Diputació de València | Protecció de Dades i Seguretat de la Informació

Boletín Protección de Datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 40| Octubre 2023

LOS ESPACIOS DE DATOS Y LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ÍNDICE

LOS ESPACIOS DE DATOS Y LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

La tecnología permite que tanto las Administraciones Públicas como las empresas privadas 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.

El presente boletín analiza desde la perspectiva de protección de datos un modelo tecnológico para la implementación eficiente del mercado interior de datos denominado "Espacios de Datos", en cuanto supone tratamientos de datos personales.

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**, servicios para establecer relaciones comerciales entre los intervinientes o, por ejemplo, Espacios de Datos en sectores específicos. Un Espacio de Datos es distinto a los almacenamientos centralizados de información, los datalakes, data warehouses, etc.

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.

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. Debemos 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, 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.

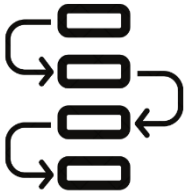
DEFINICIONES

Hemos intentado recabar algunas de las definiciones de los términos más relevantes que se emplean en la normativa y las referencias técnicas con relación a los Espacios de Datos**:**

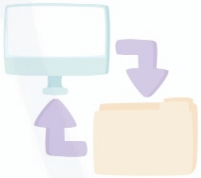
- **Agregador de datos**: servicio que permite aunar en un solo lugar datos existentes en distintas fuentes.

- **Aprendizaje federado:** servicio que permite aunar en un solo lugar datos existentes en distintas fuentes.

- **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.



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.



- **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.

- **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.

- **Entorno de tratamiento seguro:** el entorno físico o virtual y los medios organizativos para garantizar el cumplimiento del Derecho de la Unión, 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.

• **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.

- **Guardian de acceso:** se define como una empresa prestadora de servicios de plataforma, para el objeto de prestar un servicio de computación en la nube, con gran influencia en el mercado interior y con una posición afianzada y duradera.

- **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).

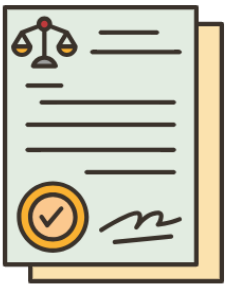
- **Mediador del Espacio de Datos, Mediador de Datos:** entidades que establecen las relaciones en el Espacio de Datos entre los Sujetos de los Datos y/o Titulares de los Datos, por una parte, y los Usuarios de los Datos, por otra. En el marco del Reglamento de gobernanza europea de datos (de ahora en adelante, DGA) se considerarán Mediadores a los "organismos competentes", los "servicios de intermediación de datos" (y su subtipo las "cooperativas de datos") y las "organizaciones de gestión de datos con fines altruistas".

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 la sujeción al Reglamento General de Protección de Datos (de ahora en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD, de ahora en adelante). Sin ánimo de exhaustividad, a continuación, se indican las siguientes normas básicas:

- El Reglamento de Gobernanza de Datos (DGA)

- El Reglamento de Mercados Digitales (DMA)
- El Reglamento de Servicios Digitales, Ley 37/2007 sobre utilización de la información del sector público.
- Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad
- Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.



No obstante, hay una serie de propuestas de regulación europea de la Comisión que actualmente están en tramitación. 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. 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."*

CATEGORIAS DE INTERVENIENTES

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

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.

2. Titular de Datos

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.

3. 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.

4. Mediadores 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.

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. De ahí cabe inferir que estas entidades son claves para la implementación de medidas de protección de datos desde el diseño y por defecto.

5. Habilitadores técnicos y legales

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.

6. 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.

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.

7. Autoridades de control

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.

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, 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.

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, en el caso de las Administraciones Públicas no habría lugar para el interés legítimo. 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 posterior compatible de los datos deben ser muy claros para todas las partes interesadas.

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.

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, 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.

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.

CASOS DE USO Y ARQUITECTURAS

En el marco de un Espacio de Datos se pueden plantear distintos tipos de tratamiento de datos personales, es decir, diferentes casos de uso 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.

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. 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:

a) 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.

b) El subcaso de uso donde se puede cumplir **comunicando el Mediador de Datos información anonimizada** al Usuario de Datos.

c) El subcaso de uso donde se puede cumplir comunicando el Mediador de Datos información seudonimizada al Usuario de Datos.

d) El subcaso de uso donde solo se puede cumplir realizando una comunicación de datos personales de Mediador de Datos a un Usuario de Datos.

Es importante subrayar 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.

ACCESO A DATOS, INFORMACIÓN Y EJERCICIO DE DERECHOS

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. 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.

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 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.

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 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.

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 o el interés público 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.

En el 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.

"Uno de los objetivos de los Espacios de Datos es de establecer un marco de gobernanza de los datos. Se considera de vital importancia de cara a implementar protección de datos desde el diseño. 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".

MATERIAL COMPLEMENTARIO

- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la gobernanza europea de los datos (Data Governance Act, DGA) Puedes consultar el Reglamento en este enlace.
- 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) (Texto pertinente a efectos del EEE). Puedes consultar el reglamento en este enlace.
- Dictamen 05/2014 sobre técnicas de anonimización del Grupo del Articulo 29. Puedes consultar el Dictamen en este enlace.
- Dictamen 03/2013 sobre la limitación del fin Grupo del Articulo 29. Puedes consultar el Dictamen en este enlace.

NOTICIAS

- **La Autoridad Catalana de Protección de Datos (APDCAT) emite un Dictamen sobre utilización de datos biométricos para el control de presencia en el puesto de trabajo**

  El Dictamen se emite en relación con la consulta formulada por el DPD "[...] se manifieste sobre la viabilidad de las EIPD en torno al uso de la biometría del trabajador (huella dactilar o facial) como sistema para llevar a cabo el registro de jornada laboral de los trabajadores. La APDCAT afirma que el consentimiento puede ser una base jurídica habilitante del tratamiento con finalidad de control horario siempre que éste constituya una manifestación de voluntad libre, específica, informada e inequívoca por parte del interesado de aceptar el tratamiento. En todo caso, antes de llevar a cabo un tratamiento como este, es necesario realizar una evaluación del impacto sobre la protección de datos donde se analice, entre otras cuestiones, la licitud del tratamiento.

  Puedes consultar el Dictamen en este enlace.
- **La APDCAT emite un Informe sobre acceso al registro de accesos de la Historia Clínica.** Considera que los accesos a la historia clínica de un paciente realizados por el personal, no se pueden considerar información que forme parte del derecho de acceso. Según la APDCAT, la trazabilidad de los accesos a la historia clínica de la reclamante formaría parte del registro de accesos a las historias clínicas. Esta información es pública a los efectos de la legislación de transparencia Considerando que la información solicitada no incluye datos de categoría especial (puesto que los datos de salud hacen referencia al reclamante solicitante de la información y no a las personas que han accedido a su historia) la APDCAT concluye que la normativa no impide comunicar a la persona reclamante la información que solicita, relativa a los accesos a su historia clínica, incluida la identidad de los profesionales, rango y categoría profesional, que han accedido a la misma.

  Puedes consultar el Informe en este enlace