INSTRUCCIONS PER L'INVESTIGADOR PER ELABORAR L'APARTAT DE PROTECCIÓ DE DADES DELS PROTOCOLS DE RECERCA

Aquest document s'elabora com a complement de la *Guia per l'avaluació dels aspectes derivats de la normativa de Protecció de Dades en Projectes derecerca.*

A través d'aquestes instruccions es vol oferir una eina practica que permeti als investigadors incorporar de forma estructurada tota la informacióen matèria de protecció de dades, que ha de contenir tot protocol de recerca, fi que el CEIM o CEIC corresponent, pugui avaluar el projecte.Aquestes instruccions consten de:

1. Una explicació detallada de les preguntes relatives al tractament de dades personals a les que s'ha de donar resposta amb el contingut d'un protocol de recerca, per tal que el CEIM o CEIC pugui avaluar el vostre projecte, i que ajuda a comprendre com completar el formulari de que s'indica en el següent punt.

2. Una proposta de formulari amb els apartats de protecció de dades que han completar els IP, i que ha de permetre al CEIm o CEIC, conèixer els tractaments de dades que es duen a terme en el marc del projecte que s'ha d'avaluar. Aquest formulari pot servir de guia per completar l'apartat de protecció de dades del protocol.

3. Una proposta de document informatiu per al tractament de dades amb finalitats de recerca per als participants en estudis de recerca.

Si teniu dubtes podeu trobar més informació els aspectes relacionats amb la normativa de protecció de dades a la *Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca*, o consultar al referent en protecció de dades de la vostra institució a través de la següent adreça de correu [*].

PREGUNTES A LES QUE HA DE DONAR RESPOSTA EL PROTOCOL

1) QUINES DADES ES TRACTEN EN EL PROJECTE, QUI LES TRACA I COMUNICACIONS?

- El primer que s'ha de determinar en un protocol són les dades que es tractaran i amb quina finalitat, fent una descripció les tipologies de dades o variables que s'utilitzaran (o referenciant a un punt del protocol on es detallin) i d'on es treuen aquestes dades. En aquest punt s'haurà d'indicar el format de les dades (anònimes, identificades o pseudonimitzades[1]) i si es creuen amb altres bases de dades. Si les dades són anònimes o s'han pseudonimitzades s'ha de descriure com s'ha fet aquest procediment.

  Les dades s'han de tractar en base al 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.

  Exemples

  - *Les variables necessàries per a portar a terme l'estudi són el pes l'edat, el nivell de glucèmia o colesterol i provindran del SAP de l'Hospital. Aquestes variables es creuaran amb informació del Registre Nacional de Difunts, i la informació es tractarà de forma identificada*
  - *Les variables necessàries, descrites a l'apartat x del protocol, provenen del programa PADRIS, i estan anonimitzades pel propi sistema del programa PADRIS.*

- En segon lloc s'ha de descriure qui tracta dades en el projecte, que poden ser diversos actors i portar a terme diversos rols.

  En primer lloc s'ha d'identificar l'entitat que decideix en relació al tractament de les dades, és a dir, qui és el responsable[2]/responsables o coresponsables[3] del tractament.

---

[1] 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, 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, dades proporcionades per comptadors intel·ligents, dades de l'hospital o metge.
Les dades **anònimes,** són aquelles que ja no permeten identificar a la persona, i 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.
Cal distingir aquest concepte de la dada **pseudonimitzada** 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

[2] **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

Exemple

- *L'Hospital X i el Promotor actuen com a responsables del tractament en el marc d'aquest estudi observacional.*

També s'han de descriure altres subjectes que accediran a les dades o que les rebran, encara que no tinguin la consideració de responsable del tractament. En aquest punt apareix la figura de l'encarregat de tractament[4], amb qui s'haurà de subscriure el corresponent contracte (aquest punt s'ha de gestionar amb serveis jurídics de la institució).

Exemples

- *L'empresa x, al subministrar oxigen al domicili dels pacients haurà de disposar de les seves dades per a la prestació del servei, pel que actuarà com a encarregat de tractament.*
- *La base de dades del projecte s'allotjarà als servidors de l'empresa x, pel que actuarà com a encarregat de tractament.*

2) QUINA ÉS LA BASE DE LEGITIMACIÓ PER A TRACTAR LES DADES I ORIGEN DE LES MATEIXES

- La normativa de protecció de dades, estableix que per tractar dades personals, és necessari disposar d'una base de legitimació. Aquesta base de legitimació pot ser el consentiment o altres, que s'expliquen en profunditat a la *Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca*. No existeix una exempció d'obtenir el consentiment en matèria de protecció de dades, el que existeixen són bases legitimadores diferents al consentiment. Així mateix també cal tenir en compte que el tractament de dades anònimes no requereix de base de legitimació ja que no aplica la normativa de protecció de dades.

- Per a utilitzar dades per recerca, o bé disposem del consentiment del titular de les dades, o són dades pseudonimitzades, pot ser un cas de reutilització de

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

[3]Quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament, se'ls considera **corresponsables del tractament.**

[4]**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.

dades o un cas d'ús de dades per part d'una autoritat en matèria de salut pública en una situació d'emergència.

- Caldrà doncs dir d'on venen les dades, i quina es la base legitimadora per utilitzar-les.

Exemples

- *Les variables necessàries per a portar a terme l'estudi s'han obtingut directament del participants del projecte mitjançant el seu consentiment.*
- *Les variables necessàries per a portar a terme l'estudi s'han obtingut del SAP, previ procés de pseudonimització per part de sistemes d'informació de la institució.*

3) COM ES TRACTEN LES DADES

- El protocol cal que indiqui les **eines informàtiques** que s'utilitzen pel tractament de les dades, i les mesures de seguretat que s'apliquen, ja siguin de tipus institucional com no institucional, indicant 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 categories especials de forma segura.

- Caldrà descriure les mesures de seguretat de que disposa.

Exemple

- *Les dades del projecte s'emmagatzemaran en servidors a la institució. Es transmetran les dades pseudonimitzades al promotor del projecte mitjançant VPN.*

- *Per a portar a terme el projecte s'utilitzarà la plataforma REDCAP, allotjada en els servidors de la institució, i que disposa de les mesures de seguretat determinades per la institució. Les dades s'emmagatzemen en el servidor web local on l'organització ha instal·lat el programari i, per tant, només accessible en equips que hi tinguin una connexió de confiança mitjançant VPN i*

credencials segures (certificats, claus RSA o contrasenyes complexes). S'ha incorporat un sistema per tal que únicament el servei de l'aplicació pugui enviar les dades al backoffice, mitjançant un firewall que únicament permeti les peticions des de les ip's de l'aplicació. El servidor web te habilitat la configuració de capçalera HTTP X-Frame-Options amb el valor «same-origin» per prevenir atacs de clickjacking.

4) ES PORTEN A TERME TRANSFERÈNCIES INTERNACIONALS

- S'han de determinar l'existència de transferències internacionals5 de dades, així com la seva adequació a la normativa de protecció de dades. Aquesta informació s'haurà de reflectir en el 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 amb els requisits mínims que la normativa europea exigeix.

Exemple

- *No existeixen transferències internacionals de dades.*
- *Les dades s'enviaran a Canadà, país amb el que existeix una decisió d'adequació d'acord amb l'article 45 del RGPD.*

5) ES DETECTEN TRACTAMENTS QUE PODEN SUPOSAR UN ALT RISC PER ALS DRETS I LLIBERTATS DELS PARTICIPANTS EN EL PROJECTE D'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 perfilat 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.

5Es 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 amb els requisits mínims que la normativa europea exigeix. Podeu trobar més informació a https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales.

- Caldrà descriure les mesures de seguretat de que disposa.

- S'ha de verificar si el projecte de recerca necessita d'una avaluació d'impacte, conforme a la disposició addicional 17.2.f de la LOPD-GDD, que estableix que qualsevol projecte de recerca realitzat d'acord a l'establert a 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 serà molt freqüent la necessitat de realitzar una avaluació d'impacte, ja que es tracten dades de salut, i freqüentment el 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 vulnerable (menors, incapaços), perfilat de dades o el tractament massiu de dades, que fan necessària la realització d'una avaluació d'impacte.

  Exemples

  - *D'acord amb l'establert a l'article 35 del RGPD s'ha realitzat la corresponent avaluació d'impacte del projecte. El projecte consisteix en la validació d'una eina d'intel·ligència artificial, però d'acord amb l'anàlisi realitzat a la corresponent avaluació d'impacte no implica una decisió automatitzada, no sent d'aplicació l'establert a l'article 22.*
  - *D'acord amb l'establert a l'article 35 del RGPD, el projecte no reuneix les característiques necessàries que obliguen a la realització de la corresponent avaluació d'impacte.*

PROPOSTA DE FORMULARI

1) **Dades del projecte**:
   - El projecte tracta dades personals: Sí / No

   - En cas de resposta afirmativa:

     - Quines dades es tracten:
       - Conté identificadors personals (incloent les inicials dels pacients o la data completa de naixement)? Sí / no
         - la utilització de dades anònimes en origen (p ex PADRIS)
         - utilització de dades pseudonimitzades per un tercer amb separació tècnica i funcional (com la unitat d'informàtica)
         - l'accés a la història clínica del pacients per la recollida de dades

     - Qui les tracta: Responsable/Coresponsables
     - Comunicacions: Encarregats,....
     - Es tracta d'un projecte multicèntric: Si/No

       - En cas de resposta afirmativa, quins centres hi participen?

2) Legitimació per al tractament de dades i origen:

   - S'ha previst sol·licitar al pacient el consentiment per al tractament de les seves dades amb finalitats de recerca? Sí / no

   - Si no s'ha previst sol·licitar el consentiment, justificar els impediments existents (recordeu que el fet que el projecte sigui retrospectiu o merament observacional no eximeix per sí mateix de l'obligació de sol·licitar el consentiment)
     ……

   - Si no s'ha previst sol·licitar el consentiment, quin dels següents supòsits seria la base legitimadora per al tractament de les dades en el projecte? (marcar el que més s'aproximi):

     - Supòsit 1 (p ex estudis epidemiològics d'interès general en situacions d'emergència autoritzats per l'Autoritat Sanitària…)
     - Supòsit 2 (p ex dades pseudonimitzades)
     - ….
     - …

   - Origen de les dades:
     - Interessat
     - ...

3) **Tractament de les dades, indiqueu**:

- Eines utilitzades
  - S'utilitzen dispositius electrònics? Sí /no
    - Lloc on es desarà informació:….
  - On s'ubica el servidor?
  - S'utilitzen bases de dades compartides de forma telemàtica amb altres centres o investigadors? Sí /no

- Descripció de les mesures de seguretat:
  - Indicació de mesures per evitar l'accés indegut de tercers no autoritzats:……..
  - Altres mesures de seguretat

4) Hi haurà transferència internacional de dades

- Sí /no. Mecanisme per efectuar la transferència: Decisió d'adequació

5) Aspectes per a projectes amb usos avançats de les dades

- Usos avançats
  - Realització de perfilat 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.

- Mesures de seguretat adoptades per aquestes actuacions

- Recordatori: Necessari adjuntar Avaluació d'Impacte

PROPOSTA DE CONTINGUT DE L'APARTAT DE PROTECCIÓ DE DADES PER AL PARTICIPANT EN UN PROJECTE DE RECERCA

DOCUMENT INFORMACIÓ DADES

QUE ÉS EL PROJECTE [*]

El projecte [*] ofereix [*],

COM ES TRACTARÁN LES SEVES DADES?

El Projecte, consistirà en [*], responsabilitat del [*], portat a terme amb col·laboració amb [*], en la seva condició d'encarregat de tractament.

El tractament d'aquestes dades es realitzarà en compliment del Reglament (UE) 2016/679 de el Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa a el tractament de dades personals i a la lliure circulació d'aquestes dades, i la Llei Orgànica 3/2018, de Protecció de Dades i garantia dels drets digitals, i per això li comuniquem que vostè podrà exercir els seus drets d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat de dades, front [*]com a responsable del tractament amb NIF [*] i domicili a [*], mitjançant l'adreça de correu electrònic [*]. Pot contactar amb el Delegat de Protecció de Dades a través de [*],

Així mateix l'informem del seu dret a presentar una reclamació davant de l'Autoritat Catalana de Protecció de Dades front qualsevol actuació del Departament de Salut que consideri que vulnera els seus drets.

Les seves dades seran tractades exclusivament amb les finalitats [*], de conformitat amb l'article 6.1, 9.2. [*], i la Disposició Addicional 17 2 [*],, de la Llei Orgànica

3/2018, de Protecció de Dades i garantia dels drets digitals, per [*], i es conservaran mentre durant el temps necessari per a la realització del projecte.

[*], tindrà accés a les dades de forma pseudonimitzada, amb l'única i exclusiva finalitat de portar a terme l'estudi de [*], havent-se adoptat mesures de seguretat específiques per evitar la reidentificació i l'accés de tercers no autoritzats.. No es preveuen transferències internacionals de dades [*], però en cas que es produïssin, serà únicament a països que garanteixen l'adequat compliment de la normativa de protecció de dades per existir una decisió d'adequació o qualsevol altre mecanisme legalment habilitat.

Per a més informació pot contactar a […]