas o jurídicas a las que se haya permitido tratar datos que obren en poder de dicha organización reconocida de gestión de datos con fines altruistas, y sus datos de contacto;
- la fecha o la duración del tratamiento de los datos personales o la utilización de los datos no personales;
- la finalidad del tratamiento de datos declarada por las personas físicas o jurídicas a las que se haya permitido dicho tratamiento;

[219] Por ejemplo, en la propuesta de EHDS, en el Artículo 37 "Funciones de los organismos de acceso a los datos sanitarios" en la letra k se propone "k) mantener un sistema de gestión para registrar y tramitar las solicitudes de acceso a los datos, las peticiones de datos y los permisos de datos expedidos y las peticiones de datos atendidas, facilitando al menos información sobre el nombre del solicitante de datos, la finalidad del acceso, la fecha de expedición, la duración del permiso de datos y una descripción de la solicitud o de la petición de datos".

[220] Artículo 12.o) de la DGA.

[221] Artículo 20.1 de la DGA

- las eventuales tasas abonadas por las personas físicas o jurídicas que efectúen el tratamiento de datos.

Trazabilidad de los conjuntos de datos

La disponibilidad de mecanismos de trazabilidad en los conjuntos de datos constituye una medida de gestión de la protección de datos relacionados con la trazabilidad de los propios datos personales.

En la protección de los derechos de autor se han utilizado diversas técnicas, como las marcas de agua o huellas digitales, para poder detectar y la difusión ilícita de contenido digital. El empleo de estas técnicas precede a la digitalización de la información y pueden ser utilizadas a nivel de conjunto de datos o a nivel de elementos dentro del conjunto de datos. Aunque en el mundo digital se han empleado fundamentalmente para controlar la difusión de contenidos de audio, video, circuitos integrados, etc., aunque también hay desarrollos específicos para bases de datos[222].

En el caso de que en el Espacio de Datos se planteen tratamientos en los que sea imprescindible la difusión de datos personales podría resultar de gran interés plantear sistemas de gestión de la trazabilidad de la difusión de los datos que incluyesen marcas de agua o huellas digitales.

Transparencia

Con relación a la transparencia a los Sujetos de los Datos, el RGPD establece unas obligaciones mínimas en su Capítulo III. El Titular de Datos deberá ejecutar las obligaciones de transparencia y ejercicio de derechos a los Sujetos de los Datos y ejecutar las obligaciones de información a los mismos de manera previa a la realización de cualquier tratamiento ulterior[223]. Sin embargo, estas obligaciones se pueden ampliar en los casos en los que los mecanismos de transparencia constituyan una medida adecuada para mitigar el alto riesgo con el que nos encontramos en el marco de un Espacio de Datos o bien como garantía para realizar el análisis de la compatibilidad de fines.

En los casos en los que haya comunicación de datos a terceros, éstos han de informar a los Sujetos de los Datos cumpliendo con lo recogido en el artículo 14 del RGPD sobre "*Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado*". Las obligaciones de información cuando los datos personales no se hayan obtenido del interesado pueden entrar dentro de excepciones establecidas en el artículo 14.5 del RGPD. Sin embargo, el Espacio de Datos ha de diseñarse para que no se entre en el supuesto del artículo 14.5.b del RGPD de forma sistemática simplemente porque no se ha tenido en cuenta desde el diseño la necesidad del cumplimiento de estas obligaciones en la medida de lo técnicamente posible.

En el caso de servicios de intermediación de datos, cuando ofrezcan servicios a los Sujetos de los Datos les informarán y, cuando corresponda, asesorarán de manera concisa, transparente, inteligible y fácilmente accesible sobre los usos previstos de los

[222] CiteSeerX (psu.edu)
[223] Artículo 13.3 del RGPD

datos por los Usuarios de Datos y las condiciones generales aplicables a dichos usos antes de que los Sujetos de los Datos presten su consentimiento[224]. En el caso de las organizaciones reconocidas como de gestión de datos con fines altruistas, estas informarán a los interesados o a los Titulares de Datos, de una manera clara y sencilla de entender, antes de cualquier tratamiento de sus datos con las condiciones del Artículo 21 de la DGA.

En el marco del Espacio de Datos, las condiciones para permitir tratamientos adicionales sobre los datos personales deben ser públicas[225]. Los Mediadores de Datos y los Habilitadores, con relación a los Usuarios de los Datos, podrán facilitar herramientas que sirvan para ejercer este principio de transparencia. Cabe plantear que, en el caso de comunicaciones a Usuarios de los Datos, exista un contrato de encargo para este tratamiento específico entre el Usuario de Datos como responsable y el Mediador del Espacio de Datos, que actuaría en este caso como encargado.

Inventario de actividades de tratamiento

Igualmente, con relación a los tratamientos en el marco del Espacio de Datos, los sujetos enumerados en el artículo 77.1 de la LOPDGDD, en particular las Administraciones Públicas, tienen la obligación de hacer público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del RGPD y su base legal.

Ejercicio de los derechos

En el marco del Espacio de Datos, el Sujeto de los Datos ha de tener la posibilidad de ejercer su oposición cuando el tratamiento se basa en el interés legítimo[226] o el interés público[227] y el resto de los derechos establecidos en el RGPD. Además, en el caso de servicios de intermediación de datos, podrán oponerse a que sus datos sean convertidos a otro formato (lo que es en sí un tratamiento), y se les tiene que ofrecer la oportunidad de ello, a menos que el Derecho de la Unión obligue a realizar dicha conversión[228].

En caso de que los Titulares de los Datos sean AAPP, cobra especial relevancia el uso de la Carpeta Ciudadana como instrumento Habilitador al ser una herramienta adicional de transparencia. En esa medida, ha de contemplarse la mejora de las posibilidades de la Carpeta Ciudadana con relación a recibir información suficiente sobre la finalidad de nuevos tratamientos, facilitar canales de comunicación para resolver dudas o poder hacerse el consentimiento o el rechazo de alguna manera en los casos que se base en el consentimiento.

[224] Artículo 12.m) de la DGA
[225] Párrafo 19 de la "*Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]*"
[226] Artículo 21.1 del RGPD
[227] Excepto, como se establece en el artículo 21.6 del RGPD, cuando traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1 del RGPD
[228] Artículo 12.d) de la DGA.

Gestión del consentimiento

El Sujeto de los Datos o Interesado también ha de tener la posibilidad de dar su consentimiento, modificarlo o retirarlo al tratamiento de sus datos personales para otros fines diferentes a los legitimaron su tratamiento. Cuando el consentimiento sea la base legitimadora elegida para el tratamiento en un Espacio de Datos, este consentimiento debe ser una manifestación de voluntad libre, específica, informada e inequívoca. En concreto, deberá atenderse a lo exigido en el artículo 7 del RGPD que se desarrolla en los considerandos 32, 42 y 43 del RGPD y más detalladamente en las Directrices 5/2020 del CEPD. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno[229]. Dentro del perjuicio al Sujeto de los Datos está el de la presión social o emocional que se puede realizar en determinadas situaciones y contextos.

En particular y entre otros, la DGA se establece el marco para la cesión altruista de datos[230] tanto personales como de empresas. En el caso de datos personales, la cesión altruista de datos se fundamentaría en el consentimiento RGPD de los Sujetos de los Datos. Los Mediadores de Datos que ofrezcan servicios a los Sujetos de los Datos deberán informar y, cuando corresponda, asesorar de manera concisa, transparente, inteligible y fácilmente accesible sobre los usos previstos de los datos por los usuarios de datos y las condiciones generales aplicables a dichos usos antes de que los interesados presten su consentimiento[231]. También sería necesario especificar el territorio del tercer país en el que se pretenda usar los datos[232].

El Espacio de Datos deberá proporcionar herramientas para obtener el consentimiento de los Sujetos de los Datos como para retirar su consentimiento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada.

En la prestación del consentimiento será preciso determinar mecanismos para establecer la granularidad de dicho consentimiento, en cuanto a categorías de datos, categorías de tratamientos y categorías de destinatarios. La granularidad ha de permitir el poder expresar y respetar la voluntad y derechos de los sujetos de los datos[233]. A ese respecto, cabe plantearse la adopción de listas "blancas" como de listas "negras"[234] que permitan definir con precisión las preferencias que reflejan los valores morales o éticos de los Sujetos de los Datos.

Un consentimiento granular exige el establecimiento de recursos para su gestión en el Espacio de Datos y estos recursos han de definirse desde el diseño. Unos criterios de granularidad mal planteados pueden originar a futuros problemas para su aplicación, con dudas en su aplicación para casos concretos y falta de efectividad, de ahí la importancia de su buena definición desde el diseño del Espacio de Datos. También es importante

[229] Considerando 42 del RGPD
[230] Capítulo IV y Considerandos 50, 51 y 52 de la DGA
[231] Artículo 21.1 de la DGA.
[232] Artículo 21.6 de la DGA
[233] Párrafo 19 de la "*Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]*"
[234] Apartado 4.3.1 del documento "*ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023]*".

plantearse que, por mucho que se depuren los criterios, surgirán dudas sobre su aplicación en tratamientos concretos[235]. En esta circunstancia el Mediador, o quien actúe como responsable del tratamiento, podría recabar el asesoramiento del DPD, para incluir los datos o excluir los datos. Otras estrategias podrían ser el ponerse en contacto con el interesado para aclarar si los fines son compatibles o no, determinar si el interesado daría su consentimiento para el propósito particular del procesamiento en cuestión, o consultar a terceros pertinentes, como las autoridades de protección de datos. En el caso de la reutilización de datos personales en poder de organismos del sector público, no deben facilitarse datos de contacto que permitan a los reutilizadores dirigirse directamente a los Sujetos de los Datos[236].

El consentimiento, y en concreto la cesión altruista de datos, no supone la renuncia a los derechos fundamentales del sujeto de los datos ni exime del cumplimiento de principios, derechos y obligaciones por los responsables, sino únicamente supone una base legitimadora para el tratamiento de dichos datos. En particular, y como se ha señalado anteriormente, en el caso de que el tratamiento se haya basado en el consentimiento, solo podrán tratarse para un fin distinto si el responsable del tratamiento solicita un consentimiento específico para ese otro propósito o si el responsable del tratamiento puede demostrar que se basa en una ley de la Unión o de un Estado miembro para salvaguardar los objetivos mencionados en el artículo 23 del RGPD[237].

Por ello, cabe plantearse la necesidad de implementar un mecanismo ágil para gestionar un ciclo de vida en el consentimiento. Un Sujeto de Datos puede decidir, en cualquier momento, modificar arbitrariamente sus demandas de procesamiento de datos, o revocar el consentimiento para el procesamiento o restringir el procesamiento en ciertos usuarios de datos. Por lo tanto, un Mediador de datos también tiene que realizar un seguimiento permanente de las instancias de procesamiento en curso de los datos de cada Sujeto de Datos, para responder a un cambio de opinión de un sujeto de datos dentro de un período de tiempo razonable[238].

Finalmente, hay que señalar que el tratamiento lícito de los datos, incluso cuando se aplican medidas como la anonimización, podría no resolver todos los problemas éticos, como, por ejemplo, los relacionados con las objeciones personales a ciertas partes interesadas del sector privado (p.ej. farmacéutica, de seguros, etc.)[239].

E. CONSERVACIÓN DE DATOS PERSONALES Y LIMITACIÓN DEL TRATAMIENTO

De acuerdo con el principio de limitación del plazo de conservación[240] en el tratamiento de datos personales, los datos personales a los que se de acceso los intervinientes del Espacio de Datos serán mantenidos durante no más tiempo del necesario para los fines

[235] Apartado 4.3.1 del documento "*ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023]*"
[236] Considerando 15 de la DGA
[237] Párrafo 53 del documento "Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad (EDPB) [9 de marzo de 2021]"
[238] Apartado 4.1 del documento "*ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA). [January 2023]*".
[239] Párrafo 20 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*
[240] Recogido en el artículo 5.1.e) del RGPD.

del tratamiento. Los mecanismos de gobernanza deben permitir el establecimiento por el Supervisor de las Solicitudes de Acceso de periodos de conservación, así como la gestión de los mismos.

La aplicación de dicho principio, y el de limitación de la finalidad del tratamiento[241], hacen imprescindible implementar los mecanismos de trazabilidad antes señalados para comunicar y ejecutar las restricciones en el tratamiento de datos. La gestión incluye la posibilidad de una actualización de las condiciones de consentimiento o de limitación del tratamiento por el interesado, su ejecución por Mediadores y Usuarios, junto con una notificación activa dirigida al Interesado.

Los mecanismos de gobernanza del Espacio de Datos deberán establecer guías y herramientas para el cumplimiento de dichos principios, así como podrían ejecutarse revisiones o auditorías por parte de las las autoridades competentes para que el Espacio de Datos cumpla con la normativa de que se ha producido la ejecución efectiva de derechos de que se ha producido la ejecución efectiva de los derechos, herramientas automáticas que detecten o garanticen que no es posible una copia local de los datos en el Usuario de Datos para uso posterior, u otras.

F. ANONIMIZACIÓN Y REIDENTIFICACIÓN

El concepto de anonimización ha sido desarrollado por el Comité Europeo de Protección de Datos, por la Agencia Española de Protección de Datos y otras entidades en diversas guías, notas técnicas y herramientas[242]. A su vez, se ha abordado la anonimización en los casos de uso del capítulo anterior.

El Considerando 15 de la DGA manifiesta que, en el caso de reutilización de datos de organismos del sector público y que el acceso a datos personales se implemente mediante transmisión de éstos, los datos personales deben anonimizarse. Sin embargo, cuando el suministro de datos anonimizados o modificados no responda a las necesidades del Reutilizador de dichos datos, deja abierta la posibilidad de emplear Entornos de Tratamiento Seguros, que se han descrito en el capítulo anterior.

El Reutilizador tiene una obligación de confidencialidad que prohíba la divulgación de cualquier información que ponga en peligro los derechos e intereses de terceros. Además, se prohibirá a los Reutilizadores reidentificar a cualquier interesado al que se refieran los datos y estarán obligados a adoptar medidas técnicas y operativas para evitar la reidentificación[243]. Sin embargo, no estará prohibida la posibilidad de realizar investigaciones sobre técnicas de anonimización[244] cuando estas impliquen pruebas de reidentificación.

El análisis de una posible reidentificación de los Interesados o Sujetos de los Datos tendrá que estar siempre presente y tendrá que ser realizado de forma entre los intervinientes en un tratamiento en el marco de los Espacios de datos. El tratamiento de

[241] Artículo 5.1.b) del RGPD
[242] Consultar el apartado sobre Anonimización y Seudonimización del Área de Innovación y Tecnología de la página web de la AEPD.
[243] Artículo 5.5 de la DGA
[244] Considerando 8 de la DGA

anonimización no es un proceso trivial y cuando los datos provienen de varias fuentes, el riesgo de reidentificación aumenta. El Mediador de Datos ha de emplear profesionales adecuados, con conocimientos en el estado del arte de las técnicas de anonimización, y también con experiencia en los ataques de reidentificación de datos no personales. Hay que determinar mediante análisis y pruebas prácticas que no es posible reidentificar el conjunto de datos, para lo que hay que considerar condiciones del peor caso, como intentos de reidentificación por personas internas o externas, con acceso a datos auxiliares, incluso los disponibles por medios ilegales, por órdenes judiciales o por agencias de información, además de considerar de que se cuenta con los recursos adecuados y extrapolando la posible evolución de las técnicas conocidas. Si en esas condiciones se puede reidentificar todo o parte del conjunto de datos no cabe hablar de riesgo de reidentificación, simplemente dicho conjunto de datos no es anónimo.

Sin embargo, siempre habrá que asumir una probabilidad residual de reidentificación. Esta probabilidad residual significa aceptar que la infalibilidad total y absoluta no existe. En cualquier caso, al responsable del tratamiento sí se le puede exigir lo expresado en el párrafo anterior: aplicación de la responsabilidad proactiva con medidas apropiadas para garantizar el cumplimiento teniendo en cuenta la naturaleza, contexto, ámbito, fines y riesgos para los derechos y libertades, además de su revisión y actualización, como podría ser incorporar medidas de reanonimización.

Finalmente, señalar las limitaciones a las transferencias internacionales de datos no personales que se podrían establecer normativamente en caso de riesgo de reidentificación, que se tratan brevemente en el apartado de Transferencias Internacionales[245].

G. ENRIQUECIMIENTO DE CONJUNTOS DE DATOS

Con relación a la interacción entre Mediadores y los riesgos de reidentificación[246] una cuestión a plantearse sería el posible impacto del enriquecimiento de los conjuntos de datos, mediante de distintas fuentes de datos y su forma de gestionarlo, sobre todo cuando pueden ir más allá del objetivo de un Espacio de Datos.

Diversidad de fuentes de datos

En el marco del Espacio de Datos hay que plantearse en qué medida se puede gestionar que se añadan datos de diferentes fuentes, bien por los titulares de los datos como por los Mediadores, incluso en el marco del tratamiento en Entornos de Tratamiento Seguro.

De igual forma, se debe asegurar el cómo garantizar que los datos se ajustan a lo previsto para un determinado Espacio de Datos y no supongan datos de diferentes fuentes y de los mismos interesados, o la posible limitación a que los Usuarios de los Datos no realicen cruces de información de Espacios de Datos distintos cuando no sea considerado lícito u oportuno.

[245] Artículo 5.13 de la DGA

[246] Ver caso en el artículo del blog de la AEPD titulado "Anonimización (III): el riesgo de la reidentificación [febrero 2023]"

En este aspecto tienen gran importancia el empleo arquitecturas de protección de datos desde el diseño y tecnologías PET descritas en apartados anteriores.

Fuentes de acceso no restringido

El que los datos personales estén accesibles sin restricciones, a través de Internet u otros medios, no es una base para la legitimación del tratamiento de datos personales.

A la aplicación de las técnicas de "*scraping*"[247] que no traten datos personales no le es de aplicación la normativa de protección datos. Sin embargo, como se ha señalado anteriormente, se tendrá que analizar que el tratamiento conjunto de distintos datos no personales puede conducir a identificación de personas físicas.

H. TRANSFERENCIAS INTERNACIONALES DE DATOS

Las transferencias internacionales de datos personales están sometidas a lo establecido en el Capítulo V del RGPD. Más allá de su estricto cumplimiento, dichas transferencias podrían presentan riesgos para los derechos y libertades de los Sujetos de los Datos, por ejemplo, en cuanto al acceso no legítimo a datos personales y a una supervisión ineficaz de los mismos datos[248]. Dichos riesgos[249] serán mayores para algunos tipos de tratamientos y datos, y precisan ser evaluados y gestionados en el marco de la gobernanza y diseño del Espacio de Datos. El CEPD y el SEPD interpretan[250], a la luz de los pronunciamientos de TJUE[251] [252], que la normativa europea requiere, en ciertas circunstancias específicas, imponer la obligación de almacenamiento en la UE para mitigar dicho riesgo, como por ejemplo con relación al Espacio Europeo de Datos de Salud[253].

Este aspecto hay que tenerlo presente cuando se implementen servicios en la nube. La diligencia ha de tener en cuenta no solo la situación de los servidores en la UE, sino también los tratamientos colaterales que sobre dichos datos pueden realizar estos servicios[254] por múltiples motivos y que terminen materializándose en transferencias internacionales. También hay implementaciones que pueden implicar transferencias

[247] *Web scraping* es una técnica utilizada mediante programas de software para extraer información de sitios web. Usualmente, estos programas simulan la navegación de un humano en Internet.
[248] Párrafo 105 y 108 del documento "*EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*"
[249] Nota al pie 15 del documento "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (EDPS) [11 de abril de 2017]"
[250] Párrafo 106 del documento "*EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*"
[251] Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland Ltd*, joined Cases C-293/12 and C-594/12; para 68. See also the Opinion of Advocate General Cruz Villalón delivered on 12 December 2013 in the same case at para 78 and 79, noting that the absence provision that lays down the requirement to 'store the data to be retained in the territory of a Member State, under the jurisdiction of a Member State', 'increases the risk of use which is incompatible with the requirements resulting from the right to privacy' and 'considerably increases the risk that such data may be accessible or disclosed in infringement of that legislation'.
[252] Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined Cases C-203/15 and C-698/15, para 122. See also the opinion of Advocate General Saugmandsgaard Øe delivered on 19 July 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined Cases C-203/15 and C-698/15, para 239 to 241
[253] Párrafo 111 del documento "*EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*"
[254] Pueden ir desde operaciones de mantenimiento, supervisión remota desde fuera de la UE, necesidad de cumplimiento de normativa de terceros países, etc.

internacionales de datos y que resultan menos evidentes. Por ejemplo, cuando se integran determinadas SDKs[255] en el desarrollo de aplicaciones móviles y web para añadir funcionalidades muy diversas, como bases de datos de alta disponibilidad, analítica web y de apps, pasarelas de pago o características en la interfaz de usuario[256] [257].

Una obligación de almacenar datos personales en la UE no excluye las transferencias a terceros países u organizaciones internacionales. De hecho, es posible conciliar un requisito general de almacenar datos personales en la UE con transferencias específicas que permiten el cumplimiento del Capítulo V del RGPD (por ejemplo, en el contexto de la investigación científica, el desembolso de la atención o la cooperación internacional)[258].

En cualquier caso, es esencial evitar un enfoque incoherente y fragmentado en toda la UE con respecto a los criterios para realizar transferencias internacionales de datos[259]. Diferentes grados de protección de los Interesados en distintos países impediría la libre circulación de datos en la UE, ya que los intervinientes serían reticentes a permitir el acceso, cuando supone comunicación de datos, desde países de la UE que no garantizasen la protección de los datos personales. Por ello, en caso de que respecto a las transferencias internacionales no haya un criterio global aceptado, se recomienda implementar a nivel nacional el criterio más garantista para que las entidades de nuestro país tengan la mejor consideración de cumplimiento.

En el caso de reutilización de datos de organismos del sector público, la DGA establece en su Capítulo VII "Acceso y transferencia internacionales" y en los Considerandos del 21 a 24 condiciones para las transferencias de datos no personales. Aunque estas condiciones estarían en principio fuera de la competencia del RGPD, sí hay una referencia a la "*protección de la privacidad y de los datos personales*" a la hora de restringir la transferencia de "datos protegidos"[260] o "datos no personales muy sensibles"[261], quedando en manos del legislador nacional o europeo el limitar las transferencias de determinadas categorías de datos no personales que obren en poder de organismos del sector público cuando pueda, entre otros, entrañar el riesgo de la reidentificación de datos no personales anonimizados[262].

Además[263], el organismo del sector público, la persona física o jurídica a la que se haya concedido el derecho a reutilizar datos de determinadas categorías de datos protegidos

[255] *Software Development Kit*. Se trata de un conjunto de herramientas que normalmente proporciona el fabricante de una plataforma de hardware, o de un sistema operativo o para un lenguaje de programación, y que facilitan el desarrollo de aplicaciones nuevas para el producto específico y su entorno de aplicación.

[256] EDPS sanctions the European Parliament for illegal EU-US data transfers - among other violations (Pasarela de pago Stripe y Google Analytics, enlace a decision en NOYB)

[257] Asunto Google Fonts, un tribunal alemán multo a una web porque al conectar con Google Fonts para descargar una fuente de texto hace una conexión con servidor USA y eso implica que la IP (dato personal) se transfiera fuera del EEE. German Court Fines Website Owner for Violating the GDPR by Using Google-Hosted Fonts – WP Tavern

[258] Párrafo 108 del documento "*EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*"

[259] Párrafo 110 del documento "*EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*"

[260] Capítulo II de la DGA

[261] Considerando 24 de la DGA

[262] Artículo 5.13 de la DGA

[263] Artículo 31.5 de la DGA

(en este caso los datos personales[264]) que obren en poder de organismos del sector público, el proveedor de servicios de intermediación de datos o la organización reconocida de gestión de datos con fines altruistas informará al Titular de Datos afectado de que una autoridad administrativa de un tercer país ha solicitado acceso a sus datos, antes de dar curso a dicha solicitud, excepto en los casos en que la solicitud sirva a fines de ejecución de las leyes y mientras sea necesario para preservar la eficacia de las actividades policiales correspondientes.

I. GOBERNANZA, POLÍTICAS DE PROTECCIÓN DE DATOS, PROCEDIMIENTOS Y CÓDIGOS DE CONDUCTA

Uno de los objetivos de los Espacios de Datos es de establecer un marco de gobernanza de los datos. De hecho, se ha mencionado a lo largo del documento y se considera de vital importancia de cara a implementar protección de datos desde el diseño. Este apartado se incluye al final del texto porque el dicho marco de gobernanza ha de recoger gran parte de las obligaciones y recomendaciones desarrolladas en el mismo para garantizar el cumplimiento del RGPD.

En particular, el artículo 24.2 del RGPD en lo que se refiere a la responsabilidad del responsable del tratamiento se establece que "*Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos*". El Espacio de Datos es proporcionalmente adecuado para la definición y aplicación de políticas de protección de datos en el marco de gobernanza de los datos.

El CEPD y el SEPD ya han manifestado, en el marco del EHDS, que "*el éxito también dependerá del establecimiento de una sólida gobernanza de datos y salvaguardias efectivas para los derechos e intereses de las personas físicas que cumplan plenamente con el RGPD*"[265].

En dicha política de protección de datos, a aplicar a todos los intervinientes en el Espacio de Datos, se tiene que trasladar como se van a materializar de forma concreta, práctica y efectiva los principios y derechos establecidos en la normativa de protección de datos y las orientaciones de este documento. La política de protección de datos no establece el "qué", que ya está desarrollado en la norma, sino que debe describir el "cómo" se ha de garantizar y poder demostrar el cumplimiento del RGPD. Por ello, en una política de protección de datos en los tratamientos en el marco de un Espacio de Datos deberían aparece referencias con relación a, entre otros:

1. La implicación de los DPD y asesores de protección de datos en el diseño de los Espacios de Datos y los tratamientos en el marco de los mismos.
2. Los procedimientos de autorización al tratamiento de datos personales en el Espacio de Datos.
3. La definición precisa de los fines del tratamiento.
4. El establecimiento de las bases jurídicas del tratamiento.

[264] Artículo 3.1.d de la DGA
[265] *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]*

5. La determinación de roles responsable/encargado/subencargado de cada uno de los intervinientes.
6. La gestión del riesgo para los derechos y libertades de los interesados, que incluya, en su caso una EIPD, coordinada entre los intervinientes en el tratamiento.
7. La gestión de la implicación de varios Mediadores de Datos en un tratamiento de datos para garantizar el cumplimiento del RGPD. En el caso anterior, cuando los Mediadores pertenezcan a distintos Espacios de Datos, se debería de plantear la gestión y la coordinación entre ellos.
8. La definición de licencias de uso de datos que incluyan garantías jurídicas para la gestión de riesgos para los derechos y libertades de los Sujetos de los Datos.
9. La gestión y limitaciones del enriquecimiento de los conjuntos de datos.
10. Los procesos para determinar, y en su caso remediar, la posible reidentificación de conjuntos de datos no personales o anonimizados procedentes de distintas fuentes.
11. En el caso de tratamientos basados en el consentimiento, el establecimiento de criterios de granularidad del consentimiento, y recursos para la gestión del ciclo de vida del mismo, en particular, para la modificación del consentimiento o su retirada.
12. Los procedimientos para resolver dudas sobre la aplicación del consentimiento granular en tratamientos específicos.
13. Las garantías para que los datos personales disponibles en el Espacio de Datos no se recopilen ilegalmente ni se utilicen para fines que no se previeron inicialmente, sean desproporcionados o carezcan de una base jurídica adecuada[266].
14. Dar publicidad a las condiciones para permitir tratamientos adicionales sobre los datos personales[267].
15. Dar publicidad a los resultados de las EIPD.
16. Dar publicidad a los mecanismos de anonimización utilizados.
17. La aplicación de los principios de minimización de datos en los accesos a datos personales en el Espacio de Datos, de protección de datos desde el diseño y por defecto a la hora de desplegar la arquitectura del Espacio de Datos, así como en la implementación de los distintos casos de uso, introduciendo limitaciones en los plazos de conservación de los datos en cada uno de los intervinientes, si procede.
18. Los procedimientos técnicos y organizativos que garanticen la seguridad para la protección de los derechos y libertades de las personas físicas.
19. La definición de los requisitos de los Entornos de Tratamiento Seguro y de los Entornos de Ejecución Confiables.

[266] Párrafo 19 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*
[267] Párrafo 19 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*

20. El procedimiento para garantizar que el tratamiento en un Entorno de Tratamiento Seguro cumple los posibles requisitos de realizar una EIPD, de consultar a la autoridad de control en virtud de los artículos 35 y 36 del RGPD, y se haya constatado que los riesgos para los derechos y los intereses de los interesados son mínimos, entre otros.
21. Las condiciones de interoperabilidad que garanticen la aplicación de medidas para el cumplimiento de la normativa de protección de datos.
22. El mecanismo integrado para la gestión de brechas de datos personales, que acorte los tiempos de reacción, permita un conocimiento en tiempo real de las incidencias para todos los intervinientes, y realice una protección efectiva del impacto para los sujetos de los datos y la sociedad.
23. La aplicación del principio de transparencia, de forma que se permita al Interesado o Sujeto de los Datos tener un control de los tratamientos realizados con sus datos personales y una trazabilidad de a quién se están comunicando sus datos y cómo se hizo esa comunicación (solicitud, transferencia, etc.).
24. El establecimiento de mecanismos para asegurar el respecto del principio de trasparencia en el caso de decisiones individuales automatizadas, incluida la elaboración de perfiles, y el derecho por parte del interesado a expresar su punto de vista, a impugnar la decisión y a obtener intervención humana por parte del responsable.
25. El establecimiento mecanismos para asegurar el respecto de los derechos a la protección de datos del Interesado o Sujeto de los Datos (derecho de acceso del interesado, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición).
26. El establecimiento mecanismos para que el Sujeto de los Datos se pueda oponer a un tratamiento que supone el cambio de formato de sus datos personales.
27. El establecimiento de periodos de conservación, así como la gestión de los mismos
28. El establecimiento mecanismos para asegurar el respecto de los derechos digitales del interesado (derecho a la seguridad digital, protección de los menores en Internet) incluidos en la Ley Orgánica 3/2018.
29. Determinar criterios y procedimientos para la supervisión humana en el proceso de autorizar la comunicación de datos personales entre responsables cuando proceda y las garantías en los procesos automatizados de acceso a los datos.
30. El aseguramiento del cumplimiento con los códigos de conducta y los programas de certificación en vigor.
31. El establecimiento mecanismos para asegurar que las transferencias internacionales de datos estén basadas en una decisión de adecuación o que, en caso contrario, se hayan establecido medidas de garantías adecuadas.

32. La implementación de registros de actividad y la realización de auditorías sobre los mismos que garanticen la responsabilidad proactiva[268].
33. La creación de un proceso iterativo para asegurar el cumplimiento del RGPD en base al principio de responsabilidad proactiva.
34. El disponer de una entidad encargada de la supervisión del Espacio de Datos, al menos, desde la perspectiva del cumplimiento de la normativa de protección de datos.

Una Política de Protección de Datos es una forma de actuar documentada, no solo un documento. La forma de actuar definida en la Política de Protección de Datos ha de ser eficaz, eficiente y ejecutiva, y para eso se ha de reflejar en las normas internas y los procedimientos a ejecutar[269].

A este respecto habría que destacar la importancia que los códigos de conducta podrían tener en el Espacio de Datos, así como el papel que el supervisor del código de conducta podría ejercer con relación a la supervisión de las solicitudes de acceso.

[268] Párrafo 26 del documento *"Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]"*
[269] Apartado "IV LA GOBERNANZA DE LOS RIESGOS PARA LOS DERECHOS Y LIBERTADES" de la Guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"

VII. REFERENCIAS

Marco normativo:

- 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)
- 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).
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos). [23/02/2022]
- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. [21/04/2021]
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios. [03/05/2022]
- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida).
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (versión consolidada).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (versión consolidada).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (versión consolidada).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (versión consolidada).
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (versión consolidada).
- Norma Técnica de Interoperabilidad (NTI) con relación a la catalogación y metadatos.

Guías y notas técnicas publicadas por la Agencia Española de Protección de Datos:

- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
- Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo
- Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)
- Guía para la gestión de brechas de datos personales

- Infografía Comunicación Brechas de Datos Personales
- Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales
- 10 Malentendidos relacionados con la anonimización
- La K-anonimidad como medida de privacidad
- Orientaciones y garantías en los procedimientos de Anonimización de datos personales
- Introducción al hash como técnica de seudonimización de datos personales
- Guía para la clientela que contrate servicios de Cloud Computing
- Orientaciones para prestadores de servicios de Cloud Computing
- 10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)
- Requisitos para Auditorías de Tratamientos que incluyan IA (realizada en colaboración con el SEPD)
- Adecuación al RGPD de tratamientos que incorporan inteligencia artificial

Herramientas de la Agencia Española de Protección de Datos:

- Herramienta EVALÚA-RIESGO v2 para el análisis de los factores de riesgo
- Herramienta para evaluar la necesidad de notificar a la Autoridad de Control: ASESORA BRECHA
- Herramienta para evaluar la obligación de comunicar a los interesados: COMUNICA-BRECHA RGPD

Artículos publicados por la Agencia Española de Protección de Datos:

- Cifrado y Privacidad: cifrado en el RGPD [noviembre 2019]
- Cifrado y Privacidad II: El tiempo de vida del dato [enero 2020]
- Brechas de seguridad: comunicación a los interesados [febrero 2020]
- Protección de datos y seguridad [abril 2020]
- Cifrado y Privacidad III: Cifrado Homomórfico [junio 2020]
- Anonimización y seudonimización [octubre 2021]
- Anonimización y seudonimización (II): la privacidad diferencial [octubre 2021]
- Sin privacidad no hay ciberseguridad [febrero 2022]
- Privacidad desde el diseño: Anonimización y seudonimización (II): la privacidad diferencial [mayo 2022]
- Anonimización (III): el riesgo de la reidentificación [febrero 2023]
- Cuándo hay que revisar las medidas de protección de datos [febrero 2023]
- Inteligencia Artificial: Sistema vs. Tratamiento, medios vs. Finalidad [abril 2023]
- Federated Learning: Inteligencia Artificial sin comprometer la privacidad [abril 2023]

Otras publicaciones nacionales:

- Evaluación del estudio de la movilidad en España con tecnología Big Data durante el estado de alarma para la gestión de la crisis del COVID-19 por el DPD del Ministerio de Transportes, Movilidad y Agenda urbana (MITMA).
- Presentación de la Plataforma del Dato de la AGE. Medida 6: Gestión e intercambio transparente del dato. Secretaría General de Administración Digital. Ministerio de Asuntos Económicos y Transformación Digital.
- Artículo publicado por la Oficina del Dato "Importancia de la Catalogación de Datos [28/12/2020]"
- Artículo publicado por la Oficina del Dato "El modelo de arquitectura de referencia IDS-RAM y su papel en los espacios de datos [26/04/2022]"
- Artículo publicado por la Oficina del Dato "Gaia-X y los espacios de datos europeos [28/04/2022]"
- Artículo publicado por la Oficina del Dato "Características para la creación de espacios de datos [05/07/2022]"
- Artículo publicado por la Oficina del Dato "¿Cuáles son los principales elementos de un espacio de datos? [20/10/2022]"
- Artículo publicado por la Oficina del Dato "Radiografía del dataspace nacional de Turismo: retos y oportunidades para el sector turístico [07/02/2023]"
- Artículo publicado por la Oficina del Dato "Especificaciones UNE – Gobierno, gestión y calidad del dato [31/03/2023]"
- Herramienta para elaborar casos de uso en espacios de datos de la Oficina del Dato
- Escenarios de compartición de datos. Francisco Javier Esteve Pradera, junio 2022 – Boletic nº 91

Publicaciones del Comité Europeo de Protección de Datos y del Grupo de Trabajo del Artículo 29:

- WP 169 Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (Grupo de Trabajo del Artículo 29) [16 de febrero de 2010]
- WP 211 Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas (Grupo de Trabajo del Artículo 29) [27 de febrero de 2014]
- WP 216 Dictamen 05/2014 sobre técnicas de anonimización (Grupo de Trabajo del Artículo 29) [10 de abril de 2014]
- WP 248 Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (Grupo de Trabajo del Artículo 29) [4 de octubre de 2017]

- Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (EDPB) [4 de mayo de 2020]
- Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (EDPB) [20 de octubre de 2020]
- Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad (EDPB) [9 de marzo de 2021]

Publicaciones conjuntas del Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos:

- Dictamen conjunto 3/2021 del CEPD y el SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) [10 de marzo de 2021]
- EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [12 July 2022]

Publicaciones del Supervisor Europeo de Protección de Datos:

- Manual para la evaluación de la necesidad de las medidas que limiten el derecho fundamental a la protección de datos personales (EDPS) [11 de abril de 2017]
- Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales [19 de diciembre de 2019]
- Opinion 3/2020 on the European strategy for data (EDPS) [16 June 2020]
- Preliminary Opinion 8/2020 on the European Health Data Space (EDPS) [17 November 2020]

Publicaciones de la Comisión Europea:

- Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea (COM(2019) 250 final) [29 de mayo de 2019]
- Comunicación sobre el principio de precaución (COM(2000)1 final) [2 de febrero de 2000]
- Una Estrategia Europea de Datos (COM(2020) 66 final) [19 de febrero de 2020]
- COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces. European Commission (SWD(2022) 45 final) [23 February 2022]

Publicaciones de la Agencia Europea de Ciberseguridad:

- Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics European Union Agency for Cybersecurity (ENISA). [17 December 2015]
- RECOMMENDATIONS ON SHAPING TECHNOLOGY ACCORDING TO GDPR PROVISIONS, An overview on data pseudonymisation. European Union Agency for Cybersecurity (ENISA). [November 2018]

- DATA PSEUDONYMISATION: ADVANCED TECHNIQUES & USE CASES, Technical analysis of cybersecurity measures in data protection and privacy. European Union Agency for Cybersecurity (ENISA). [January 2021]
- INGENIERÍA DE LA PROTECCIÓN DE DATOS, De la teoría a la práctica. European Union Agency for Cybersecurity (ENISA) [Enero de 2022]
- ENGINEERING PERSONAL DATA SHARING, Emerging Use Cases and Technologies. European Union Agency for Cybersecurity (ENISA) [January 2023]

Otras publicaciones internacionales:

- PDPC Singapore: Guía Básica de Anonimización versión en español [Marzo 2022]
- PDPC Singapore: Herramienta Básica de Anonimización versión en español [Marzo 2022]
- What is a Data Space? Definition of the concept Data Space. White Paper 1/2022. (gaia-x – Hub Germany) [September 2022]