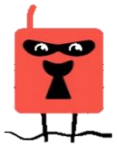
FITXES DEL DPD **Ref. 8/2021**

RGPD i Seguretat en Aplicacions i Sistemes



Aspectes de protecció de dades a tenir en compte en el desenvolupament d'aplicacions

1. Introducció. Privacitat per disseny i per defecte

- Els principis de protecció de dades personals s'han d'integrar en els desenvolupaments informàtics **des de la fase de disseny** per tal de protegir la privacitat de les dades de les persones, de manera que siguin tractades per donar un millor control sobre aquestes i limitar errors, pèrdues, modificacions no autoritzades o mal ús de les dades en les aplicacions.

- Per a determinades operacions del tractament (ús de categories especials, ús de dades a gran escala, dades biomètriques, persones vulnerables, etc.) és obligatori realitzar **una Avaluació d'Impacte relativa a la Protecció de Dades (AIPD)**. En altres casos, és una bona pràctica que permetrà identificar i mitigar els riscos dels desenvolupaments i fer-ne el corresponent seguiment.

L'Oficina del Delegat de Protecció de Dades[1] posa a disposició una metodologia i una **eina**[2] per a dur a terme l'Avaluació Relativa a la Protecció de Dades en salut basada en el model de l'Autoritat Catalana de Protecció de Dades. Amb aquesta proposta, disponible en accés obert, es pretén contribuir a homogeneïtzar i estandarditzar la metodologia i els criteris per a dur a terme la tasca d'avaluació a les entitats de salut. Aquesta eina permet aprofundir en aquests aspectes i particularitats del sector de forma coordinada i sistematitzada, repetible i comparable, i que estigui centrada en el sistema de recerca i innovació en Salut. Aquesta metodologia consta de 6 fases:

- Anàlisi prèvia: necessitat de realitzar una AIPD
- Descripció sistemàtica del tractament
- Avaluació de la necessitat i proporcionalitat
- Gestió de riscos en la seguretat de les dades (compliment amb l'Esquema Nacional de Seguretat)
- Documentació i implantació
- Monitoratge i revisió

[1] Oficina del Delegat de Protecció de Dades (DPD) de Salut, http://dpdsalut.cat

[2] Es pot consultar la Metodologia de la FTSS específica per salut. https://ticsalutsocial.cat/dpd-salut/avaluacio-dimpacte-relativa-a-la-proteccio-de-dades-aipd-en-salut/

2. Requeriments

- Representar i descriure com funcionarà l'aplicació abans d'iniciar el projecte, amb un **esquema de fluxos de dades i una descripció detallada de les operacions de tractament a realitzar**.

- **Identificar el tractament/s de dades personals**. Si son tractaments ja creats o s'han de donar d'alta al registre d'activitat de tractament de la entitat.

- **Identificar el responsable/s de tractament i encarregats**, així com el paper que juga al projecte cada agents.

- **Identificar els diferents tipus de dades** que es necessita recopilar i intenteu **limitar-la a allò que és estrictament necessari**.

- El tractament de dades personals s'ha de basar en una de **les bases legals esmentades a l'article 6 del RGPD**. La base legal d'una operació de tractament és en certa manera la justificació de l'existència d'aquesta operació. L'elecció d'una base legal té un impacte directe sobre les condicions per a l'execució de l'operació de tractament i els drets de les persones. Així, preveure la base legal de les operacions del tractament abans de qualsevol desenvolupament ajudarà a integrar les funcions necessàries per garantir que aquestes operacions compleixin la llei i respectin els drets de les persones.

- Si el processament conté dades sensibles com **les dades de salut**, haureu d'identificar, a més de la base legal, **una excepció prevista a l'article 9 del RGPD**.

- **Realitzar, si escau una avaluació d'impacte**. Per exemple, per tractaments a gran escala (tots els usuaris del sistema de salut) de categories especials (salut) seria un requisit obligatori realitzar una avaluació d'impacte.

- **Minimitzar la quantitat de dades recollides** també pel que fa a **les dades de registre (logs)** i evitar emmagatzemar dades sensibles o crítiques (dades de salut, contrasenyes, etc.).

- **Processar i emmagatzemar dades**. Si les dades encara són útils, es pot reduir la seva sensibilitat mitjançant mètodes de **pseudonimització o fins i tot d'anonimització**. En cas de pseudonimització, recordar que aquestes dades es mantenen subjectes al RGPD.

- **Gestionar perfils**. Definir perfils d'accés i autorització diferents perquè cada persona, de manera que pugui accedir només a les dades que realment necessiti.

- Tant en el cas de la recollida directa de dades als interessats, (per exemple un formulari) o quan es recopilen mitjançant dispositius o tecnologies per observar l'activitat de persones (exemples: anàlisi de la navegació a Internet, geolocalització, etc.) **s'ha d'informar als interessats sobre les circumstàncies relatives al tractament de les seves dades**[3].

[3] Consultar la guia per al compliment del deure d'informar RGPD https://apdcat.gencat.cat/es/documentacio/guies_basiques/Guies-apdcat/guia_per_al_compliment_del_deure_d_informar_RGPD/

En aquest apartat hem de tenir en compte que per aplicacions podem informar: mitjançant peus d'informació a l'apartat d'informació bàsica sobre protecció de dades i a la política de privacitat[4] . També hem d'incloure les condicions d'us de l'aplicació.

Quan la recollida d'informació l'efectua un encarregat del tractament, se li pot encomanar que informi les persones interessades.

- D'acord al principi de transparència la informació o comunicació relativa al tractament de dades personals **ha de ser concisa, transparent, comprensible i fàcilment accessible i expressada en un llenguatge clar i senzill**.

- **Definir períodes de retenció de dades**. Les dades personals no es poden conservar durant un període de temps indefinit. Cal associar períodes de retenció per a cada categoria de dades, segons l'objectiu del tractament i les obligacions legals o reguladores. Per exemple, en salut cal tenir en compte els períodes de conservació per la Història clínica. S'han de documentar les duracions de retenció definides i s'han de poder justificar. Un cop assolit aquest propòsit, les dades s'han d'arxivar, suprimir o fer anònimes (per exemple, per tal de produir estadístiques). **Els registres (logs) també han de tenir un període de retenció**. La guia per a desenvolupadors de la CNIL[5] parla de 6 mesos per a la conservació de logs.

- **Utilització de cookies i eines d'analítica**. La Directiva Europea sobre privacitat electrònica *ePrivacy* requereix el consentiment de l'usuari abans que es faci qualsevol acció per emmagatzemar informació a través de cookies, identificadors o altres rastrejadors o per accedir a la informació emmagatzemada en l'equip terminal de l'usuari. Per tant, **abans de dipositar cookies**, els administradors han de:

  - informar els usuaris de la finalitat de les cookies;
  - obtenir el seu consentiment;
  - proporcionar-los un mitjà per rebutjar-los.

Programari de codi obert com Matomo[6] , es postulen com alternatives a Google Analytics per protegir les dades i la privacitat d'usuaris, i per tal de corregir la falta de limitació del propòsit del tractament i la falta de transparència en l'ús de les dades dels clients i dades de diagnòstic per part dels serveis de Google.

[4] Decálogo para la adaptación al RGPD de las políticas de privacidad en internet AEPD: https://www.aepd.es/es/media/estudios/decalogo-politicas-de-privacidad-adaptacion-RGPD.pdf
[5] Guia desenvolupadors CNIL https://www.cnil.fr/fr/guide-rgpd-du-developpeur
[6] Matomo https://matomo.org/

MESURES DE SEGURETAT APLICABLES ALS SISTEMES D'INFORMACIÓ DE SALUT

Atenent als riscos que suposen els tractaments de dades personals de categoria especial, com les dades relatives a la salut, l'oficina del Delegat de Protecció de Dades de Salut ha realitzat un **resum de les mesures de seguretat relatives a la protecció de dades** que recomana implementar als sistemes d'informació.

Tot i que el Reglament General de Protecció de Dades[7] no estableix un llistat de les mesures de seguretat que s'han d'aplicar segons la tipologia de dades objecte de tractament, s'indica que **el responsable i l'encarregat del tractament han d'aplicar les mesures tècniques i organitzatives adequades al risc que comporta el tractament**. Per determinar les mesures de seguretat que cal implementar s'ha de fer una **avaluació dels riscos** associats prèvia a cada tractament i triar el model de bones pràctiques en seguretat de la informació que s'utilitzarà per concretar les mesures a implantar.

En el cas del **sector públic**, la disposició addicional primera de l'**LOPDGDD**[8] estableix que l'**Esquema Nacional de Seguridad**[9] (ENS) inclourà les mesures que s'hagin d'implementar en cas de tractament de dades de caràcter personal, per evitar la seva pèrdua, alteració o accés no autoritzat. Des del punt de vista de l'ENS, la seguretat de la informació contempla cinc dimensions de protecció:

1) La **confidencialitat**, que impedeix els accessos i usos no autoritzats de la informació sensible.

2) La **integritat**, que avala la inalterabilitat de les dades emmagatzemades en trànsit i en repòs.

3) La **disponibilitat**, que garanteix el correcte funcionalment i accés als serveis.

4) La **traçabilitat**, mitjançant un **registre d'activitat** dels sistemes d'informació.

5) L'**autenticitat** i l'**autorització** dels usuaris per protegir dades sensibles, que permeti controlar l'accés a la informació i als recursos, i garanteixi la identitat de les dades comunicades.

En aquest document, a demés, es contemplen tres dimensions addicionals:

6) El **no repudi**, entès com la capacitat de demostrar la participació de les parts en una comunicació.

7) L'**actualitat** de les dades implica que cada conjunt de dades és recent i vàlid.

8) La **resiliència**, la **tolerància a errades**, i l'**autoreparació** dels sistemes d'informació.

[7] RGPD (UE) 2016/679, https://www.boe.es/doue/2016/119/L00001-00088.pdf

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

[9] Real Decreto, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

Addicionalment l'oficina del Delegat de Protecció de Dades de Salut ha desenvolupat una eina, anomenada *Eina_DPD_Requisits_Seguretat_Aplicacions_Salut.xlsx*[10], que té com a finalitat facilitar als fabricants d'aplicacions comprovar i ajudar a complir amb els requisits de seguretat de la informació durant el desenvolupament d'aplicacions que tractin dades de salut, seguint els criteris i proposant les mesures preventives indicades a l'**Esquema Nacional de Seguridad** (ENS) i l'**Open Web Application Security Project** (OWASP). D'altra banda l'**Agència Europea d'Informació i Seguretat** (ENISA) ha desenvolupat una **guia de bones pràctiques per a la seguretat informàtica dels serveis sanitaris**[11] amb l'objectiu de facilitar informació sobre els requisits de ciberseguretat per a l'adquisició de serveis, productes i infraestructures als hospitals. La seguretat de la informació consisteix per tant en la implementació d'un conjunt de mesures tècniques destinades a preservar la confidencialitat, la integritat i la disponibilitat de la informació, podent a més abastir altres propietats com l'autenticació, la responsabilitat, la fiabilitat i el no repudi. La manca de mecanismes per assegurar aquests principis pot comportar **un risc alt per als drets i llibertats de les persones** físiques. Aquestes mesures de seguretat es detallen a continuació.

1. Mesures per garantir la confidencialitat

La confidencialitat fa referència al fet que la informació només ha de ser coneguda i accessible per les persones que necessiten conèixer-la i que han estat degudament autoritzades per a tractar-les.

Aquest principi assegura també que la informació no serà divulgada de manera fortuïta o intencionada, per tal de garantir-la es recomana seguir les següents mesures:

a. Xifrar en trànsit[12] de qualsevol informació a nivell de protocol de xarxa, a nivell de transport (TLS) i a nivell d'aplicació (HTTPS).

b. Xifrar en repòs[13] de la informació sensible ja sigui en local, en el núvol o en entorns híbrids per als fitxers amb informació sensible utilitzant algorismes de xifrats coneguts i fiables (per exemple AES-256), i utilitzant contrasenyes de xifrat segures (veure punt 4.f).

   i. *El xifrat en repòs pot realitzar-se tant per la banda de l'usuari abans de fer l'enviament del fitxer, utilitzant eines com 7-ZIP, com per la banda del sistema utilitzant algorismes de xifrat segur com el AES-256.*

   ii. *La contrasenya de desxifrat, o codi de desprotecció, s'ha de transmetre per una altre via diferent a la persona que s'indica i de forma separada.*

[10] Descarregar *Eina_DPD_Requisits_Seguretat_Aplicacions_Salut.xlsx*
https://ticsalutsocial.cat/wp-content/uploads/2021/05/eina-dpd-requisits_seguretat_aplicacions_salut_v2.zip
[11] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services/#/
[12] https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf
[13] https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

c. Efectuar un procés d'esborrat segur de les dades i neteja de metadades un cop acabi el termini de conservació.

e. Emprar tècniques d'anonimització[14] o en el seu defecte de pseudonimització[15] de cara a impossibilitar o dificultar la reidentificació dels subjectes i a protegir-los.

i. Les dades pseudonimitzades segueixen sent dades de caràcter personal.

ii. Des de l'oficina del DPD s'ha desenvolupat una guia sobre les tècniques i bones pràctiques de la pseudonimització .

f. Evitar sempre que sigui possible realitzar **transferències internacionals** de dades personals, i en cas de fer-les complir amb les condicions de l'article 44 de l'RGPD.

2. Mesures per garantir la integritat

La integritat de les dades es refereix a la precisió i coherència general de les dades, quan la integritat de les dades és segura, la informació emmagatzemada en una base de dades seguirà sent completa, precisa i fiable per molt temps que passi emmagatzemada o per moltes vegades que s'accedeixi a ella.

La integritat de les dades també garanteix que les seves dades estaran lluny de forces externes, i es manté gràcies a un conjunt de processos, regles i normes que es posen en pràctica durant la fase de disseny:

a. Comprendre amb quines dades treballa el sistema:

i. Com es recopilen i produeixen

ii. Si es validen abans de ser introduïes

iii. Quines son les parts més sensibles d'aquestes

b. Recopilar únicament les dades necessàries en relació amb la finalitat del tractament, tenint en compte el principi de minimització de dades de l'RGPD.

c. Realitzar periòdicament còpies dels sistemes de fitxers i de les bases de dades.

d. Emprar algorismes de xifratge asimètrics i certificats de signatura.

e. Emprar algorismes hash (p.ex. SHA-256) als conjunts de dades per verificar-ne la integritat després de transferir-los o emmagatzemar-ne còpies.

[14] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-to-the-rescue-pseudonymisation-for-personal-data-protection
[15] Veure *Guia sobre les tècniques i bones pràctiques de la pseudonimització*.

3. Mesures per garantir la disponibilitat

Ens referim a aquest terme quan parlem de l'**accés de persones o organismes a les dades** amb les què treballa, fins i tot en cas d'incidents tècnics o físics.

D'altra banda **la informació estarà disponible únicament durant el temps necessari** per dur a terme les finalitats del tractament.

Per tal de garantir la disponibilitat s'han de posar en marxa determinats mecanismes que permetin a les persones interessades i autoritzades a accedir a aquesta informació sempre que ho necessitin i puguin fer-ho de forma segura i senzilla:

a. Activar el balanceig de càrrega dels Centres de Processament de Dades (CPD), sempre que sigui possible.

b. Replicar informació i realització d'snapshots dels servidors periòdicament.

c. Monitoritzar constantment les alertes i el rendiment dels sistemes per detectar problemes i riscos amb l'objectiu d'evitar que caigui o s'aturi el servei.

d. Estructurar la informació correctament de manera que en un futur sigui possible realitzar exportacions i/o migracions cap a altres sistemes d'informació i/o proveïdors.

e. Bloquejar l'accés a les dades un cop acabi el termini de conservació establert, tal i com indiquen els principis de limitació del termini de conservació i de minimització de dades.

4. Mesures per garantir l'autenticació i l'autorització

Per tal de garantir l'autenticitat de la informació introduïda als sistemes, i permetre l'accés o modificació de les dades únicament als usuaris amb autorització, cal:

a. Proporcionar **accés i permís d'usuaris controlats** (per exemple utilitzant eines de gestió d'usuaris ja existents com GICAR).

b. Disposar de **polítiques condicionals d'accés** dels usuaris.

b. Assignar a cada usuari del sistema un **identificador d'accés als recursos únic**.

c. **Separar funcionalitats** d'usuaris administratius respecte d'usuaris ordinaris.

d. **Limitar** el número de persones amb accés a les dades sensibles.

e. Utilitzar **doble factor d'autenticació** pels usuaris que tinguin accés a informació confidencial o sensible.

f. Establir una **política de contrasenyes segura**:

   i. Forçar un canvi de contrasenya a la primera entrada de l'usuari al sistema, de manera que l'usuari en defineixi una de pròpia.

   ii. Que tingui una longitud d'entre 8 i 30 caràcters.

   iii. Que disposi de números i lletres (amb minúscules i majúscules).

   iv. Que caduqui cada 6 mesos i que no es puguin repetir les darreres 6 contrasenyes.

   v. Que no puguin contenir el NIF, data de naixement, nom ni cognom de la persona.

D'altra banda les mesures de seguretat exigibles en els accessos a les dades de caràcter personal a través de xarxes de comunicacions hauran de garantir un nivell de seguretat equivalent al corresponent als accessos en mode local. Les comunicacions en les plataformes de tractament de dades assistencials, es realitzen de manera segura, utilitzant encriptació del canal, amb certificats amb clau mínima de 2048 bits instal·lats en els servidors.

5. Mesures per garantir el no repudi

El no reputi, o la irrenunciabilitat, permet provar la participació de les diferents parts en una comunicació o en la realització d'una acció mitjançant la seva identificació. La diferència amb l'autenticació és que la primera es produeix entre les parts que estableixen la comunicació i el servei de no repudi es produeix davant d'un tercer. Hi ha dues possibilitats d'implementar-lo:

- En l'origen: L'emissor no pot negar l'enviament perquè el destinatari té proves de la mateixa. El receptor rep una prova infalsificable de l'origen de l'enviament.
- En el destí: El receptor no pot negar que va rebre el missatge perquè l'emissor té proves de la recepció. que l'han rebut.

Un exemple de no repudi seria el sistema de missatgeria de WhatsApp, que utilitza algorismes de xifrat asimètric en l'origen i destí (efectuat als dispositius mòbils) per tal de garantir la confidencialitat, integritat i autenticitat de l'usuari. L'enviament de missatges xifrats d'aquesta manera i la verificació de lectura mitjançant el doble check blau permet les dues possibilitats de no repudi, ja no podem negar que hem enviat el missatge ni poden negar que l'han rebut.

6. Mesures per garantir l'actualitat de les dades

Tenir una base de dades amb informació de qualitat i actualitzada és molt important per mantenir el valor i utilitat del conjunt d'informació, com també per evitar despeses innecessàries d'emmagatzematge i processament, i per impedir que es reprodueixin missatges o dades desactualitzades.

Les mesures que ha adoptar son les següents:

a. Verificar que les dades hagin sigut ben introduïdes i siguin vàlides abans d'introduir-les al sistema.

b. Sol·licitar periòdicament al propietari de les dades (subjecte o interessat) que verifiqui l'actualitat d'aquestes i en cas contrari que les actualitzi.

c. Utilitzar alertes que adverteixin en cas de tenir registres amb data de creació antiga o que portin molt de temps sense ser actualitzats.

d. Treballar amb bases de dades relacionals o multi-relacionals per tal de tenir segmentació avançada i facilitar la interacció amb múltiples bases de dades.

7. Mesures per garantir la resiliència

La resiliència és un terme relativament nou que està relacionat amb la capacitat que han de tenir els sistemes d'informació de recuperar-se ràpidament d'atacs deliberats o incidents que afectin l'ús de les tecnologies de la informació i la comunicació. Per assolir-la es recomana seguir aquests punts:

a. **Avaluar** la infraestructura i les dades contingudes en els sistemes amb l'objectiu de localitzar les bretxes de seguretat i jerarquitzar-les segons el seu nivell d'urgència.

b. Prendre les **mesures necessàries per garantir la protecció** dels sistemes amb la idea de minimitzar el risc d'atac i protegir cada un dels elements que interactuen en els sistemes.

c. **Monitoritzar** de forma ràpida les fonts d'atacs i els seus abastos.

d. Desenvolupar un **pla de resolució de problemes** que descrigui clarament els passos a seguir en cas d'un incident.

e. Disposar d'estratègies que permetin la **restauració** ràpida d'aquelles dades i serveis afectats per l'atac.

8. Disposar d'un registre d'activitats

Els sistemes d'informació han de disposar d'un registre de traces, en anglès *logs*, que permeti deixar constància de, per exemple: l'accés de cada usuari, la data i hora en que es va realitzar, el programa, servei o aplicació al que s'ha accedit, l'acció que ha realitzat, el temps d'activitat i si s'ha autoritzat o denegat l'accés.

El registre d'accessos no pot quedar desactivat, de manera que si es detecta algun problema en relació a accessos no autoritzats, el registre ha de permetre controlar els accessos o intents d'accessos que s'hagin produït.

Si les traces o *logs* contenen informació de caràcter personal, com l'adreça IP, el correu electrònic, el codi CIP, el DNI, el codi d'usuari, etc., aquestes han d'estar correctament xifrats per tal de garantir la confidencialitat de les dades.

Podeu trobar més informació sobre la gestió de *logs* en el següent enllaç [16].

Podeu fer-nos arribar consultes, suggeriments i idees de millora enviant un correu electrònic a: dpd@ticsalutsocial.cat.

[16] Política de seguridad para la pyme (Instituto Nacional de Ciberseguridad), https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

CONCEPTES CLAU

- **Dada personal**: Qualsevol informació sobre una persona física identificada o identificable (l'interessat). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament, per exemple el nom i cognom o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona. Per tant, entre les dades personals s'inclou per exemple: la direcció IP, el identificador d'un dispositiu mòbil, l'identificador dels navegadors, les identificacions dels comptes d'usuari i qualsevols altra forma de dades generades pel sistema que identifiqui a una persona física.

- **Dada personal de salut**: Qualsevol informació relacionada amb la salut física o mental d'una persona física que revelen informació sobre el seu estat de salut, inclosa la prestació de serveis d'atenció sanitària. Es tracta d'informació especialment sensible que afecta de ple a la intimitat de les persones. S'interpreta aquesta categoria de dades en sentit ampli, no es tracta només d'informació mèdica. Per exemple: Informació sobre l'estat de salut present, passada o futura, número o codi identificador assignat a efectes sanitaris (CIP i número de HC), informació sobre una malaltia o una discapacitat, etc.

- **Responsable del tractament**: persona física o jurídica, autoritat pública o qualsevol organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament.

- **Encarregat del tractament**: la persona física o jurídica, autoritat o organisme que tracta dades personals per compte del responsable.

- **Tractament de dades personals**: qualsevol operació o conjunt d'operacions realitzades sobre dades personals, ja sigui per procediments automatitzats o no (la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la supressió, etc.).

- **Procés d'anonimització de dades personals**: té com a objectiu fer impossible la identificació de persones dins dels conjunts de dades. Per tant, és un procés irreversible. Quan aquesta anonimització és efectiva, **les dades ja no es consideren dades personals i els requisits del RGPD ja no són aplicables**.

- **Pseudonimització** fa referència al tractament de dades personals de manera que ja no es poden atribuir dades relacionades amb una persona física **sense informació addicional**. El RGPD insisteix que aquesta informació addicional que permet reidentificar les dades pseudonimitzades s'ha de conservar per separat i estar sotmesa a mesures tècniques i organitzatives per evitar la identificació de les persones interessades. A diferència de l'anonimització, la pseudonimització és un procés reversible. **Les dades derivades de la pseudonimització es consideren dades personals**. Per tant, en el procés de pseudonimització es **substitueix les dades identificatives directament (cognoms, nom, etc.) per dades identificatives indirectament** (generades per un comptador, un generador de nombres aleatoris, un sistema de xifratge, etc.) per tal de reduir la seva sensibilitat. Les dades pseudonimitzades també poden resultar d'aplicar un hash criptogràfic a les dades originals de l'usuari: com ara l'adreça IP, l'ID d'usuari, l'adreça de correu electrònic, etc.

TRACTAMENT DE DADES PERSONALS

- Qualsevol operació sobre dades personals **(recollida, enregistrament, transmissió, modificació, difusió, etc.)** constitueix un tractament en el sentit del RGPD i, per tant, ha de complir els requisits establerts pel reglament. Aquestes operacions de tractament han de ser lícites i tenir un propòsit específic. Les dades personals recollides i tractades han de ser les mínimes necessàries i limitar-se a allò que és estrictament necessari per assolir la finalitat en qüestió.

- Qualsevol tractament de dades personals només és lícit **si tenim una base de legitimació** que ens permet fer-lo. Les diferents bases possibles es recullen a l'article 6 RGPD, i són:
  - Consentiment de l'interessat
  - Execució d'un contracte
  - Obligació legal
  - Protecció d'interessos vitals
  - Interès públic o en l'exercici de poders públics
  - Satisfacció d'interessos legítims

- Quan el tractament afecta a categories especials de dades, com ara dades relatives a la salut, l'article 9 de l'RGPD estableix una prohibició general de tractament, sense perjudici d'unes excepcions. Les circumstàncies en què l'RGPD permet tractar aquestes categories especials de dades són les següents:
  - **El consentiment és explícit**.
  - El tractament és necessari per complir obligacions.
  - El tractament és efectuat per una entitat sense ànim de lucre que tingui una finalitat política, filosòfica, religiosa o sindical.
  - El tractament és necessari per protegir interessos vitals d'una persona.
  - La persona les ha fet manifestament públiques.
  - El tractament és necessari per raons d'un interès públic essencial.
  - **El tractament està vinculat a temes de salut de la persona o salut pública**.
  - Es tracten amb fins d'arxiu o la investigació científica o històrica.

- L'administració pública actua la majoria de vegades sota "L'Interès públic o en l'exercici de poders públics" i en aquest cas, es necessari una llei que avali el tractament. La llei contempla que els centres de la xarxa de salut pública poden tractar les dades dels seus pacients per prestar assistència sanitària.