UTILITZACIÓ DE DADES DE PLATAFORMES PER RECERCA

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

Sota la denominació de plataformes per recerca, parlarem de diversos softwares que s'utilitzen en l'àmbit de la recerca.

Podem categoritzar les plataformes utilitzades en recerca des del punt de vista del grau del control que hi tenim, trobem des de plataformes generalistes comercials com *google drive*, *wetransfer* o *google cloud*, on el grau de control de la plataforma és nul i no garanteixen el compliment de la normativa de protecció de dades, o plataformes especialitzades en recerca on es permet cert grau de control per l'usuari, per exemple REDCAP, o finalment plataformes o softwares fets a mida on la configuració de la seguretat està en mans de l'usuari final.

En l'àmbit de la recerca freqüentment s'utilitzen aplicacions o plataformes, ja sigui com a suport o per gestionar la recerca, o en ocasions l'aplicatiu és l'objecte del projecte de recerca. Parlem o bé de programari d'un tercer, no fet a mida on la capacitat de l'investigador o del centre per influir en la seva configuració és nul·la, o bé de serveis fets a mida.

Les dades de pacients utilitzades per projectes de recerca, recollides i emmagatzemades per necessitats metodològiques del projecte degudament justificades, no han d'aparèixer en cap moment el nom i cognoms del pacient, ni les seves inicials, ni la data de naixement (en format dia, mes i any), ni el codi postal de la residència dels pacients, ni el número d'història clínica.

Tot i això, en l'àmbit de la recerca, quasi sempre es treballa amb dades codificades o pseudonimitzades, ja que és necessari poder identificar als malalts per relacionar les seves dades mitjançant un número seqüencial o aleatori sense cap mena de significació. El fet que es tractin dades **codificades o pseudonimitzades** (que també es consideren dades personals) fa que sigui d'aplicació la normativa de protecció de dades.

Per aquest motiu quan utilitzem una plataforma o software en un projecte de recerca hem de garantir el compliment de la normativa de protecció de dades.

Que hem de garantir quan utilitzem una plataforma o un software d'un tercer?

Des del punt de vista de la normativa de protecció de dades sorgeixen diversos elements que hem de garantir:

a. **Legitimació per al tractament de dades, accessos de tercers i usos secundaris de les dades.** S'ha de garantir que si un tercer té accés a dades (p. ex. és accés a dades l'allotjament en servidors) disposa del corresponent encarregat de tractament establert per l'article 28 del RGPD, o si es dona una situació de coresponsabilitat, i no es duen a terme usos secundaris de dades.

b. **Transferències internacionals de dades.** Considerem com a transferència internacional de dades 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 du a terme segons les condicions establertes als articles 44 a 50 RGPD.

En aquest sentit, s'ha de destacar que el *Privacy Shield* (l'acord en l'àmbit de la legislació de protecció de dades entre els EUA i la UE) ha sigut invalidat recentment, i aquesta eina era la que permetia realitzar transferències internacionals de dades a Estats Units. Per aquest motiu s'hauran de buscar vies alternatives.

c. **Avaluació d'impacte.** El RGPD, en el seu article 35, estableix que en aquells casos en què 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 altre banda, de conformitat a la disposició addicional 17.2.f de la LOPD-GDD, qualsevol projecte de recerca amb dades 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.

   Es considera que en els projectes que es fa un ús de tecnologies innovadores i el tractament de categories especials de dades suposa un alt risc per als drets i les llibertats dels participants en la investigació. Aquest punt serà necessari analitzar-lo de forma prèvia a iniciar el projecte.

d. **Mesures de seguretat.** 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 lligat 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 forma que garanteixin la seguretat per defecte.

   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.

   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 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 en el núvol que no garanteixin el compliment del RGPD.

- Si en el projecte es tracten dades amb un software 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 porta a terme.

Quins tipus de plataformes s'utilitzen en l'àmbit de la recerca?

REDCAP. Es una plataforma de gestió de dades per recerca. Les dades que s'incorporen al REDCAP en principi són dades codificades o pseudonimitzades, de participants en projectes de recerca, motiu pel que és d'aplicació el RGPD. Si bé aquesta eina s'ha analitzat a la llum de les estipulacions establertes per l'HIPAA *(Health Insurance Portability and Accountability Act)*, manca fer-ne un anàlisis des del punt de vista del RGPD, per tant no es pot garantir la seva adequació al mateix.

EUSURVEY. Aquesta plataforma és de la Comissió Europea i està dirigida a la realització d'enquestes. En aquest cas es disposa de dues versions, una que s'utilitzen servidors d'un tercer, i una altre que es permet allotjar les dades en un servidor propi.

Un element fonamental per valorar si podem utilitzar aquestes dues eines és determinar on s'allotja aquest software. Si utilitzen la versió de REDCAP al núvol, es desconeix on s'emmagatzemen les dades, i per tant existeix el risc que es produeixi una transferència internacional de dades.

En aquest sentit, s'ha de tenir en compte que si s'utilitzen els servidors d'un tercer per a emmagatzemar dades, s'haurà de signar un acord d'encarregat de tractament en els termes de l'article 28 del RGPD, però que donada la dificultat de negociar amb determinats interlocutors, **es recomana utilitzar la opció de plataforma que permeti allotjar les dades en un servidor propi,** i de la mateixa forma que en el cas anterior, que ***securitzem*** **amb mesures que permetin garantir que la informació no és accessible per tercers** (mitjançant, per exemple, antivirus o tallafocs). D'aquesta manera, cal informar als responsables de sistemes de l'obligació de fixar les mesures de seguretat establertes a l'ENS – Esquema Nacional de Seguretat.

Així mateix també pot ser útil donar pautes generals al investigadors en quan al seu ús, com per exemple:

- Incloure únicament dades pseudonimitzades, mai dades que directament siguin identificatives com nom i cognoms, CIP, DNI, ...

- Cada usuari ha de correspondre a una única persona, és a dir, no es poden compartir usuaris ni les claus d'accés a l'eina.

- Deixar la sessió tancada quan s'acabi de treballar amb la base de dades.

En cas que el servidor sigui d'un tercer centre i aquest no aporti els anàlisis de riscos i l'avaluació d'impacte del sistema, cal requerir com a mínim que s'acrediti el compliment de les recomanacions descrites.

Una altre eina que es pot utilitzar en l'àmbit de la recerca és **TIXEO**, que segons l'anàlisi realitzat per la CNIL *(Commission Nationale de l'Informatique et des Libertés)* és una eina de videoconferència segura.

Eines de GOOGLE (CLOUD, DRIVE, FORMS), SURVEY MONKEY, WETRANSFER i DROPBOX, ONEDRIVE SHAREPOINT.

La problemàtica d'aquestes plataformes són diverses i es deriven del fet que donem accés a dades de categories especials de dades, de forma codificada o pseudonimitzada, a un tercer com per exemple Google, amb qui no tenim signat un encarregat de tractament quan es produeix un accés a dades per part d'un tercer en el marc d'una prestació de serveis en els termes de l'article 28 del RGPD. El mateix succeeix amb les plataformes de Survey Monkey, WeTransfer i Dropbox.

D'aquesta forma no és garanteix l'ús de les dades que farà aquest tercer, ni les mesures de seguretat que aplicarà en el seu tractament. Així mateix, si es tracten d'empreses nord americanes, degut a la derogació del *Privacy Shield* es produeix una transferència internacional de dades.

Per tant**, no es recomana l'ús d'aquestes eines per al tractament de cap tipus de dada personal.**

Quins criteris han de complir les aplicacions, des del punt de vista de la seguretat informàtica, que s'utilitzen en l'àmbit de la salut?

Tot software que s'utilitzi per a tractar dades de salut, des del punt de vista de la seguretat informàtica, ha de complir uns requeriments mínims, i que com a referencia per determinar-los podem fer servir la guia del Centro Criptológico Nacional anomenada "Requisitos de seguridad para Aplicaciones de Cibersalud en el contexto del ENS", que estableix quins **requisits mínims de seguretat** han de tenir aquest tipus d'aplicacions per garantir el compliment de la normativa de protecció de dades.

Aquestes requisits, els quals han de ser satisfets pels fabricants de les aplicacions, estan organitzats en funció dels següents objectius de seguretat:

1. Prova de la finalitat de l'aplicació
2. Prova de l'arquitectura
3. Prova del codi font
4. Prova del software de tercers
5. Prova de l'aplicació de la criptografia
6. Prova de l'autenticació
7. Prova de l'emmagatzemat i la protecció de dades
8. Prova dels recursos de pagament
9. Prova de les interaccions específiques de la plataforma
10. Prova de la comunicació de xarxa
11. Prova de la resiliència

Per fer més fàcil la implementació d'aquests objectius, s'adjunta un Excel que conté un formulari amb tots aquests requisits de seguretat anomenat *Eina DPD Requisits_Seguretat_Aplicacions_Salut.xlsx*.

Cada centre haurà d'establir els mecanismes necessaris, per exemple a través d'una revisió prèvia a través de sistemes d'informació i l'emissió del corresponent certificat de compliment, per a garantir que quan un projecte arriba al CEIM s'ha verificat que compleix amb els requeriments detallats a l'Excel, i, per tant, que pot ser avaluat considerant que compleix els requisits de seguretat corresponents.

Conclusions

En resum, quan avaluem un projecte de recerca que consisteix o utilitza una aplicació, aplicarem els següents criteris:

- No admetrem l'ús de plataformes tipus *google cloud, we transfer, google drive, drop box* o *google form.*
- L'ús de plataformes com *REDCAP* o *EUSURVEY*, s'admeten si no s'utilitza la opció *cloud*, sinó la instal·lada en servidors propis i *securitzada* amb les mesures de seguretat que impedeixin l'accés de tercers.
- Si s'avalua un projecte que consisteix o disposa d'un software, a més de les verificacions que s'han de dur a terme en tot protocol de recerca des del punt de vista de protecció de dades[1], s'hauran de portar a terme les verificacions que es detallen a continuació:
  - La plataforma o software ha de disposar de la corresponent avaluació d'impacte, i en cas de no disposar-ne, fonamentar el motiu que no fa necessari fer-la.
  - Si es produeixen accessos de tercers a les dades (p. ex. allotjament de dades o manteniment de software), s'ha de garantir que no es produeix cap transferència internacional de dades, i que es disposa el corresponent acord d'encarregat de tractament segons l'article 28 del RGPD.
  - El software ha d'implementar els requisits de seguretat que s'indiquen en l'Excel annex a aquest document.

[1] Els elements que s'han de valorar en un projecte de recerca es detallen a la Guia per l'avaluació dels aspectes derivats de la normativa de Protecció de Dades en Projectes de recerca.