



**Hogyan lehet egyensúlyt teremteni az adatvédelem,
a kutatási érték és a gyakorlati megvalósíthatóság között?**

Anonimizálás/pszeudonimizálás a kutatásban



Info törvény és GDPR

Info. tv. (2011 évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról)

GDPR (2016. május 24. - 2018. május 25.)

A GDPR bevezetése előtt az információs önrendelkezési jogról és az információszabadságról szóló Infotv. szabályozta az adatkezelést. Lényegi különbség volt, hogy a törvény nem definiálta külön az anonimizálás fogalmát, és nem határozott meg szigorú technológiai követelményeket.

Személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére most is az Info. tv.-t törvényt kell alkalmazni, vagyis ilyen esetekben csak a magyar jogi előírások alapján kell az adatkezelőnek eljárnia (amik egyébként nagyrészt a GDPR előírásaival azonosak). Minden olyan esetben, amikor a fenti céloktól eltérő az adatkezelés a GDPR előírásai alkalmazandók.



Anonimizálás vs pszeudonimizálás (álnevesítés)

- Anonimizálás: az érintett véglegesen nem azonosítható
- Pszeudonimizálás: az azonosítók helyettesítése kóddal vagy mással
- A visszafejtési kulcs megléte a két megoldás közötti alapvető különbség, így az álnevesített adatok visszaállíthatók, emiatt továbbra is személyes adatnak minősülnek



Leggyakrabban alkalmazott anonimizálási megoldások

- Eltávolítás
- Elkódolás (Kovács János ⇨ Xkd213sd)
- Maszkolás (Kovács János ⇨ Horváth János)
- Általánosítás (életkor ⇨ korcsoport, település ⇨ régió)
- Aggregálás (egyéni jövedelmek helyett átlagjövedelem településenként)



Mikor anonimizáljunk?

- Ha nincs szükség későbbi visszakapcsolásra
- Nyílt adatmegosztás előtt
- Adatminimalizálási célból



Mikor jobb a pszeudonimizálás?

- Longitudinális kutatásokban
- Utánkövetés vagy adathelyesbítés esetén
- Több adatforrás összekapcsolásakor



Megőrizzük-e a kulcsot?

Előnyök:

- Korrekció és utánkövetés lehetősége
- Adatkészletek összekapcsolása

Kockázatok:

- Biztonsági incidens esetén újraazonosítás
- További védelmi intézkedések szükségessége



Fő dilemmák

- Adathasznosíthatóság vs. Adatvédelem
- Kutatási érték vs. újraazonosítási kockázat
- Nyílt tudomány vs. bizalmas információk védelme
- Technikai és szervezeti költségek



Gyakorlati döntési szempontok

- Mi a kutatás célja?
- Szükséges-e a résztvevők későbbi elérése?
- Mekkora az újraazonosítás kockázata?
- Tervezett-e adatmegosztás vagy archiválás?
- Milyen jogi és etikai követelmények vonatkoznak az adatokra?



Személyes adatok hosszabb távú megőrzése, repositálása

- Jogalap (személyes adatok kezelésének rendelkeznie kell GDPR szerinti joggalappal)
- Célhoz kötöttség (csak a kutatási célhoz köthető személyes adatok kezelhetők és tehetők elérhetővé)
- Tájékoztatás (Az érintetteket előzetesen tájékoztatni kell arról, hogy adataik repositóriumban kerülnek elhelyezésre, és arról is, hogy kik férhetnek hozzá)
- Hozzáférés korlátozása (korlátozott vagy engedélyköteles hozzáféréssel)
- Biztonsági intézkedések (technikai és szervezési intézkedések)



Vitaindító kérdések

- Minden kutatási adatot anonimizálni kell?
- Mi a helyzet a kvantitatív és a kvalitatív adatokkal, a kapcsolattartási és a kutatási adatokkal?
- Mikor elegendő a pszeudonimizálás?
- Ki férhet hozzá a kulcshoz?
- Mikor indokolt a kulcs megsemmisítése?



ELTE TÁRSADALOMTUDOMÁNYI KUTATÓKÖZPONT
KUTATÁSI DOKUMENTÁCIÓS KÖZPONT



KÖSZÖNÖM A FIGYELMET!