Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca

31 de juliol de 2020

Generalitat de Catalunya
Departament de Salut

S/Sistema de
Salut de Catalunya

Editen:

Direcció General de Recerca i Innovació en Salut.

Direcció General d'Ordenació i Regulació Sanitària.

Oficina del DPD - Fundació TIC SALUT SOCIAL.

1a edició:

Barcelona, juliol de 2020.

Revisió corporativa:

Oficina de Comunicació.

Número de registre editorial:

82780

Disseny de plantilla accessible 1.04:

Oficina de Comunicació. Identitat Corporativa

Sumari

1 Objectius del document

Aquest document és una guia informativa dels principals aspectes que en matèria de protecció de dades s'han de tenir en compte a l'hora d'avaluar projectes de recerca, tant pel membre expert en protecció de dades dels CEI o CEIm, com pels avaluadors.

A fi de facilitar la tasca d'avaluació, s'inclouen enllaços a diversos documents que fixen els principals criteris interpretatius, i permeten ampliar informació de tots els temes per avaluar.

També conté una proposta de taula amb la informació que ha de contenir el protocol i el full d'informació i consentiment per tal que promotors i investigadors tinguin coneixement de la informació que ha de constar-hi, així com una proposta de metodologia per als avaluadors a fi de facilitar-les-hi la tasca d'avaluació dels aspectes de protecció de dades perquè siguin capaços d'identificar les situacions de risc l'avaluació de les quals cal comentar amb l'expert en protecció de dades del CEI o CEIm.

Els apartats IV (Aspectes que s'han d'incloure en el protocol dels projectes de recerca des de la perspectiva de la protecció de dades) i V (Metodologia per avaluar els aspectes derivats de la normativa de protecció de dades en projectes de recerca) d'aquesta guia es poden distribuir com a documents independents, però fent referència al document principal.

2 Introducció

La realització d'un projecte de recerca implica el tractament de categories especials de dades, i per tant s'hauran de tenir en compte les previsions establertes a l'article 9 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant el RGPD).

Així mateix, cal atenir-se a la regulació establerta per la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (en endavant la LOPD-GDD), en especial a la seva Disposició Addicional 17.2, on es desenvolupen els criteris per al tractament de dades per recerca.

Els criteris interpretatius de la normativa de protecció de dades en l'àmbit de la recerca s'han anat establint a través de diversos documents, tant d'àmbit estatal com europeu, en especial destaquem:

- ✓ EC - Document Guidelines on FAIR Data Management in Horizon 2020, de la Comissió Europea de 26 de Juliol de 2016.

- ✓ EC - Document Ethics and data protection, de la Comissió Europea de 4 de Febrer de 2019.
- ✓ EC - Document Guidance How to complete your ethics self-assessment, de la Comissió Europea de 14 de Novembre de 2018.
- ✓ APDCAT - Dictamen 15/2019 en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut pseudonimitzades en investigació biomèdica de 14 de maig de 2019.
- ✓ APDCAT - Dictamen 18/2019 en relació amb la consulta d'una associació de l'àmbit sanitari sobre diferents aspectes relacionats amb l'apartat 2 de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de 14 de maig de 2019.
- ✓ EDPB - Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (RGPD) (art.70.1.b)), adopted on 23 January 2019.
- ✓ EDPB - Guidelines 03/2020 on the processing of data concernint health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020.
- ✓ APDCAT - Dictamen 14/2020 en relació amb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital, de 27 d'abril de 2020.
- ✓ BIOÈTICA - Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de covid-19, de 28 de abril de 2020.

A fi d'avaluar els aspectes relatius a la protecció de dades en un projecte de recerca, els avaluadors del CEI o CEIm hauran de verificar que el protocol disposa d'una sèrie d'ítems indicats a l'apartat **IV** d'aquest document i per analitzar-los es podran basar en la metodologia proposada a l'apartat **V.**

Així mateix, per avaluar l'adequació del protocol al RGPD, s'han de tenir en compte els **conceptes de protecció de dades en l'àmbit de recerca i la seva interpretació** indicats en aquest document, i que són un reflex dels documents i informes emesos per les autoritats competents en matèria de protecció de dades, i altres organismes d'àmbit europeu.

3 Conceptes bàsics de protecció de dades i la seva interpretació en l'àmbit de recerca

3.1 Naturalesa de les dades com a dades personals

El RGPD s'aplica a les dades personals, entenent com a tal, la informació relativa a una persona física identificada o identificable.

Una persona física identificable és aquella que pot ser identificada, directament o indirectament, en particular fent referència a un identificador com ara un nom, un número d'identificació, unes dades d'ubicació, un identificador en línia o un o més factors específics per als aspectes físics, fisiològics, genètics, mentals, econòmics, identitat cultural o social de la persona física.

Exemples: nom, adreça, número d'identificació, pseudònim, ocupació, correu electrònic, CV, dades d'ubicació, adreça del protocol d'Internet (IP), identificador de galetes, número de telèfon, imatge o CIP.

Les dades anònimes no queden sotmeses a la normativa de protecció de dades. En cas que el protocol indiqui que les dades estan anonimitzades s'ha de descriure el sistema d'anonimització. En aquest sentit l'AEPD va emetre un document relatiu a l'anonimització on podem trobar més informació "Orientaciones y garantías en los procedimientos de anonimización de datos personales".

Cal distingir aquest concepte de les dades pseudonimitzades entenent que unes dades han estat pseudonimitzades quan ja no es puguin identificar sense necessitat de disposar d'informació addicional, que estigui per separat, i que s'hagin aplicat una sèrie de mesures tècniques i organitzatives enfocades a evitar la reidentificació.

En el marc de la recerca cal que existeixi una separació tècnica i funcional entre l'equip investigador i els encarregats de realitzar la pseudonimització i conservar la informació que permeti la reidentificació, si fos necessària.

En cas de no existir aquesta separació tècnica i funcional, estaríem davant el que comunament es coneix en l'àmbit de recerca com a codificació. En els dos casos, pseudonimització i codificació, ens trobem sota l'aplicació de la normativa de protecció de dades. Podem trobar més informació en relació amb la pseudonimització a l'informe de l'AEPD "Introducción al hash como técnica de seudonimización de datos personales", i al document d'ENISA "Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions".

"Tractament de dades personals" significa qualsevol operació (o conjunt d'operacions) realitzada a les dades personals, de forma manual o automàtica.

Exemples: accés/consulta d'una base de dades que conté dades personals; gestió de la base de dades; publicar/posar una foto d'una persona en un lloc web; emmagatzemar adreces IP o adreces MAC; enregistrament de vídeo (CCTV); crear una llista de correu o una llista de participants.

El concepte de tractament de dades personals inclou qualsevol acció que utilitzi dades amb finalitats de recerca (fins i tot la revisió de registres a l'efecte d'identificar els participants en un projecte o l'accés a dades per anonimitzar-les).

Les dades personals poden procedir de qualsevol tipus d'activitat investigadora (investigació TIC, genètica, recollida de mostres, emmagatzematge de teixits), registres personals (educació, finances, penal, etc.), informació sobre l'estil de vida i la salut, històries familiars, característiques físiques, sexe i ètnia, informació sobre el seguiment de la ubicació i el domicili, etc.).

Cal recordar que la normativa de protecció de dades, de conformitat amb el que estableix el considerant 27 del RGPD, no s'aplica a les dades de difunts.

3.2 Principi de minimització de les dades

El tractament de les dades ha de ser **lícit**, **just** i **transparent**.

Només s'han d'incloure les dades que siguin **necessàries i proporcionades** per assolir la tasca o finalitat específica per a la qual van ser recollides (article 5.1, RGPD).

Així, **només s'han de recollir les dades que siguin necessàries per assolir els objectius de la recerca**, per tant, el seu tractament ha de tenir un propòsit específic rellevant i limitat als objectius i a la metodologia del projecte.

La minimització de dades s'aplica no només a la quantitat de dades personals recollides, sinó també a la forma en que s'hi podrà accedir, es podran processar i compartir, els motius pels quals s'utilitzen, així com el període de conservació.

Si no es pot identificar del tot el propòsit del tractament de dades en el moment de la recollida de dades o és necessari mantenir les dades més enllà de la durada del projecte, s'ha d'explicar i justificar.

3.3 Privacitat des del disseny i per defecte

El RGPD, a través de l'article 25 introdueix els conceptes de privacitat en el disseny i privacitat per defecte. La interpretació d'aquest concepte ha esta feta per l'EDPB a través del "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default."

- Privacitat des del disseny

Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades i integrar en el tractament les garanties necessàries per complir els requeriments del Reglament.

En aquest sentit, la Comissió Europea ha acordat que s'han d'establir mesures tècniques i organitzatives a les primeres fases del disseny de les operacions del tractament, de manera que es garanteixi la intimitat i els principis de protecció de dades des del primer moment («protecció de dades des el disseny»). L'ús de

tècniques de pseudonimització i de xifratge són exemples de privacitat des del disseny.

La AEPD disposa de la Guia de Privacitat des del Disseny, en la qual es detallen els principis que cal tenir en compte.

- Privacitat per defecte

Així mateix, el responsable ha d'aplicar les mesures tècniques i organitzatives adequades per garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament. Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a l'accessibilitat de les dades.

En aquest sentit, la Comissió Europea ha establert que s'ha de garantir que les dades personals es tracten amb la major protecció de la intimitat (per exemple, només les dades necessàries, un termini de conservació curt i accessibilitat limitada), de manera que per defecte les dades personals no siguin accessibles a un nombre indefinit de persones («protecció de dades per defecte»). La principal manifestació d'aquest principi en els projectes de recerca seria la de recollir per defecte el mínim de dades possibles per realitzar el projecte.

És especialment important garantir aquests principis en els projectes de recerca relacionats amb la creació de solucions tecnològiques. En aquest sentit, l'Autoritat Noruega de Protecció de Dades va elaborar el document *Software development with Data Protection by Design and by Default*, on s'estableixen els criteris que s'han de tenir en compte des del punt de vista de la privacitat des del disseny i per defecte en el desenvolupament de solucions de programari.

3.4 Principi de transparència

El RGPD, a través del seu article 5, introdueix el principi de transparència que significa que les dades personals seran processades de forma justa i transparent en relació amb la persona afectada. Aquest principi està relacionat amb l'obligació d'informació d'acord amb l'article 13 o l'article 14 RGPD.

Com a criteri general, s'haurà d'informar individualment a un subjecte de l'existència del tractament de dades amb finalitats de recerca, incloent-hi tots els punts de l'article 13 i 14 RGPD.

El full d'informació del participant en el projecte de recerca, ha de permetre informar adequadament del tractament de les dades personals del participant a l'assaig, ha de contenir la informació mínima establerta a l'article 13 del RGPD, a més d'altra informació relativa al tractament d'aquestes dades, que inclourà:

- La identitat del responsable o coresponsables del tractament de les dades i davant de qui i com poden exercir els seus drets.
- La identificació de la forma de contacte amb el Delegat de Protecció de Dades.
- La descripció de les finalitats del tractament de les dades, i comunicacions previstes, incloent –hi les transferències internacionals de dades.

- El tipus d'informació que es recull i el termini durant el qual es conservaran les dades.
- Les mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.
- El dret a conèixer perquè s'utilitzen les seves dades; qui les té; a qui les pot cedir; a sol·licitar al responsable la cancel·lació de les dades i el dret a la rectificació de les dades quan siguin inexactes o estiguin incompletes.
- El dret a retirar el consentiment en qualsevol moment i la informació identificable de la base de dades de salut, així com el dret a sol·licitar i rebre informació sobre les seves dades i el seu ús.
- El dret a presentar una reclamació davant l'autoritat competent.
- Una breu descripció de les mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.

De vegades, els investigadors tracten dades de salut que no han obtingut directament del titular de les dades, sinó que s'han obtingut de registres de pacients. D'acord amb l'article 89 del RGPD, en el cas de l'ús secundari de dades personals en l'àmbit de la recerca, es lliurarà la informació a l'interessat en un termini raonable abans de la implementació del nou projecte de recerca.

Aquest deure d'informació només es podrà excepcionar quan concorrin les situacions indicades a l'article 14.5 del RGPD. Una d'aquestes situacions, per exemple, es pot donar quan es requereixen esforços desproporcionats, com seria si disposem d'un gran nombre d'informació sense dades de contacte, però els responsables hauran de prendre les mesures que garanteixin els drets dels titulars de les dades.

3.5 Avaluació d'impacte

El RGPD, al seu article 35, estableix que en aquells casos en els quals sigui probable que els tractaments comportin un alt risc per als drets i llibertats de les persones físiques, incumbeix al responsable del tractament realitzar una avaluació d'impacte relativa a la protecció de dades, que avaluï, en particular, l'origen, la naturalesa, la particularitat i la gravetat del risc.

Per altra banda, de conformitat amb la disposició addicional 17.2.f de la LOPD-GDD, qualsevol projecte de recerca amb dades realitzat d'acord amb el que estableix l'article 89 del RGDP, requerirà la realització d'una avaluació d'impacte, sempre i quan estiguem en una de les situacions previstes a l'article 35 del RGPD, o ens troben en un dels supòsits previstos per les Autoritats de protecció de dades.

Es considera que el tractament de dades suposa un alt risc per als drets i les llibertats dels participants en la investigació quan es duen a terme perfilats, seguiment sistemàtic d'individus o processament a gran escala de categories especials de dades o s'utilitzen mètodes intrusius de processament de dades (com ara seguiment, vigilància, enregistrament d'àudio i vídeo, seguiment de geolocalització, etc.).

La AEPD i l'APDCAT han publicat uns llistats dels tractaments que requereixen la realització d'una avaluació d'impacte, de conformitat amb el que estableix l'article 35.4 del RGPD, conjuntament amb unes guies i metodologies de com es poden dur a terme les avaluacions d'impacte.

A fi de determinar quan es necessari realitzar una avaluació d'impacte també s'ha de tenir en compte el document de l'EDPB "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".

En aquest sentit els llistats de la AEPD i l'APDCAT estableixen una sèrie de supòsits, i indiquen que si es donen dos o més de les situacions enunciades serà necessari realitzar una avaluació d'impacte.

Donades les característiques dels projectes de recerca és altament probable que sigui necessari realitzar la corresponent avaluació d'impacte d'acord amb el que estableix l'article 35.3 RGPD, ja que a l'àmbit de la recerca serà molt habitual que es donin dos o més supòsits dels indicats a les llistes de la AEPD i l'APDCAT.

El CEIm no ha de dur a terme l'avaluació d'impacte sinó que ha de verificar que existeix, així com que el seu resultat no evidencia l'existència de cap incompliment del RGPD en el marc del projecte de recerca. El responsable del tractament, amb l'assessorament del Delegat de Protecció de Dades, ha de dur a terme l'avaluació d'impacte.

Finalment, cal indicar que no és necessari realitzar una avaluació d'impacte per a cada projecte de recerca concret, sinó que és possible que determinats projectes de recerca comparteixin una mateixa avaluació d'impacte. S'haurà d'avaluar en cada cas la necessitat de realitzar una avaluació d'impacte específica per al projecte, i que vindrà determinada per l'existència d'elements únics i característics d'aquest projecte, per exemple els projectes amb un alt component tecnològic com seria l'avaluació d'un algoritme, l'ús d'una App en el projecte de recerca o l'ús de tecnologies Big Data).

3.6 Bases legítimes i supòsits de tractament de dades per recerca

Per utilitzar categories especials de dades, com són les dades de salut amb finalitats de recerca, hem d'utilitzar alguna de les bases legítimes de l'article 6 del RGPD, així com aixecar la prohibició de tractament d'aquesta categoria especial de dades que estableix l'article 9.1 del RGPD, utilitzant algun dels supòsits de l'article 9.2 del RGPD, i en relació amb l'article 89 del RGPD. L'ús d'aquestes bases legitimadores es concreta en diversos supòsits que permeten l'ús de dades per recerca i que es desenvolupen mitjançant la disposició addicional 17 de la LOPD-GDD.

Per interpretar aquest conjunt normatiu s'ha de tenir en compte també el que estableixen els considerants 26, 28, 33, 34, 52, 53, 54 i 83. Així mateix, hem de tenir en compte diversos pronunciaments de les autoritats nacionals i europees en matèria de protecció de dades que han anat interpretant i concretant l'abast d'aquestes disposicions.

Aquests pronunciaments són:

- ✓ APDCAT - Dictamen 15/2019 en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut pseudonimitzades en investigació biomèdica de 14 de maig de 2019.
- ✓ APDCAT - Dictamen 18/2019 en relació amb la consulta d'una associació de l'àmbit sanitari sobre diferents aspectes relacionats amb l'apartat 2 de la disposició addicional dissetena de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de 14 de maig de 2019.
- ✓ EDPB - Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (RGPD) (art.70.1.b)), adopted on 23 January 2019
- ✓ EDPB - Guidelines 03/2020 on the processing of data concernint health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020.
- ✓ APDCAT - Dictamen 14/2020 en relació amb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital, de 27 d'abril de 2020.
- ✓ BIOÈTICA – Informe del Comitè de Bioètica d'Espanya sobre els requisits ètics i legals en recerca amb dades de salut de 8 d'abril de 2020.

Com a punt de partida, és rellevant indicar que la pròpia LOPD-GDD, a través de la disposició final novena, ha modificat la Llei 41/2002, de 14 de novembre, bàsica, reguladora de l'autonomia del pacient i dels drets i obligacions en matèria d'informació i documentació clínica, que té la consideració de llei bàsica, i que regula, entre d'altres, l'accés a la història clínica, i les finalitats amb les quals es pot dur a terme, incloent-hi la recerca. La modificació suposa una remissió a la disposició addicional 17 de la LOPD-GDD, on es regula el règim de l'ús de dades de salut.

Per tant, en la interpretació de tot aquest conjunt normatiu, cobra especial rellevància la disposició addicional 17 de la LOPD-GDD, i permet inferir que els supòsits que permeten tractar dades de salut amb finalitats de recerca són molt amplies, i les podem agrupar en:

- Marc normatiu en l'àmbit de salut (art. 6.1.c.), d), e) i f)+ 9.2.g), h), i) i j)

En primer lloc, i a través de l'apartat primer de la Disposició addicional dissetena, es preveuen una sèrie de supòsits on els tractaments de dades de salut per a finalitats de recerca, previstos a diverses normes estatals, poden trobar cobertura en diferents supòsits del RGPD (art. 9.2.g), h), i) i j) RGPD), que aixequen la prohibició de tractar dades de categories especials, entre d'altres, les dades de salut, i n'habiliten el tractament. Aquest és el llistat de normes que enumera la disposició addicional 17.1:

a) La Llei 14/1986, de 25 d'abril, general de sanitat.

b) La Llei 31/1995, de 8 de novembre, de prevenció de riscos laborals.

c) La Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.

d) La Llei 16/2003, de 28 de maig, de cohesió i qualitat del Sistema Nacional de Salut.

e) La Llei 44/2003, de 21 de novembre, d'ordenació de les professions sanitàries.

f) La Llei 14/2007, de 3 de juliol, de recerca biomèdica.

g) La Llei 33/2011, de 4 d'octubre, general de salut pública.

h) La Llei 20/2015, de 14 de juliol, d'ordenació, supervisió i solvència de les entitats asseguradores i reasseguradores.

i) El text refós de la Llei de garanties i ús racional dels 105 medicaments i productes sanitaris, aprovat pel Reial decret legislatiu 1/2015, de 24 de juliol.

j) El text refós de la Llei general de drets de les persones amb discapacitat i de la seva inclusió social, aprovat pel Reial decret legislatiu 1/2013, de 29 de novembre.

Per tant, quan ens trobem en l'àmbit d'aquestes normes haurem d'analitzar si el text de la norma ens dóna habilitació suficient per dur a terme el tractament de dades amb finalitats de recerca.

- Consentiment (Article 6.1.a + 9.2.a RGPD)

Aquest primer supòsit permet el tractament de dades de categories especials, com són les de salut, basant-nos en l'existència del consentiment. Aquest consentiment ha de ser explícit i lliure. Només es podrà utilitzar per aquesta via quan no existeixi un desequilibri entre les parts.

En aquest sentit, l'EDPB ha establert que en determinats supòsits en el marc dels assaigs clínics pot donar-se aquest desequilibri entre les parts, i per tant serà necessari acudir a una altra base legitimadora pel que s'haurà d'estar al cas concret. Veure Opinion 3/2019 concerning the Questions and Answers on the

interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (RGPD) (art.70.1.b)).

Aquest consentiment es pot obtenir per tractar dades per a un projecte de recerca concret, o bé atenent al que estableix la disposició addicional 17.2.a), es pot obtenir per tractar dades per a finalitats que abastin "categories relacionades amb àrees generals vinculades a una especialitat mèdica o investigadors". Aquesta previsió ens obra la porta a demanar dades per ser utilitzades en diversos projectes de recerca.

- Ús amb finalitats de recerca per a salut pública (Article 6.1.e + 9.2.j RGPD)

La disposició addicional 17.2.b, estableix la possibilitat de tractar dades de categories especials, i habilita el seu tractament sense consentiment dels afectats, sempre que es compleixin dos requisits. En primer lloc, que el tractament sigui dut a terme per una autoritat sanitària o institució pública competent en vigilància de salut pública i, en segon lloc, que es donin unes circumstàncies d'excepcional rellevància i gravetat per a la salut pública.

Per analitzar aquest supòsit cal que tinguem en compte els criteris indicats a Guidelines 03/2020 on the processing of data concernint health for the purpose of scientific research in the context of the COVID-19 outbreak, i al Dictamen 14/2020 en relació a mb la consulta d'un hospital sobre l'accés a dades dels seus professionals en el marc d'un estudi científic desenvolupat en un altre hospital.

- Reutilització de dades (Article 6.1.e + 9.2.j + 89 RGPD)

La reutilització de dades es preveu a la disposició addicional 17.2. c, i a la disposició transitòria sisena de la LOPD-GDD (aquesta amb relació a les dades recollides abans de l'entrada en vigor de la LOPD-GDD). Aquesta legitimació es basa en la previsió feta per l'article 9.2.j RGPD que permet utilitzar les dades amb finalitats compatibles incloent-hi la recerca en el termes de l'article 89 del RGPD, que al seu torn es remet a la legislació de cada país. Es tracta doncs d'un cas d'ús secundari de dades amb finalitats de recerca compatible amb el RGPD.

En aquest sentit, podem veure el document Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de covid-19, on es reflexiona sobre l'ús secundari de dades per recerca.

Per poder basar-se en aquest supòsit, caldrà donar compliment al deure d'informació del titular de les dades (rat. 13 RGPD) i disposar del corresponent informe favorable del CEIm.

- Pseudonimització de dades (art. 6. e) i f) + 9.2. j) + 89 RGPD)

En primer lloc, s'ha de fer referència a que el concepte de pseudonimització vol dir "el tractament de dades personals de manera que ja no es puguin atribuir a un interessat sense utilitzar una informació addicional, sempre que aquesta informació consti per separat i estigui subjecta a mesures tècniques i organitzatives

destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable." (art.4.5. RGPD).

La pseudonimització al RGPD es configura com una mesura tècnica, i s'ha de distingir de l'anonimització, ja que a diferència d'aquesta, a les dades pseudonimitzades els hi és plenament aplicable la normativa de protecció de dades (art. 6.4.e), 25.1, i 32.1.a)) RGPD, entre d'altres.

L'habilitació en la qual es basa la disposició addicional 17.2 d, es fonamenta en l'article 9.2.j), en connexió amb l'article 89.1, els dos de l'RGPD, sobre quan el tractament és necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics del responsable del tractament (article 6.1.e) RGPD), o també si és necessari per a la satisfacció d'interessos legítims del responsable o d'un tercer (article 6.1.f) RGPD).

És a dir, podem utilitzar dades pseudonimitzades, per a finalitats de recerca d'acord amb el que estableix la disposició addicional 17.2.d, garantint que existeix:

- Una separació tècnica i funcional entre l'equip investigador i els que duguin a terme la pseudonimització i conservin la informació que possibiliti la reidentificació.

- Que les dades pseudonimitzades únicament siguin accessibles per a l'equip de recerca quan:

  i) Hi hagi un compromís exprés de confidencialitat i de no dur a terme cap activitat de reidentificació.

  ii) S'adoptin mesures de seguretat específiques per evitar la reidentificació i l'accés de tercers no autoritzats.

Es pot procedir a la reidentificació de les dades al seu origen quan, amb motiu d'una recerca que utilitzi dades pseudonimitzades, s'aprecií que hi ha un perill real i concret per a la seguretat o la salut d'una persona o un grup de persones, o una amenaça greu per als seus drets o quan sigui necessària per garantir una assistència sanitària adequada.

Així mateix, quan utilitzem dades pseudonimitzades per a la recerca, també haurem de garantir el compliment d'allò que estableix l'apartat f i g de la disposició addicional 17, que reproduïm a continuació:

> "f) Quan de conformitat amb el que preveu l'article 89 del Reglament (UE) 2016/679 es dugui a terme un tractament amb finalitats de recerca en salut pública i, en particular, biomèdica s'ha de procedir a:
>
> **1r** Dur a terme una **avaluació d'impacte** que determini els riscos derivats del tractament en els supòsits previstos en l'article 35 del Reglament (UE) 2016/679 o en els establerts per l'autoritat de control. Aquesta avaluació ha d'incloure de manera específica els

riscos de reidentificació vinculats a l'anonimització o la pseudonimització de les dades.

2n Sotmetre la recerca científica a les normes de qualitat i, si s'escau, a les directrius internacionals sobre bona pràctica clínica.

3r Adoptar, si s'escau, mesures dirigides a garantir que els investigadors no accedeixen a dades d'identificació dels interessats.

4t Designar un representant legal establert a la Unió Europea, de conformitat amb l'article 74 del Reglament (UE) 536/2014, si el promotor d'un assaig clínic no està establert a la Unió Europea. Aquest representant legal pot coincidir amb el que preveu l'article 27.1 del Reglament (UE) 2016/679.

g) L'ús de dades personals pseudonimitzades amb finalitats de recerca en salut pública, i en particular biomèdica, s'ha de sotmetre a l'informe previ del comitè d'ètica de la recerca previst en la normativa sectorial. Si no existeix aquest comitè, l'entitat responsable de la recerca ha de requerir un informe previ del delegat de protecció de dades o, si no n'hi ha, d'un expert amb els coneixements previs a l'article 37.5 del Reglament (UE) 2016/679."

El RGPD, introdueix el concepte de pseudonimització, i regula la realització de projectes de recerca amb dades pseudonimitzades a través de la disposició addicional 17.2.d. En l'avaluació d'aquest tipus de projectes, s'han de tenir en compte diversos aspectes, tant relatius als requisits establerts per la pròpia LOPD-GDD, com als principis bàsics de recerca interpretats a la llum d'aquesta normativa (necessitat de justificar la pertinença científica de l'estudi, separació tècnica i funcional entre l'equip investigador i qui realitza la pseudonimització, necessitat de realitzar una avaluació d'impacte).

- Els estudis retrospectius en l'àmbit de la recerca

Finalment, cal fer menció d'un tipus d'estudi on es donen moltes controvèrsies en relació amb la necessitat de consentiment, o d'una altra base legitimadora, com són els estudis retrospectius.

És un tema bastant complex de resoldre, ja que són una tipologia d'estudis on la línia entre assistència i recerca es desdibuixa. Així mateix, hi ha la dificulta p e r trobar una base legítima en l'àmbit de la recerca adequada per al tractament d'aquestes dades ja que, per una banda és difícil localitzar el pacient i, per altra banda, es requereix una traçabilitat de les dades.

Com a pas previ, hem de partir de que quan estem en l'àmbit de recerca, abans d'iniciar el projecte en si, el professional ha de fer una cerca de pacients a la seva base de dades assistencials per saber quins poden ser candidats a participar en l'estudi

de recerca (segmentació), i per aquest motiu cal que el procediment sigui realitzat per un professional que legítimament pugui accedir a aquestes dades. Per tant, fent una interpretació àmplia d'aquest concepte podem entendre que pot ser qualsevol professional de l'equip mèdic que atén el pacient, en qualsevol de les patologies que pot desenvolupar.

Un cop realitzada aquesta segmentació, i si considerem que estem en l'àmbit de la recerca, cal disposar de la base legítima per dur a terme l'estudi de recerca, és a dir o bé pseudonimitzem, demanem el consentiment, o ens basem en la reutilització de dades.

En aquest punt cal fer esment de la frontera que existeix entre recerca i assistència, ja que de vegades alguns CEIm aproven aquests tipus d'estudis sense necessitat de consentiment, ni de la concurrència de cap altra base legal, per considerar que estem davant d'una revisió d'històries clíniques amb finalitats assistencials, però aquesta interpretació no és acceptable, ja que si un projecte retrospectiu es sotmet al dictamen del CEIm o del CEI, és perquè té la consideració de recerca.

Si considerem que el tractament de dades té una finalitat de millora de la qualitat assistencial, i que aquest és l'objecte de la revisió retrospectiva de les històries clíniques, no s'ha de passar com a projecte de recerca pel CEIm. Aquest fet té com a conseqüència, que al no entendre aquet projecte com a recerca, sinó com a millora de la qualitat assistencial al centre, els resultats obtinguts tampoc seran susceptibles de publicar-se en revistes científiques (ja que demanen el dictamen favorable del CEI o CEIm per publicar els articles científics).

Si considerem que l'objecte d'aquests estudis retrospectius és la recerca, és a dir, volem confirmar una hipòtesi mitjançant l'ús de dades, i per tant es genera un nou coneixement científic, sotmetrem el projecte al dictamen del CEI o CEIm, i el resultat es podrà publicar en revistes científiques, però caldrà que concorri alguna de les bases legitimadores de l'ús de dades per recerca.

3.7 Relacions amb tercers, encarregats de tractament i transferències internacionals

Un "tercer", en l'àmbit de la recerca, l'hem d'entendre com aquella persona o entitat que no és ni el pacient ni el metge responsable que obté les dades de salut per a l'estudi.

En el context d'un projecte de recerca, l'enviament de dades de salut al promotor (sigui comercial o acadèmic) o a un registre ubicat fora del servidor del centre on estan allotjades, es considera una comunicació de dades a tercers, encara que estiguin codificades o pseudonimitzades, doncs als dos casos les dades (la informació) són identificables, amb més o menys dificultat.

La comunicació de dades és un tractament, i per tant, caldrà que disposi d'una base legítima, ja sigui el consentiment del titular o una de les altres previstes a l'article 6 del RGPD, i concorri algun dels supòsits de l'article 9 RGDPD que permetin aixecar la prohibició de tractament de les categories especials de dades.

En relació amb l'encarregat de tractament, és el supòsit previst a l'article 28 del RGPD, i es dóna quan el "tercer" és una empresa de prestació de serveis, com per exemple una empresa que gestiona el lliurament de medicació a casa dels participants en un estudi. En aquests casos caldrà verificar que s'ha signat amb l'empresa prestadora de serveis un contracte d'encarregat de tractament.

En relació amb les transferències internacionals de dades, es considera com a tal l'enviament d'aquestes fora de la Zona Econòmica Europea. En aquests casos, a més de disposar de la corresponent base legitimadora, cal garantir que la comunicació es duu a terme segons les condicions establertes als articles 44 a 50 RGPD. Podem trobar informació detallada de les transferències internacionals de dades al següent enllaç de l'AEPD.

En relació amb les transferències internacionals de dades hem de fer referència al Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació d el sector públic i telecomunicacions, que modifica diverses normes aplicables a les entitats del sector públic, entre les quals es troba la Llei 40/2015, de l'1 d'octubre, de Règim Jurídic del Sector Públic, a la qual afegeix un nou article 46 bis

> *"Article 46 bis. Ubicació dels sistemes d'informació i comunicacions per al registre de dades.*
>
> *Els sistemes d'informació i comunicacions per a la recollida, emmagatzematge, processament i gestió del cens electoral, els padrons municipals d'habitants i altres registres de població, dades fiscals relacionats amb tributs propis o cedits i dades dels usuaris de sistema nacional de salut, així com els corresponents tractaments de dades personals, hauran d'ubicar i prestar dins del territori de la Unió Europea.*
>
> *Les dades a les quals es refereix l'apartat anterior no podran ser objecte de transferència a un tercer país o organització internacional, amb excepció dels que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya."*

Per tant, en l'avaluació de projectes de recerca on existeixen transferències internacionals, i ens trobem en l'àmbit d'aplicació de l'article 46, hem de tenir en compte la limitació establerta per aquest article, i valorar la seva aplicabilitat en el projecte de recerca concret.

3.8 Seguretat en el tractament de dades amb finalitats de recerca

La seguretat de les dades es regula a través de l'article 32, i específicament en l'àmbit de la recerca a través de l'article 89 del RGPD, i està estrictament lligada al principi d'integritat i confidencialitat establert per l'article 5 del RGPD.

Així mateix, a través l'article 19 del Real decret 3/2010 mitjançant el qual s'aprova l'Esquema Nacional de Seguretat (i que d'acord a la Disposició Addicional Primera de la LOPD-GDD, s'aplica als tractaments de dades realitzats per les entitats del sector públic), es defineix la seguretat per defecte que implica que els sistemes informàtics s'han de dissenyar de manera que garanteixin la seguretat per defecte, fet que suposa que:

> *"a) El sistema proporcionarà la mínima funcionalitat requerida perquè l'organització assoleixi els seus objectius.*
>
> *b) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'ha d'assegurar que només són accessibles per les persones, o des d'emplaçaments o equips, autoritzats. Es pot exigir, si escau, restriccions d'horari i punts d'accés facultats.*
>
> *c) En un sistema d'explotació s'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que no siguin d'interès, siguin innecessàries i, fins i tot, aquelles que siguin inadequades a la finalitat que es persegueix.*
>
> *d) L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi d'un acte conscient per part de l'usuari."*

Cal que el sistema de tractament de les dades, com a mínim, garanteixi que:

- Disposa de les mesures tècniques i organitzatives necessàries per salvaguardar els drets dels participants en el projecte de recerca durant tot el cicle de tractament de les dades.
- El sistema de tractament de dades disposa de les mesures tècniques i organitzatives necessàries per evitar l'accés no autoritzat a dades personals.

Els criteris de seguretat que, de forma orientativa, s'han de tenir en compte en l'àmbit de la recerca són:

A) Pseudonimització, acords de confidencialitat, registres d'accés i distribució estricta de rols d'accés.

B) S'ha de fer una avaluació d'impacte de protecció de dades d'acord amb l'article 35 RGPD, quan aquest tractament pugui "comportar un risc elevat

per als drets i les llibertats de les persones físiques" d'acord amb l'article 35, apartat 1, RGPD.

C) Consulta i assessorament del DPD quan sigui necessari. En aquest sentit, tots els CEIm han de disposar de la figura d'expert en protecció de dades que pot coincidir o no amb el DPD.

D) Les mesures adoptades per protegir les dades (incloses durant les transferències) haurien de ser adequades i documentades en el registre d'activitats de tractament.

Quan en els projectes de recerca utilitzem recursos institucionals, hem de seguir les directrius de seguretat indicades per la institució. Per aquest motiu, és important que la institució disposi d'una política de protecció de dades (art. 24 RGPD).

Quan en el marc del projecte de recerca s'utilitzen recursos externs, hem de poder verificar que les eines que s'utilitzen garanteixen els criteris de seguretat indicats en els anteriors paràgrafs. Algunes indicacions pràctiques són:

- Si les dades s'emmagatzemen en servidors externs, s'ha de garantir que aquests són segurs i s'han de detallar les mesures de seguretat aplicades a l'accés, incloent-hi una descripció de qui accedeix a les dades, quan, com i on s'emmagatzemen.

- S'evitarà l'ús d'eines comercials no segures d'emmagatzemament al núvol que no garanteixin el compliment del RGPD.

- Si en el projecte es tracten dades amb un programari no institucional, cal que el codi desenvolupat per a les aplicacions utilitzi tècniques d'ofuscament de codi, sobretot en aplicacions mòbils, i que les aplicacions desenvolupades segueixin metodologies de desenvolupament segures.

L'aplicació del principi de privacitat des del disseny i per defecte, i la realització d'una avaluació d'impacte, permetran garantir que aquestes mesures de seguretat són les adequades per al tractament de dades que es duu a terme.

3.9 Perfilatges i decisions automatitzades

El RGPD, introdueix dos conceptes com són el perfilatge o profiling, i la presa de decisions automatitzades que de vegades són complexes d'identificar, però que es donen sovint en el marc de projectes de recerca, i tenen una especial rellevància a l'aplicació de la normativa de protecció de dades, especialment l'article 22 del RGPD.

Partim de que existeix una **elaboració de perfils** quan es donen els següents elements: existeix una forma automatitzada de tractament, en relació amb dades personals, l'objectiu del qual és avaluar aspectes personals en relació amb una determinada persona física (art.4.4 RGPD).

S'ha de distingir de la simple classificació de persones, ja que hi un element a la definició, avaluar, que implica analitzar o fer prediccions sobre persones.

Aquesta elaboració de perfils pot implicar que:

i) es doni una decisió a partir únicament d'una decisió automatitzada,

ii) pot ser que l'elaboració de perfil no impliqui cap presa de decisions basades únicament en una decisió automatitzada o,

iii) que directament no impliqui la presa de cap decisió.

L'article 22 del RGPD, només aplicaria al primer cas, quan s'estableix el **dret a no ser objecte d'una decisió basada únicament en un tractament automatitzat**.

Per tant, la clau està en el concepte de decisió automatitzada, és a dir, la capacitat de presa de decisions basades únicament en mitjans tecnològics **sense** una **participació humana** que permet descartar l'aplicació del 22 del RGPD.

Per determinar si hi ha participació humana, aquesta **supervisió humana s'**ha de dur a terme de manera que sigui **significativa** per a la presa de la decisió, no únicament simbòlica. L'ha de dur a terme una **persona autoritzada** i competent amb **capacitat suficient per modificar la decisió**, i capaç d'entendre totes les dades per tenir-les en compte a l'hora de realitzar la corresponent anàlisi. En aquestes situacions, quan es duu a terme **l'avaluació d'impacte** per justificar la no aplicació de l'article 22, s'ha **d'identificar el grau de participació humana en el procediment de presa de decisions**.

Aquest concepte l'hauríem d'incloure com a element a valorar en la metodologia d'avaluació d'impacte que fem, i determinar com afecta la participació humana en el procediment de presa de decisions i si aquesta descarta l'aplicació de l'article 22 del RGPD.

Per tant, els conceptes de decisió automatitzada i elaboració de perfils se solapen, però es poden donar de manera independent. És a dir, les decisions automatitzades es poden donar sense elaboració de perfils, i l' elaboració de perfils es pot donar sense que hi hagi decisions automatitzades.

Podem concloure que l'article 22 del RGPD només és aplicable quan hi ha una decisió automatitzada que afecta els drets dels interessats i que l'elaboració de perfils no sempre caurà dins l'àmbit del 22 RGPD, únicament serà així quan es pren una decisió automatitzada a partir d'aquesta elaboració de perfils.

Tant en el cas de decisions automatitzades com en el d'elaboració de perfils, al marge de l'article 22 del RGPD, s'ha de considerar el fet d'aplicar els principis de l'article 5 del RGPD i les bases legitimadores. A fi de garantir que en aquestes situacions s'apliquen correctament els principis de la normativa el document

Directrius sobre decisions individualitzades automatitzades i elaboracions de perfils del Grup de Treball de l'article 29, inclou un annex de bones pràctiques per garantir el compliment dels principis de l'article 5 del RGPD.

4 Aspectes que s'han d'incloure en el protocol dels projectes de recerca des de la perspectiva de la protecció de dades

Els CEim, quan revisin projectes de recerca, han de garantir que el tractament de les dades en el marc del projecte compleix els requeriments del RGPD i de la LOPD-GDD.

Amb aquesta finalitat, quan es presenti un projecte de recerca, s'haurà d'adjuntar un apartat específic on es detallin tots els aspectes relacionats amb el tractament de dades personals. Així mateix, s'haurà de garantir que el document d'informació i consentiment que signen els participants en un projecte de recerca, conté tota la informació relativa al tractament de dades en el marc del projecte de forma clara i comprensible per al participant, així com tota la informació relativa a l'exercici dels seus drets. El document de consentiment haurà de permetre donar el consentiment per als diferents tractaments de dades que es duguin a terme en el marc de l'estudi de recerca.

Els CEIm quan reben els protocols dels projectes de recerca han de revisar que contenen tots els elements que es detallen a continuació:

Taula 1. Informació que ha d'incloure un protocol d'un projecte de recerca.

Ítem a revisar	Informació que s'ha d'aportar al protocol
Identificació del responsable del tractament	• Cal identificar quina entitat és la **responsable del tractament**, les dades de contacte, la forma de contacte amb el seu Delegat de Protecció de Dades i la forma d'exercici dels drets. • En cas de donar-se una situació de coresponsabilitat, cal que s'indiquin les dades dels dos coresponsables, així com la descripció de la part de tractament realitzada per cada coresponsable. • Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.

Descripció del tipus de dades que es tractaran i de la forma com es tractaran	• S'ha d'aportar informació en relació amb les tipologies de dades que es tracten (identificatives, hàbits, salut, genètiques, biomètriques ...). • S'ha d'aportar informació en relació amb la forma com es tractaran aquestes dades (identificades, codificades, pseudonimitzades o anonimitzades). Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca. • Indicar si les dades estaran codificades, pseudonimitzades o anonimitzades, s'ha d'explicar la forma com es fan servir. • S'ha d'aportar informació en relació amb el temps de conservació de les dades. Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.
Origen de les dades i legitimació per al seu tractament	• S'ha d'indicar **d'on provenen** les dades que s'utilitzaran en el marc del projecte de recerca, així com la **base de legitimació** per a la seva utilització. Les dades poden provenir: • Directament del titular en el marc del projecte de recerca concret. • De tractaments preexistents (reutilització de dades). • Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.
Minimització	• Si es recullen els ítems mínims necessari per assolir els objectius de recerca, és a dir que no es recullen més dades de les necessàries. • Si s'ha considerat la possibilitat d'utilitzar dades anònimes o pseudonimitzades.
Comunicacions de dades	• El protocol del projecte ha de detallar totes les comunicacions de dades que es produeixen en el marc del projecte, i la seva legitimació. Caldrà distingir i indicar la existència de: • Encarregats de tractament (art. 28 RGPD) • transferències internacionals de dades (art. 44 a 45 RGPD) • Altres comunicacions de dades • La informació relativa a l'existència de comunicacions i la transferència internacional de dades s'haurà de reflectir al full d'informació del participant al projecte de recerca.

Sistemes de tractament de la informació	• El protocol ha d'indicar les eines informàtiques que s'utilitzen per al tractament de les dades, ja siguin tant de tipus institucional com no institucional, indicant –ho de forma específica i descrivint els següents supòsits: ✓ Ús de sistemes d'emmagatzemament al núvol ✓ Ús de wearables ✓ Ús d'apps sotmeses a clàusules generals ✓ Si es recopilaran, transmetran i emmagatzemaran dades de categoria personal / categories especials de forma segura. ✓ Si el nivell de seguretat proporcionat és adequat per als riscos que representa el tractament. ✓ Si es posaran en marxa procediments per a l'eliminació i/o la destrucció segura de dades personals o dades de categoria especial quan ja no es necessitin.
Avaluació d'impacte	• S'ha d'aportar informació en relació amb els resultats de l'avaluació d'impacte que s'ha realitzat del tractament de dades del projecte de recerca. • Si l'avaluació d'impacte determina que el tractament implica un alt risc per als titulars de les dades, s'hauran d'indicar les mesures que s'han pres per mitigar-lo.
Explicació de les mesures preses en relació amb els tractaments que poden suposar un alt risc per als drets i les llibertats dels participants en la investigació	• El protocol ha d'explicitar si es donen les situacions que es detallen a continuació, i la forma com s'han mitigat els riscos: ✓ Realització de perfilatges de dades o presa de decisions automatitzades respecte participants individuals ✓ Ús d'eines d'intel·ligència artificial. ✓ Utilització de tècniques d'explotació de dades amb tecnologies Big Data. ✓ Utilització de sistemes de biometria ✓ Utilització de sistemes de geolocalització

Aquests elements són els que després els avaluadors hauran de verificar que estiguin inclosos al protocol i al full d'informació i consentiment (en cas que n'hi hagi).

Aquesta taula es pot adaptar per a cada centre a fi de que es demanin els seus requeriments a tots els investigadors i promotors.

5 Metodologia per avaluar els aspectes derivats de la normativa de protecció de dades en projectes de recerca

Per avaluar un projecte de recerca s'ha de verificar que el protocol i el consentiment de recerca contenen els elements que determina la normativa de protecció de dades. A continuació, en format llistat, es repassen tots

els elements que s'ha de verificar que inclouen els protocols de recerca, així com el document de consentiment informat. S'acompanya de notes a peu de plana per definir els conceptes principals.

1. Identificar responsables del tractament

Identificació de l'entitat que decideix en relació amb el tractament de les dades, és a dir, qui és el responsable[1]/responsables o coresponsables[2] del tractament, NIF i domicili social, així com la forma de contacte del Delegat de Protecció de Dades[3]. Per exemple, en els assaigs clínics són coresponsables del tractament el centre on es duu a terme l'assaig i el Promotor.

Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca, i la forma d'exercici dels drets d'accés, rectificació, cancel·lació, oposició, portabilitat, oblit i limitació (drets ARCO-POL).

2. Identificar els tractaments que es realitzen

S'ha d'aportar informació en relació amb les tipologies de dades que es tracten (salut, genètiques, biomètriques, ...).

S'ha d'aportar informació en relació amb la forma com es tractaran aquestes dades (identificades, codificades, pseudonimitzades[4] o anonimitzades).

Les dades s'han de tractar d'acord amb el principi de minimització, és a dir, únicament s'han de tractar les dades que siguin necessàries, i s'han de conservar mentre siguin necessàries per a la realització del projecte de recerca.

---

[1] **Responsable del tractament o responsable**: la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament; si el dret de la Unió o dels Estats membres en determina les finalitats i els mitjans del tractament, el responsable del tractament o els criteris específics per al seu nomenament els pot establir el dret de la Unió o dels Estats membres

2 Quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament, se'ls considera **coresponsables del tractament.**

3 **Delegat de Protecció de dades o DPD** es tracta d'una nova figura que esdevé obligatòria al sector sanitari. Aquesta figura té diverses funcions assignades pel nou Reglament Europeu. Entre d'altres, assessora i supervisa l'ús de dades de salut al centre. Cada entitat té el seu propi DPD.

4 **Pseudonimització:** el tractament de dades personals de manera que ja no es puguin atribuir a un interessat sense utilitzar informació addicional, sempre que aquesta informació consti per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable.

Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.

En cas que les dades estiguin codificades, pseudonimitzades o anonimitzades, s'ha d'explicar la forma com es duu a terme aquesta pseudonimització o anonimització. Per exemple, si es codifica s'explicarà qui assigna el codi i quins criteris es segueixen.

3. Origen de les dades i legitimació per al seu tractament

S'ha d'indicar **d'on provenen** les dades que s'utilitzaran en el marc del projecte de recerca així com **la base de legitimació**[5] per a la seva utilització. Les dades poden provenir:

a) Directament del titular en el marc del projecte de recerca concret.

b) De tractaments preexistents (reutilització de dades).

Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca. Per exemple, en un assaig clínic les dades provenen de la història clínica del pacient i s'incorporen al Quadern de Recollida de Dades de forma codificada.

4. Minimització

El protocol del projecte ha de detallar si es recullen els ítems de dades personals/dades de categories especials mínimes necessàries per assolir els objectius de recerca. Caldrà detallar la necessitat de recollir les dades personals objecte de tractament en relació amb la finalitat prevista. En aquest punt, s'ha de valorar si s'ha considerat la possibilitat d'utilitzar dades anònimes o pseudonimitzades i, en cas que no sigui així, la justificació.

El protocol ha d'incloure si l'accés a les dades personals/dades de categoria especial dels participants es restringirà a persones autoritzades.

---

5 Concretament per utilitzar **categories especials** de dades com són les **dades de salut**, amb finalitats de recerca hem d'utilitzar alguna de les bases legítimes de l'article 6 del RGPD, així com aixecar la prohibició de tractament d'aquesta categoria especial de dades que estableix l'article 9.1 del RGPD, utilitzant algun dels supòsits de l'article 9.2 del RGPD. En aquest sentit també hem de tenir en compte l'article 89 del RGPD, així com la disposició addicional dissetena de la LOPD-GDD, que estableix un règim específic per a l'ús de les dades de salut, i la normativa específica a l'àmbit sanitari i de recerca. En el document general podeu trobar una descripció de en que consisteixen totes aquestes bases.

Finalment, si les dades dels participants es conservaran com a dades totalment identificables durant un període de temps determinat i la justificació del temps de conservació en aquests casos.

5. Comunicacions de dades, encarregats de tractament i transferències internacionals

El protocol del projecte ha de detallar totes les comunicacions de dades que es produeixen en el marc del projecte, i la seva base legítima. Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.

S'han de determinar i identificar les relacions d'encarregats de tractament[6], i verificar/advertir de la necessitat o existència del corresponent contracte. Són els casos d'empreses de prestació de serveis, com per exemple una empresa que gestiona els viatges de les persones incloses en un estudi on caldrà verificar o advertir que l'empresa prestadora de serveis signi un contracte d'encarregat de tractament amb el centre que cedeix les dades.

S'ha de determinar l'existència de transferències internacionals[7] de dades, així com la seva adequació a la normativa de protecció de dades. Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca. Es considera transferència internacional de dades l'enviament d'aquestes fora de la zona Econòmica Europea quan no hi ha un acord que garanteixi que el país o l'entitat de destí de les dades compleixen els requisits mínims que la normativa europea exigeix.

6. Descripció dels sistemes de tractament de la informació, dels fluxos de dades i de les mesures de seguretat aplicables

Cal que el protocol indiqui les eines informàtiques que s'utilitzen per al tractament de les dades, ja siguin de tipus institucional com no institucional, així com les mesures de seguretat que s'apliquen per garantir la seguretat de les mateixes.

Quan als projectes de recerca utilitzem recursos institucionals, hem de seguir les directrius de seguretat indicades per la institució. Per aquest motiu, és important que la institució disposi d'una política de protecció de dades (art. 24 RGPD), així com d'una política de seguretat.

---

6 **Encarregat del tractament o encarregat:** la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.

7 Es considera **transferència internacional de dades** l'enviament d'aquestes fora de la zona Econòmica Europea quan no hi ha un acord que garanteixi que el país o l'entitat de destí de les dades compleix els requisits mínims que la normativa europea exigeix.

Quan en el marc del projecte de recerca s'utilitzen recursos externs, hem de poder verificar que les eines que s'utilitzen garanteixen els criteris de seguretat indicats en els anteriors paràgrafs. Algunes indicacions pràctiques són:

- Si les dades s'emmagatzemen en servidors externs, s'ha de garantir que aquests són segurs i detallar les mesures de seguretat aplicades a l'accés, incloent-hi una descripció de qui accedeix a les dades, quan, com i on s'emmagatzemen.
- S'evitarà l'ús d'eines comercials no segures d'emmagatzemament al núvol que no garanteixin el compliment del RGPD.
- Si en el projecte es tracten dades amb un programari no institucional, cal que el codi desenvolupat per a les aplicacions utilitzi tècniques d'ofuscament de codi, sobretot en aplicacions mòbils, i que les aplicacions desenvolupades segueixin metodologies de desenvolupament segures.

  L'aplicació del principi de privacitat des del disseny i per defecte, i la realització d'una avaluació d'impacte, permetran garantir que aquestes mesures de seguretat són les adequades per al tractament de dades que es duu a terme.

En aquest punt, cal fer especial esment que l'ús de determinades tecnologies o dispositius en l'àmbit del projecte de recerca pot generar conflictes en l'aplicació de la normativa de protecció de dades per la complexitat de la seva anàlisi. En aquests casos, és recomanable contrastar el projecte amb el membre expert en protecció de dades del comitè:

a) Ús de sistemes de geolocalització, sistemes de biometria (per exemple reconeixement facial, empremta dactilar, ...) o l'aplicació de tècniques de perfilatges amb dades.

b) Projectes que utilitzin tècniques d'explotacions massives de dades, o d' intel·ligència artificial (per exemple es dóna aquest supòsit quan es volen validar algoritmes amb dades de pacients).

c) Projectes que volen emprar una *app* o un *wearable* com a part integrant del projecte de recerca, i que la *app* o *wearable* té accés a dades dels participants en l'assaig, (per exemple ús d'una polsera que registra les constants vitals dels participants o l'ús d'una app per recollir informació dels pacients).

7. Avaluació d'impacte

S'ha de verificar si el projecte de recerca necessita d'una avaluació d'impacte, de conformitat amb la disposició addicional 17.2.f de la LOPD-GDD, que estableix que

qualsevol projecte de recerca realitzat d'acord amb el que estableix l'article 89 del RGDP requerirà la realització d'una avaluació d'impacte, sempre i quan estiguem en una de les situacions previstes a l'article 35 del RGPD, o ens troben en un dels supòsits previstos per les Autoritats de Protecció de Dades.

En el marc de la recerca la necessitat de realitzar una avaluació d'impacte serà molt freqüent, ja que es tracten dades de salut, i sovint els projectes de recerca contenen altres elements de risc com l'ús de tecnologies innovadores (tècniques d'intel·ligència artificial, *wearables o apps*, sistemes de realitat virtual, geolocalització o biometria), el tractament de col·lectius especialment vulnerables (menors, discapacitats), perfilatges de dades o el tractament massiu de dades, que fan necessària la realització d'una avaluació d'impacte.
Podeu trobar més informació en relació amb els supòsits on s'ha de realitzar una avaluació d'impacte al document general, i consultar a l'expert de protecció de dades.

El CEIm o CEI no ha de dur a terme l'avaluació d'impacte sinó que ha de verificar que existeix, així com que el seu resultat no indica l'existència de cap incompliment del RGPD en el marc del projecte de recerca. El responsable del tractament, amb l'assessorament del Delegat de Protecció de Dades, ha de dur a terme l'avaluació d'impacte.

Finalment, indicar que no és necessari realitzar una avaluació d'impacte per a cada projecte de recerca concret, sinó que és possible que determinats projectes de recerca comparteixin una mateixa avaluació d'impacte. S'haurà d'avaluar a cada cas la necessitat de realitzar una avaluació d'impacte específica per al projecte, i que vindrà determinat per l'existència d'elements únics i característics d'aquest projecte, (per exemple els projectes amb un alt component tecnològic com seria l'avaluació d'un algoritme, l'ús d'una app en el projecte de recerca o l'ús de tecnologies *Big Data*).

8. Identificació de situacions d'especial complexitat en projectes de recerca

Cal identificar aquelles situacions d'especial risc i complexitat en projectes de recerca, com són:

- Realització de perfilatges de dades o presa de decisions automatitzades respecte a participants individuals.
- Ús d'eines d'intel·ligència artificial.
- Utilització de tècniques d'explotació de dades amb tecnologies Big Data.
- Utilització de sistemes de biometria.
- Utilització de sistemes de geolocalització.

Caldrà verificar amb l'expert en protecció de dades l'adequació d'aquests tractaments de dades a la normativa de protecció de dades.

9. Contingut del full d'informació i consentiment del pacient

A mode de resum de la informació donada fins al moment, el full d'informació i consentiment, ha de contenir:

- Identitat del responsable o coresponsables del tractament de les dades i davant de qui i com poden exercir els seus drets.
- Identificació de la forma de contacte amb el Delegat de Protecció de Dades.
- Descripció de les finalitats del tractament de les dades, i comunicacions previstes, incloent-hi les transferències internacionals de dades.
- Tipus d'informació que es recull i el termini durant el qual es conservaran les dades.
- Mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.
- Dret a conèixer perquè s'utilitzen les seves dades; qui les té; a qui les pot cedir; quins són els seus drets, entre els quals s'inclou el dret a sol·licitar al responsable la cancel·lació de les dades i el dret a la rectificació de les dades quan siguin inexactes o estiguin incompletes.
- Dret a retirar el consentiment en qualsevol moment i la informació identificable de la base de dades de salut, així com el dret a sol·licitar i rebre informació sobre les seves dades i el seu ús.
- Dret a presentar una reclamació front l'autoritat competent.
- Breu descripció de les mesures de seguretat per protegir la privacitat i els riscos per a la confidencialitat.

6 Glossari i agraïments

APDCAT - Autoritat Catalana de Protecció de Dades

AEPD - Agencia Española de Protección de Datos.

DPD – Delegat de Protecció de Dades

EDPB - European Data Protection Board.

EDPS - European Data Protection Supervisor.

EIPD - Avaluació d'impacte en Protecció de Dades.

CEI - Comitè d'Ètica en Investigació.

CEIm - Comitè d'Ètica en Investigació ambPHGLFDPHQW

BIOÈTICA - Comité de Bioética deEspaña.

Agraïm a tots els experts i expertes i coordinadors i coordinadores de Protecció de Dades que han participat en el Grup de Treball de Recerca de l'Oficina del DPD, ja que sense la seva col·laboració i les seves aportacions aquesta guia no hauria estat possible, i les valuoses recomanacions de l'Observatori de Bioètica i Dret de la Universitat de Barcelona. Volem agrair igualment el suport per part de la Direcció General de Recerca i Innovació en Salut i de la Direcció General d'Ordenació i Regulació Sanitaria del Departament de Salut.