

Milyen feladataik lennének az egészségügyi intézményeknek a GDPR bevezetése kapcsán?



Dr. Alexin Zoltán, PhD.
Szegedi Tudományegyetem, TTIK,
Szoftverfejlesztés Tanszék
H-6720 Szeged Árpád tér 2.
e-mail: alexin@inf.u-szeged.hu
<http://www.inf.u-szeged.hu/~alexin>

A GDPR helyzete Magyarországon

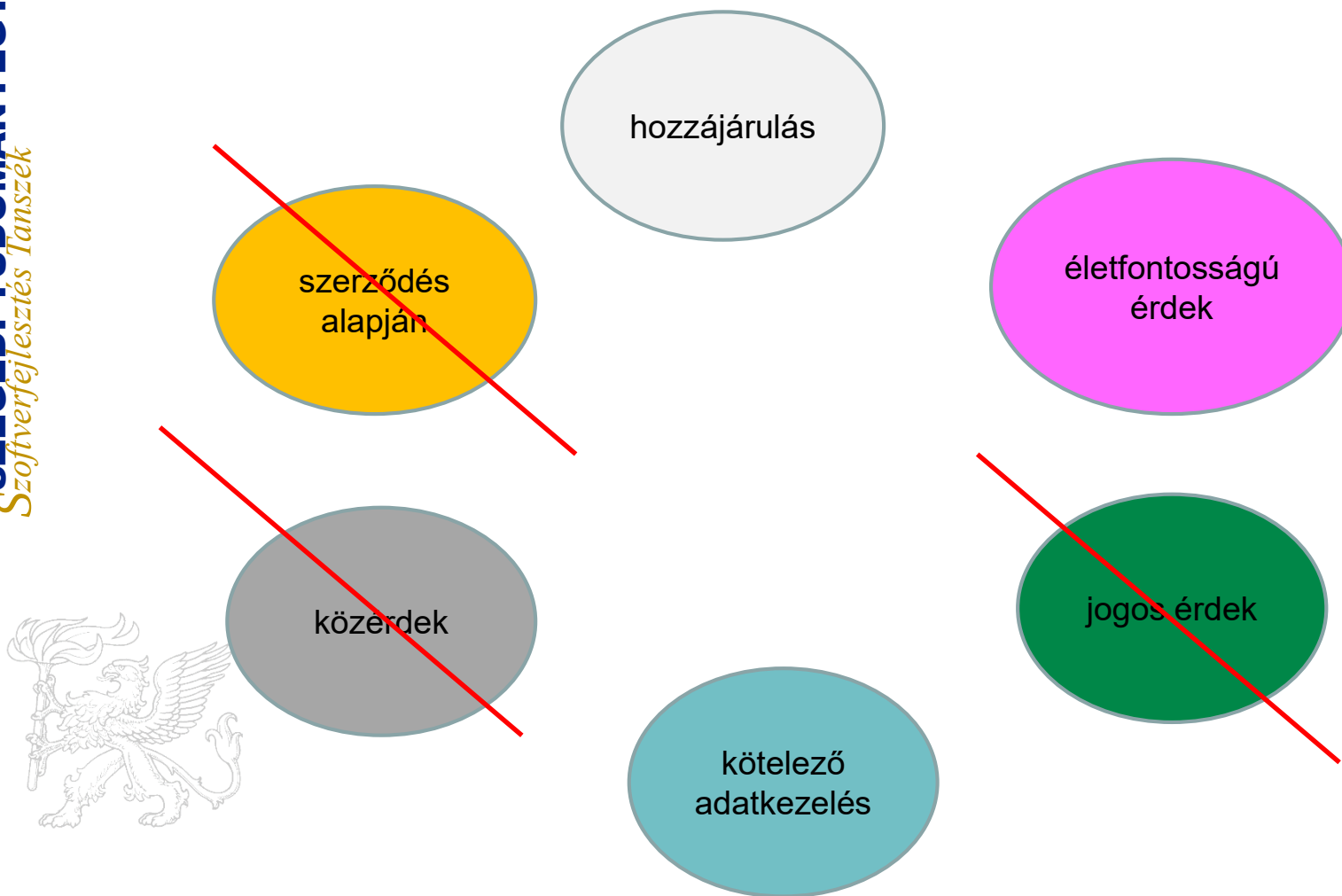
- Az Infotv. Módosítása nincs az Országgyűlés előtt (tervezetről tudunk) – sajnos a minősége meglehetősen gyenge.
- A NAIH nincs felhatalmazva a GDPR végrehajtására.
- A GDPR 43 helyen engedne nemzeti szabályozást. A tervezetben ebből csak kettőt használnának ki (nyilatkozat korhatár, elhunytak személyes adatai).
- Nagyjából 700 jogszabály tartalmaz rendelkezéseket személyes adatokról, ezek harmonizációja el sem kezdődött.
- Mintegy 10 törvény és majdnem 100 rendelet tartalmaz kötelező egészségügyi adatkezelést, ezek harmonizációjáról semmit sem tudunk.
- A GDPR szerint megszűnik a kötelező adatkezelés az egészségügyben, és csak közérdekű adatkezelésre lesz lehetőség, amely ellen van tiltakozási és jogorvoslati lehetőség.



Alapjogi szabadságharc

- A GDPR hatályba lépése összefonódik a jogalapok bevezetésével, amellyel 23 éve adós a magyar állam.
- Eddig a személyes adatok védelméhez fűződő alapjog – bár szerepelt az Alaptörvényben – használhatatlan volt.
- A jogorvoslat lehetőségének megjelenése a közérdekből történő adatkezeléseknél fontos mérföldkő (lesz).
- A vállalkozások számára megnyílik a szolgáltatási szerződés alapján történő adatkezelés – maguk definiálhatják a termékeiket és a hozzá tartozó adatkezeléseket (pl. telemedicina)
- A vállalkozások saját jogos érdekeik védelme érdekében kezelhetnek személyes adatokat (hozzájárulás nem szükséges)
- **Az adatkezeléssel kapcsolatos vitás ügyek végre visszakerülnek a polgári jog hatálya alá.**
- **Magyar polgár még sosem élte át azt az érzést, hogy nemet mondhat egy állami adatkezelésre.**

Az eddig ismeretlen jogalapok





Jogalapok helytelen használata

Adatkezelés	EU jogalap	Magyar jogalap
Társadalombiztosítás	Közérdek	Jogi kötelezettség
Népegészségügy	Közérdek	Jogi kötelezettség
Kutatás	Hozzájárulás, kivételesen közérdek	Jogi kötelezettség
Állami egészségügyben a minőségbiztosítás	Jogos érdek vagy közérdek	Jogi kötelezettség
Járványügyi intézkedés	Jogi kötelezettség	Jogi kötelezettség
EHR	Hozzájárulás vagy közérdek	Jogi kötelezettség

Mi lehet jogos érdek?

Az EUB C-543/09. számú ítélté: Deutsche Telekom AG v. Németország: jogos érdekből, törvény felhatalmazásával partnerek adatai átadhatók nyilvánosságra hozás céljából.

Példák a WP-217 anyagból (25. oldal)

- A szólásszabadság gyakorlása, közérdekű adatokhoz hozzájutás, művészetekben és a médiában
- Hirdetés, piackutatás, direkt marketing
- Üzenetek küldése előzetes engedély nélkül – jótékonyági vagy politikai célból
- Jogos követelések érvényesítése, adósság behajtás
- Csalások, visszaélések és a pénzmosás megelőzése
- Dolgozók megfigyelése biztonsági, vagyonvédelmi és menedzsment célból
- Whistle-blowing (névtelen bejelentők védelme)
- Fizikai biztonság, informatikai eszközök és hálózatok védelme
- Adatfeldolgozás tudományos és statisztikai célból
- Adatfeldolgozás kutatás (piackutatás is) célból

Kik a kötelezettek?

- NEAK, ÁEEK, OTH, NEFI, OEK
- Kórházak és klinikák
- **Magánklinikák**
- **Gyógyszertárak**
- Rendelőintézetek
- Szociális otthonok
- Nevelőintézetek
- Házi orvosok
- Magánorvosi rendelők



Az érintettek jogai

- GDPR 13-15. cikk
 - **előzetes adatvédelmi tájékoztatás** (kötelező adatkezelésnél is)!
 - **utólagos tájékoztatás** (az adatkezelés céljairól és az adatok kategóriáiról)
 - azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják;
 - adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
 - az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok **helyesbítését, törlését** vagy **kezelésének korlátozását**, és **tiltakozhat** az ilyen személyes adatok kezelése ellen;
 - a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
 - ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden információ;
 - **Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja.** Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Adminisztratív terhek

- **Adatkezelési nyilvántartást** kell vezetni (de nem kell bejelenteni az adatkezeléseket az adatvédelmi hatósághoz), a GDPR 30. cikke szerint
- **Adatvédelmi tisztviselő kinevezése** (kis gyógyszerárnak, magán- és háziornak nem kell)
- **Adatvédelmi tájékoztatást** kell adni az ügyfeleknek, partnereknek – ehhez célszerű megfelelő nyomtatványt kell készíteni, GDPR 13-14. cikk
- **Az adatfeldolgozókkal új szerződést** kell kötni, a GDPR 28. cikke definiálja, hogy minek kell szerepelnie a szerződésekben.
- Gondoskodni kell arról, hogy a belső információs rendszer támogassa, az egy érintetthez vonatkozó adatok összegyűjtését és másolat készítését, elektronikus formában történő exportálását, kijavítását, zárolását és törlését.
- El kell készíteni **a szolgáltatási szerződést** és kiválasztani a megfelelő jogalapot az adatkezeléshez.
- **Belső eljárásokat és ellenőrzési rendszert kell kialakítani** az érintettek panaszainak, kéréseinek kezelésére, a hozzáférések szabályozására, információbiztonsági rendszabályok (pl. vírusvédelem, mentés, hozzáférés szabályozás, naplózás) megvalósítására.

Minimális jogkorlátozás

- Személyes adat csak akkor kezelhető, ha az adatkezelés célját egyéb észszerű módon nem lehetséges elérni (39) preambulum.
- A személyes adatokat minél előbb álnevesíteni kell (78) preambulum.
- Az álnevesítés nem jelent semmilyen felmentést, az álnevesített adatok személyes adatok: az érintettek minden egyes jogát biztosítani kell álnevesített adatok esetében is (11. cikk)
- A HIS-ből származó lekérdezések eredménye kizárólag akkor tartalmazhat személyazonosítást lehetővé tevő kódot (TAJ, KBA, születési dátum stb.), ha azt jól meg lehet indokolni.
- Kutatási hozzáférés esetén eleve nem jelenhet meg semmilyen személyes azonosító adat (név, lakcím, TAJ, születési hely/idő, ...)
- Pénzügyi, elszámolási adatkezelés során is csak annyi adat jelenhet meg, ami elengedhetetlen a feladat ellátásához.

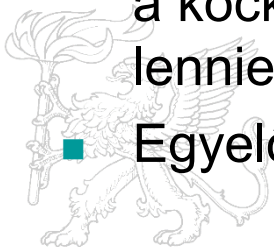


Magatartási kódex

- Adatvédelmi szabályzat nem szerepel a GDPR-ben
 - A szabályzat logikája az volt, hogy a releváns jogszabályokat össze kell gyűjteni, ami az adott intézményre vonatkozik. A GDPR szerint ilyen nem lesz (esetleg kivételesen egy-kettő). Ezért az intézmények nagy szabadságuk lenne abban, hogy milyen adatkezelési rendet alakítanak ki.
- Nem az intézményeknek kell létrehozniuk
 - A Magatartási Kódexet a GDPR (98) és (99) preambuluma szerint az érdekképviselő szervezetek, kamarák hozzák létre (pl. MOK, MGYK)
- Intézménykategóriánként (pl. háziorvosokra, gyógyszertárakra, rendelőintézetekre, kórházakra, szociális otthonokra, ...)
- A NAIH-nak jóvá kell hagynia. Összhangban kell legyen a GDPR-rel.
- Ez után az adott praxis, intézmény eldöntheti, hogy az előre elkészített Magatartási Kódex szerint működik, vagy saját működési rendet alakít ki.
- A tagállamok a GDPR-nél szigorúbb szabályokat alkothatnak az érintettek jogai védelmére, tehát érvényben maradhat az Eüak. 32. §

Adatvédelmi hatásvizsgálat

- Az 1990-es évek óta van Kanadában, az ottani adatvédelmi biztos „találta fel”.
- Onnan került át az USA-ba és az Egyesült Királyságba, majd Franciaországba és végül az EU-ba.
- Eddig egy magyar hatásvizsgálatról lehet tudni, amelyet nem fogadott el a NAIH.
- A hatásvizsgálat két részből kell álljon: egy adatkezeléssel és információbiztonsággal kapcsolatos helyzetkép (kezelt adatok köre, jogalapja, tárolási ideje, hálózat leírása, szerverek, tűzfalak, rendszerparaméterek, működési körülmények), majd ezt követi egy a kockázatokat elemző dokumentáció, legalább ötven oldalnak kell lennie (vagy még többnek).
- Egyelőre csak külföldi szakirodalom áll rendelkezésre.



Informatikai rendszer

- Az érintettek közvetlen hozzáférését biztosítani kellene a saját adataihoz (kórház, rendelőintézet, gyógyszerár) a (63) preambulum szerint, amennyiben lehetséges.
 - A HIS-ben sokkal régebbi adatok vannak, mint az EESZT-ben
- Az érintettek jogosultak lennének elektronikusan hordozható formában másolatot kapni a saját adataikról (nem csak PDF, hanem strukturált HL7, XML, DICOM, stb. formában)
- Az érintettek korlátozhatják az adataikhoz történő hozzáférést, tiltakozhatnak egy-egy adatkezelés ellen (ha kapnak előzetes felvilágosítást róla) és kérhetik az adatok törlését is.
- Egyes szerepkörökben olyan képernyők legyenek, ahol nem jelennek meg a személyes adatok (név, cím, TAJ) pl. gazdasági iroda, kutatás.



A GDPR-rel ütköző adatkezelések

- Az EESZT kényszerintézkedés alapú működtetése tiltakozási lehetőség nélkül,
- Az ÁEEK TEA adatállománya,
- A NEAK, OTH, NEFI 30 éves adatmegőrzési ideje,
- A személyes egészségügyi adatok 30 éves adatmegőrzési ideje,
- A felvilágosítás nélkül, kényszerintézkedés alapon működő regiszterek,
- A felvilágosítás (és hozzájárulás/tiltakozás) nélküli orvostudományi kutatás,
- A személyes egészségügyi adatok különféle hatósághoz továbbítása,
- A gyógyszerterek jogellenes machinációi a vényadatokkal,
- A HIS rendszerekben a mindenki minden adatot láthat beállítás
- Az egészségügyi adatok hosszú ideig online tartása.

Összefoglalás

- A jogi bizonytalanság miatt nem tudják az intézmények teljesíteni a kötelezettségeiket, amíg az adatkezelések jogalapja nem tisztázódik
- Nem világos, hogy a GDPR milyen módon lesz kikényszeríthető, ha a magyar bírósági rendszer nem hajlandó az alapján ítéletet hozni.
- Ha a NAIH nem tesz semmit, akkor az Európai Adatvédelmi Testületnél panaszt lehet tenni ellene.
- Alexin, Z.: *Jogalkotási feladatok az egészségügyben az Európai Unió Általános Adatvédelmi rendeletének hatályba lépésére tekintettel*, IME Interdiszciplináris Magyar Egészségügy, Vol. XVI. No.: 10, pp. 51-56, Larix Kiadó Kft. (2017.)





Köszönöm a figyelmet!