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

Butlletí Protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 40| Octubre 2023

ELS ESPAIS DE DADES I LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

ÍNDEX

ELS ESPAIS DE DADES I LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpto. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

La tecnologia permet que tant les Administracions Públiques com les empreses privades utilitzen dades personals en una escala sense precedents a l'hora de realitzar les seues activitats. La transformació digital i el creixent ús dels serveis digitals també comporta nous riscos i desafiaments per als destinataris individuals dels corresponents serveis, les empreses i la societat en el seu conjunt.

El present Butlletí analitza des de la perspectiva de protecció de dades un model tecnològic per a la implementació eficient del mercat interior de dades denominat "*Espais de Dades*", quan suposa tractaments de dades personals.

Normativament **es plantegen diferències jurídiques en relació amb la definició dels intervinents, els límits dels tractaments i les garanties necessàries, en funció de si es tracta de la reutilització de dades en poder d'organismes del sector públic**, serveis per a establir relacions comercials entre els intervinents o, per exemple, Espais de Dades en sectors específics. Un Espai de Dades és diferent als emmagatzematges centralitzats d'informació, els *datalakes*, data *warehouses*, etc.

Les iniciatives europees i nacionals d'Espais de Dades, i els seus desenvolupaments normatius, plantegen models de tractaments de gran complexitat organitzativa, jurídica i tecnològica, així com d'una gran escala en el nombre de subjectes afectats, en la diversitat de categories de dades tractades.

Aquestes iniciatives no es plantegen com una reducció o un compromís dels drets i llibertats de les persones físiques en relació amb la protecció de les seues dades personals. Hem de tindre en compte que l'accés a les dades que es planteja en un Espai de Dades es defineix com tota utilització de dades de conformitat amb uns requisits específics, però, sense que això implique necessàriament la transmissió o la descàrrega de les dades, ni desplaçant els principis i drets del RGPD. Referent a això, existeixen diferents recursos tecnològics que permeten l'accés a dades personals amb garanties de protecció de dades, oferint més opcions que únicament l'anonimització o recórrer a la comunicació de dades personals.

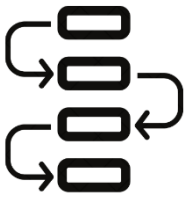
DEFINICIONS

Hem intentat recaptar algunes de les definicions dels termes més rellevants que s'empren en la normativa i les referències tècniques en relació amb els Espais de Dades:

- **Agregador de dades**: servei que permet conjuminar en un sol lloc dades existents en diferents fonts.

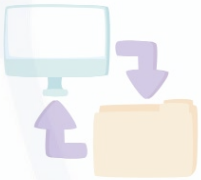
- **Aprenentatge federat:** servei que permet conjuminar en un sol lloc dades existents en diferents fonts.

- **Cicle de vida de la dada:** des de la perspectiva de l'Espai de Dades, el cicle de vida remet a les diferents etapes per les quals passa una dada des del seu naixement fins a la fi. La dada no és un actiu estàtic durant el seu cicle de vida, sinó que passa per diferents fases.



Cal no confondre el concepte de cicle de vida de la dada en el marc d'un Espai de Dades, amb el cicle de vida de la dada en un tractament.

- **Compute – to – data:** estratègia que consisteix en el fet que, en comptes d'enviar les dades cap als recursos de computació, els recursos de computació s'emporten a l'origen de les dades. D'aquesta manera es preserva la privacitat de les dades i el responsable (Titular de Dades) manté un major control sobre el seu tractament.



- **Entorn d'execució de confiança:** és un entorn de tractament inviolable que té lloc en el processador principal d'un dispositiu amb un maquinari i un programari dissenyat de tal manera que es garanteix la integritat i confidencialitat de les dades i del tractament realitzat en aquest processador enfront de qualsevol tipus d'atac.

No ha de confondre's amb Entorn de Tractament Segur on a més dels aspectes de confidencialitat, integritat i disponibilitat de les dades, es garanteixen les obligacions legals recollides en el Dret nacional i de la Unió.

- **Entorn de tractament segur:** l'entorn físic o virtual i els mitjans organitzatius per a garantir el compliment del Dret de la Unió, el RGPD, en particular, pel que respecta als drets dels interessats, els drets de propietat intel·lectual i la confidencialitat comercial i estadística, la integritat i l'accessibilitat, així com per a garantir el compliment del Dret nacional aplicable i permetre que l'entitat encarregada de proporcionar l'Entorn de Tractament Segur determine i supervise totes les accions de tractament, inclosa la presentació, l'emmagatzematge, la descàrrega i l'exportació de dades, així com el càlcul de dades derivades mitjançant algorismes computacionals.

• **Espai de dades:** infraestructura basada en mecanismes comuns de governança, organitzatius, normatius i tècnics, que facilita l'accés a les dades i, amb això, el desenvolupament de models de negoci basats en la seua exploració i explotació.

- **Guardià d'accés:** es defineix com una empresa prestadora de serveis de plataforma, per a l'objecte de prestar un servei de computació en el núvol, amb gran influència en el mercat interior i amb una posició afermada i duradora.

• **Dades personals dinàmiques i estàtics:** els espais de dades podrien contindre dades personals estàtiques, com el nom, l'adreça o la data de naixement, així com dades dinàmiques que genera una persona, per exemple, a través de l'ús d'un servei en línia o un objecte connectat a la Internet de les coses.

També podrien utilitzar-se per a emmagatzemar informació d'identitat verificada, com, per exemple, el número de passaport o la informació sobre seguretat social, i credencials (per exemple, permís de conduir, diplomes o informació sobre comptes bancaris).

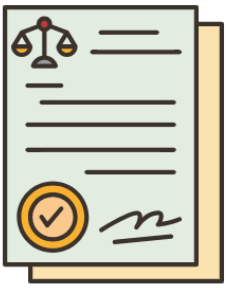
- **Mediador de l'Espai de Dades, Mediador de Dades:** entitats que estableixen les relacions en l'Espai de Dades entre els Subjectes de les Dades i/o Titulars de les Dades, d'una banda, i els Usuaris de les Dades, per una altra. En el marc de l Reglamento de governança europea de dades(d'ara en avant, DGA) es consideraran Mediadors als "*organismes competents*", els "*serveis d'intermediació de dades*" (i el seu subtipus les "*cooperatives de dades*") i les "*organitzacions de gestió de dades amb finalitats altruistes*".

MARC NORMATIU PER ALS ESPAIS DE DADES

En la mesura en què es realitzen tractaments de dades personals en un Espai de Dades el marc normatiu comença a definir-se per la subjecció al Reglament General de Protecció de Dades (d'ara en avant, RGPD) i la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD, d'ara en avant). Sense ànim d'exhaustivitat, a continuació, s'indiquen les següents normes bàsiques:

- El Reglament de Governança de Dades (DGA)

- El Reglament de Mercats Digitals (DMA)
- El Reglament de Serveis Digitals Llei 37/2007 sobre utilització de la informació del sector públic.
- Llei 34/2002 de serveis de la societat de la informació i de comerç electrònic.
- Reial decret 311/2022 pel qual es regula l'Esquema Nacional de Seguretat
- Reial decret 4/2010 pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.



No obstant això, hi ha una sèrie de propostes de regulació europea de la Comissió que actualment estan en tramitació. En l'àmbit nacional, a l'hora de redactar aquestes orientacions, s'ha previst la creació d'un Espai de Dades Integrat de Mobilitat (EDIM) en la futura Llei de Mobilitat Sostenible (avantprojecte de llei aprovat en Consell de Ministres de 12 de desembre 2022).

En la norma s'establirà la seua creació, definició i governança. En particular, en el seu article 104 sobre infraccions greus identifica referent a subministrament de dades al EDIM: *"la utilització per a finalitats diferents de subministrament de dades al EDIM de les dades personals obtingudes directament per part dels operadors de transport, gestors d'infraestructura i centres d'activitat. En aquest cas, el procediment sancionador serà l'establit en la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals per l'òrgan competent en matèria de protecció de dades personals."*

CATEGORIES D'INTERVINENTS

Des del punt de vista de la protecció de dades es podrien identificar els següents intervinents o rols en l'Espai de Dades:

1. Interessats o Subjectes de les dades

El Interessat o Subjecte de les Dades, és a dir, la persona física identificada o identificable les dades personals de la qual són els que es planteja tractar, podria associar-se a la definició de "*productor de les dades*" utilitzada en alguns esquemes d'Espais de Dades.

Quan s'associa la figura de "*productor de les dades*" a sistemes o serveis que recullen o generen dades personals de persones físiques (p. ex. sistemes IoT), en la mesura en què aquestes dades estiguen vinculats a persones identificades o identificables, continuarem parlant de dades d'un interessat.

2. Titular de Dades

Aquella persona que tinga dret a concedir accés a determinades dades personals o no personals. Els Titulars de Dades, en el marc d'un Espai de Dades, podrien executar operacions de comunicació de dades, d'aplicació de mecanismes per a permetre el tractament *on-premises*, realitzar tractaments de seudonimización i

anonimització, altres tractaments com extraure dades sintètiques, proporcionar accés amb implementació de privacitat diferencial, realitzar comunicacions de dades a altres responsables o un altres.

En marcs generals d'Espais de Dades es pot trobar aquesta figura etiquetada com el "*propietari de les dades*" o "*custodi de les dades*". Aquesta denominació és enganyosa quan es refereix a dades personals, perquè un responsable de tractament no posseeix les dades dels Interessats o Subjectes de les Dades, sinó que disposa d'una base jurídica que ho legitima per al seu tractament conforme a les obligacions que s'estableixen en la normativa de protecció de dades.

3. Usuari de Dades

L'Usuari de Dades és tota persona física o jurídica que tinga accés legítim a determinades dades personals o no personals i el dret, inclòs el que li atorga el RGPD en el cas de les dades personals, a usar-los amb finalitats comercials o no comercials.

4. Mediadors de l'Espai de Dades

Els Mediadors de l'Espai de Dades són les entitats que estableixen les relacions en l'Espai de Dades entre els Subjectes de les Dades i/o Titulars de les Dades, d'una banda, i els Usuaris de les Dades, per una altra.

Són aquells que implementen els mitjans tècnics, jurídics, organitzatius, o d'un altre tipus que permeten l'operació de l'Espai de Dades entre múltiples Titulars i múltiples Usuaris de Dades.

En el marc d'un Espai de Dades genèric, una o diverses entitats Mediadores podrien realitzar tractaments per a la creació de catàlegs de dades, creació de bases de dades centralitzades, transformació de les dades, creació de plataformes d'intercanvi o explotació de dades, gestió de consentiments, etc. A més, el Mediador realitzaria un seguiment de totes les fonts de dades i tractaments, avaluaria i actualitzaria les polítiques d'ús de dades al llarg del cicle de vida del tractament de dades. El Mediador de Dades registraria les comunicacions de dades per a cada Usuari de Dades amb el qual interactua, i també per a la majoria dels Subjectes de les Dades, a més d'altres funcions. D'ací cal inferir que aquestes entitats són claus per a la implementació de mesures de protecció de dades des del disseny i per defecte.

5. Habilitadors tècnics i legals

Els Habilitadors a l'entorn d'un Espai de Dades serien aquells que donaran suport a tots els intervinents anteriorment descrits per a poder garantir que la implementació es realitza un procés eficient, coherent, implementant els mecanismes de governança i gestió entre múltiples intervinents, evitant duplicitats i repeticions de tasques, facilitant els tràmits i sol·licituds.

6. Supervisor de les sol·licituds d'accés

Les entitats supervisores seran aquelles encarregades d'avaluar les sol·licituds presentades per part d'un Usuari de Dades per al tractament de dades personals.

Depenent de la finalitat de l'Espai de Dades, la concessió de la sol·licitud pot estar subjecta a diferents normatives i principis ètics. Una de les normatives a tindre en compte serà l'específica i sectorial en relació amb la protecció de dades.

En el cas que les sol·licituds incloguen accés a les dades personals, aquest Supervisor haurà d'establir les condicions en la qual se li donarà accés a les dades en funció, entre altres, de la base jurídica en la qual es basa la petició i les mesures que es presenten per a garantir i poder demostrar el compliment.

També hauria d'establir en unes certes ocasions les condicions d'accés a les dades personals, independentment de les mesures per a la gestió del risc, on figuraran, entre altres coses, els mecanismes de seudonimización i/o anonimització previstos, l'Entorn de Tractament Segur habilitat per al tractament de dades personals i la limitació temporal d'accés a aquestes dades. Les Avaluacions d'Impacte en la Protecció de Dades (EIPDs) en relació amb el tractament sol·licitat haurien de ser part dels elements a incloure en les sol·licituds.

7. Autoritats de control

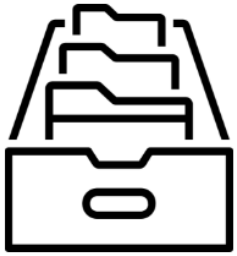
Les autoritats competents seran les indicades en el RGPD, que en el cas d'Espanya serà l'AEPD, o les Autoritats Autonòmiques d'acord amb la seua competència. Quan altres autoritats actuen com a autoritats competents, per exemple, conformement a la DGA, ho han de fer sense perjudici de les facultats i competències de supervisió de les autoritats responsables de la protecció de dades conformement al RGPD.

LEGITIMACIÓ DELS TRACTAMENTS

El tractament de dades personals en el marc d'un Espai de Dades manca d'una legitimació per-sé, com estableix la DGA, i necessita d'una legitimació concreta basada en l'article 6 del RGPD. Per a la reutilització de dades que obren en poder d'organismes del sector públic, el Dret de la Unió o dels Estats membres ha de preveure un fonament jurídic adequat en virtut del RGPD, i els organismes del sector públic definir-lo de manera conscienciosa.

La legitimació del tractament de dades personals en el marc d'un Espai de Dades pot basar-se en qualsevol de les bases jurídiques de l'Article 6 del RGPD, incloent-hi el compliment d'obligacions legals, en el cas de les Administracions Públiques no pertocaria per a l'interés legítim. La qüestió és que la legitimació siga clara i correctament definida en el tractament.

Estretament vinculat a la legitimitat del tractament, està el principi de limitació de fins. Els límits del que constitueix un tractament lícit i un tractament posterior compatible de les dades han de ser molt clars per a totes les parts interessades.



A més, en el cas que els fins siguen d'arxiu en interés públic, fins d'investigació científica i històrica o fins estadístics, ha d'estar d'acord amb el que s'estableix en l'article 89, apartat 1, del RGPD (salvaguardes i excepcions relatives al tractament amb finalitats científics), llegit a la llum de l'article 50 del RGPD. L'Opinió 3/2013 del Grup de Treball de l'Article 29 proporciona una guia útil sobre la implementació del principi de limitació de la finalitat, així com sobre l'ús apropiat de les diverses bases legals per al processament de dades personals i continua sent rellevant en gran manera també sota el RGPD.

Des de la perspectiva de protecció de dades, la part més important de l'estructura de governança d'un Espai de Dades és l'establiment amb claredat dels rols de responsables i encarregats/subencargados quan es tracten dades personals, i que ha d'estar definida des del disseny.

A més, aquests rols han de ser establits d'acord amb la normativa i a les directrius establides per les autoritats de control.

Amb relació amb l'anonimització, cal assenyalar que és un tractament de dades personals, i com tot tractament, ha de complir amb els mateixos requisits assenyalats anteriorment.

CASOS D'ÚS I ARQUITECTURES

En el marc d'un Espai de Dades es poden plantejar diferents tipus de tractament de dades personals, és a dir, diferents casos d'ús en els quals es podran adoptar estratègies específiques per a implementar la protecció de dades des del disseny per als accessos entre Titulars de Dades i Mediadors de Dades:

1. El cas d'ús que requereix tractar **informació no personal** en supòsits diferents a l'anonimització de dades personals.

2. El cas d'ús on es pot executar el tractament sense cedir dades personals pel Titular de Dades, sinó tractant-los en els seus propis sistemes i **proporcionant informació que no constituïsquen dades de caràcter personal** al Mediador de Dades (agregada, processada o altres). És a dir, implementant estratègies "*compute-to-data*".

3. El cas d'ús que es pot complir comunicant el Titular de Dades informació anonimitzada al Mediador de Dades.

4. El cas d'ús que es pot complir comunicant el Titular de Dades **informació seudonimizada** al Mediador de Dades.

5. El cas d'ús que només es pot complir realitzant una **comunicació de dades personals** dels Titulars de les Dades a un Mediador de Dades.

Els casos anteriors descriuen la relació entre els Titulars de les Dades i els Mediadors de Dades.
També es podrien aplicar quan un Usuari de Dades vulga accedir a la informació de múltiples Titulars de Dades. Només en els casos 4 i 5 es comunica informació personal al Mediador, en el cas 4 seudonimizada i en el cas 5 sense seudonimizar.

Caldria plantejar-se que, en aquests dos últims casos, entre el Mediador de Dades i l'Usuari de Dades es podrien desplegar els següents subcasos:

a) El subcàs d'ús on es pot executar el tractament sense cedir dades personals pel Mediador de Dades, sinó tractant-los en els seus propis sistemes i proporcionant informació que no constituïsquen dades de caràcter personal a l'Usuari de Dades (agregada, processada o altres). És a dir, implementant entorns de tractaments segurs de dades.

b) El subcàs d'ús on es pot complir **comunicant el Mediador de Dades informació anonimitzada** a l'Usuari de Dades.

c) El subcàs d'ús on es pot complir comunicant el Mediador de Dades informació seudonimizada a l'Usuari de Dades.

d) El subcàs d'ús on sol es pot complir realitzant una **comunicació de dades personals** de Mediador de Dades a un Usuari de Dades.

És important subratllar que l'Espai de Dades ha d'estar definit des del disseny per a poder implementar aquelles arquitectures que es plantegen tinguen un risc acceptable per als drets i llibertats dels subjectes de les dades i la societat d'acord amb els diferents tractaments concrets.

ACCÉS A DADES, INFORMACIÓ I EXERCICI DE DRETS

En la DGA es defineix "accés" com tota utilització de dades de conformitat amb uns requisits específics de caràcter tècnic, jurídic o organitzatiu, sense que això implique necessàriament la transmissió o la descàrrega de les dades. És a dir, en el marc dels Espais de Dades es fa la distinció entre dos conceptes que poden semblar similars però que són molt diferents:

- Accés a les dades mitjançant la **transmissió o la descàrrega**.
- Accés a la informació generada pel **tractament de les dades mitjançant un accés que no implique ni transmissió o descàrrega** de les dades.

Un Espai de Dades ha de permetre a l'Usuari de Dades aconseguir la informació necessària per a cadascun dels tractaments, i això no implica necessàriament la comunicació o difusió de dades personals.

Per tant, un Espai de Dades podria (i des del punt de vista de protecció de dades és el més recomanable) concedir accés a les dades personals, però sense difondre'ls, és a dir, no necessàriament comunicació a tercers de les dades.
De fet, una arquitectura d'Espai de Dades, que es construïsca aplicant els principis de protecció de dades des del disseny minimitzarà l'exposició de dades personals (principi de minimització) i preservarà la capacitat de disposar de la informació necessària per a complir les finalitats dels Espais de Dades.

La infraestructura d'un Espai de Dades ha de donar accés a les dades entés com la possibilitat de realitzar una explotació dels mateixos per a obtindre valor (informació) sense que això implique necessàriament la comunicació de dades, en aquest cas personals, entre intervinents.

Els Espais de Dades que permeten disposar de la informació, però sense comunicació o difusió de les dades personals, p. ex. deixant el control real de les dades i de les finalitats en mans dels Titulars de les Dades augmentaran la confiança d'aquests Titulars per a participar en l'Espai de Dades i, a més, la predisposició dels Titulars a implicar-se en el desenvolupament de l'economia digital.

En el marc de l'Espai de Dades, el Subjecte de les Dades ha de tindre la possibilitat d'exercir la seua oposició quan el tractament es basa en l'interés legítim o l'interés públic i la resta dels drets establits en el RGPD.

A més, en el cas de serveis d'intermediació de dades, podran oposar-se al fet que les seues dades siguen convertides a un altre format (el que és en sí un tractament), i se'ls ha d'oferir l'oportunitat d'això, llevat que el Dret de la Unió obligue a realitzar aquesta conversió.

En el cas que els Titulars de les Dades siguen AAPP, cobra especial rellevància l'ús de la Carpeta Ciutadana com a instrument Habilitador a l'ésser una eina addicional de transparència. En aqueixa mesura, ha de contemplar-se la millora de les possibilitats de la Carpeta Ciutadana en relació amb rebre informació suficient sobre la finalitat de nous tractaments, facilitar canals de comunicació per a resoldre dubtes o poder fer-se el consentiment o el rebuig d'alguna manera en els casos que es base en el consentiment.

"Un dels objectius dels Espais de Dades és d'establir un marc de governança de les dades. Es considera de vital importància de cara a implementar protecció de dades des del disseny. Referent a això caldria destacar la importància que els codis de conducta podrien tindre en l'Espai de Dades, així com el paper que el supervisor del codi de conducta podria exercir en relació amb la supervisió de les sol·licituds d'accés".

MATERIAL COMPLEMENTARI

- Proposta de Reglament del Parlament Europeu i del Consell sobre la governança europea de les dades (Data Governance Act, DGA) Pots consultar el Reglament en este enllac.
- Reglament (UE) 2022/1925 del Parlament Europeu i del Consell de 14 de setembre de 2022 sobre mercats disputables i equitatius en el sector digital i pel qual es modifiquen les Directives (UE) 2019/1937 i (UE) 2020/1828 (Reglament de Mercats Digitals) (Text pertinent a l'efecte del EEE). Pots consultar el reglament en aquest enllac.
- Dictamen 05/2014 sobre tècniques d'anonimització del Grup del Articulo 29. Pots consultar el Dictamen en aquest enllac.
- Dictamen 03/2013 sobre la limitació de la fi Grup del Articulo 29. Pots consultar el Dictamen en aquest enllac.

NOTÍCIES

- **L'Autoritat Catalana de Protecció de Dades (APDCAT) emet un Dictamen sobre utilització de dades biomètriques per al control de presència en el lloc de treball**

  El Dictamen s'emet en relació amb la consulta formulada pel DPD "[...] es manifeste sobre la viabilitat de les EIPD entorn de l'ús de la biometria del treballador (empremta dactilar o facial) com a sistema per a dur a terme el registre de jornada laboral dels treballadors. La APDCAT afirma que el consentiment pot ser una base jurídica habilitant del tractament amb finalitat de control horari sempre que aquest constituïsca una manifestació de voluntat lliure, específica, informada i inequívoca per part de l'interessat d'acceptar el tractament. En tot cas, abans de dur a terme un tractament com aquest, és necessari realitzar una avaluació de l'impacte sobre la protecció de dades on s'analitze, entre altres qüestions, la licitud del tractament.
  Pots consultar el Dictamen en aquest enllaç.
- **La APDCAT emet un Informe sobre accés al registre d'accessos de la Història Clínica.** Considera que els accessos a la història clínica d'un pacient realitzats pel personal, no es poden considerar informació que forme part del dret d'accés. Segons la APDCAT, la traçabilitat dels accessos a la història clínica de la reclamant formaria part del registre d'accessos a les històries clíniques. Aquesta informació és pública a l'efecte de la legislació de transparència Considerant que la informació sol·licitada no inclou dades de categoria especial (ja que les dades de salut fan referència al reclamant sol·licitant de la informació i no a les persones que han accedit a la seua història) la APDCAT conclou que la normativa no impedeix comunicar a la persona reclamant la informació que sol·licita, relativa als accessos a la seua història clínica, inclosa la identitat dels professionals, rang i categoria professional, que han accedit a aquesta.
  Pots consultar l'Informe en aquest enllaç