# GDPR AZ EGÉSZSÉGÜGYBEN

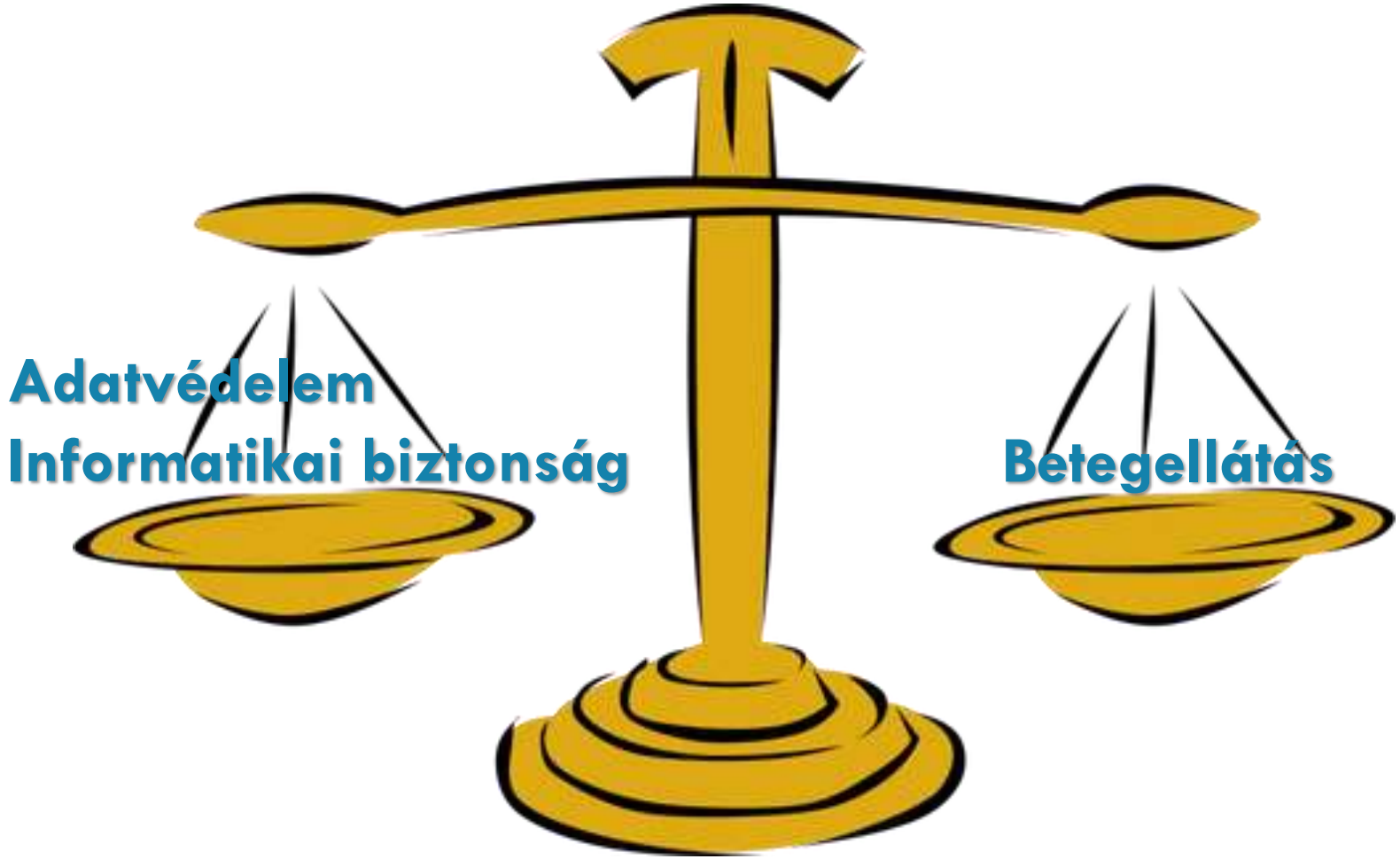
Az adatvédelem, az informatikai biztonság és a betegellátás egyensúlya

Varga Ferenc
Adatvédelmi tisztviselő
Elektronikus információbiztonsági rendszer felelős

2020. január30.

# BEVEZETŐ

# MI A FONTOSABB?




Képforrás: https://publicdomainvectors.org/en/free-clipart/Balance-scale-vector-image/9148.html

# MIRŐL LESZ SZÓ?

## RÖVIDEN A LEGFONTOSABBAKRÓL

EURÓPAI ÉS NAIH HATÁROZATOK

OKTATÁSOK, TUDATOSÍTÓ KAMPÁNYOK SZÜKSÉGESSÉGE

MIRE VAN IDŐ?

- Az adatvédelem a magánszféra egyik eszköze, **szükségszerűen a személyre irányul**
- Az adatbiztonság tárgya maga az adat, mely az adat integritásának és bizalmasságának a védelmét jelenti
- Az adatbiztonság megteremtését szolgálhatják **technikai** és **szervezési** intézkedések.

Forrás: EUZERT Kft. - oktatóanyag

# JOGSZABÁLYI HÁTTÉR

*1997. évi CLIV. törvény* az egészségügyről;

a *2013. évi L. törvény* az állami és önkormányzati szervek elektronikus információbiztonságáról;

*Az Európai Parlament és a Tanács (EU) 2016/679. rendelete* – GDPR (General Data Protection Regulation, azaz Általános Adatvédelmi Rendelet);

*2015. évi CXXIII. törvény* az egészségügyi alapellátásról;

*az 1997. évi XLVII. törvény* az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről;

*2011. évi CXII. törvény* az információs önrendelkezési jogról és az információszabadságról;

*2015. évi CCXXIV. törvény* az egyes egészségügyi és egészségbiztosítási tárgyú törvények módosításáról;

*187/2015. (VII. 13.) Kormány rendelet* az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;

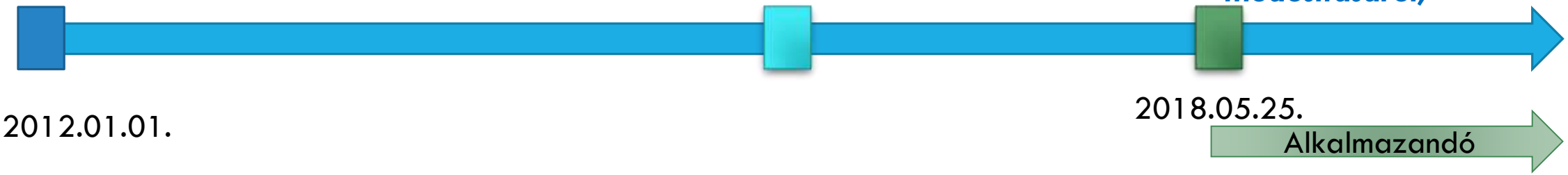
*2018. évi XXXVIII. törvény* az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról;

# GDPR

***2011. évi CXII. törvény***

***az információs önrendelkezési jogról és az információszabadságról (Info tv.)***

***2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról;***




GDPR – az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

# ÉRINTETT, AZONOSÍTHATÓ TERMÉSZETES SZEMÉLY

GDPR ->

„személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

Infotv. -> *

érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

* Megállapította: 2018. évi XXXVIII. törvény 2. § (1). Hatályos: 2018. VII. 26-tól.

# EGÉSZSÉGÜGYI ADAT

4. cikk

Fogalommeghatározások ->

15. „egészségügyi adat”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

12. „adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

# GDPR – JOGALAP (6. CIKK)

**A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:**

a) az érintett **hozzájárulását adta** személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan **szerződés teljesítéséhez** szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez** szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek** védelme miatt szükséges;

e) az adatkezelés **közérdekű** vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az **adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez** szükséges…

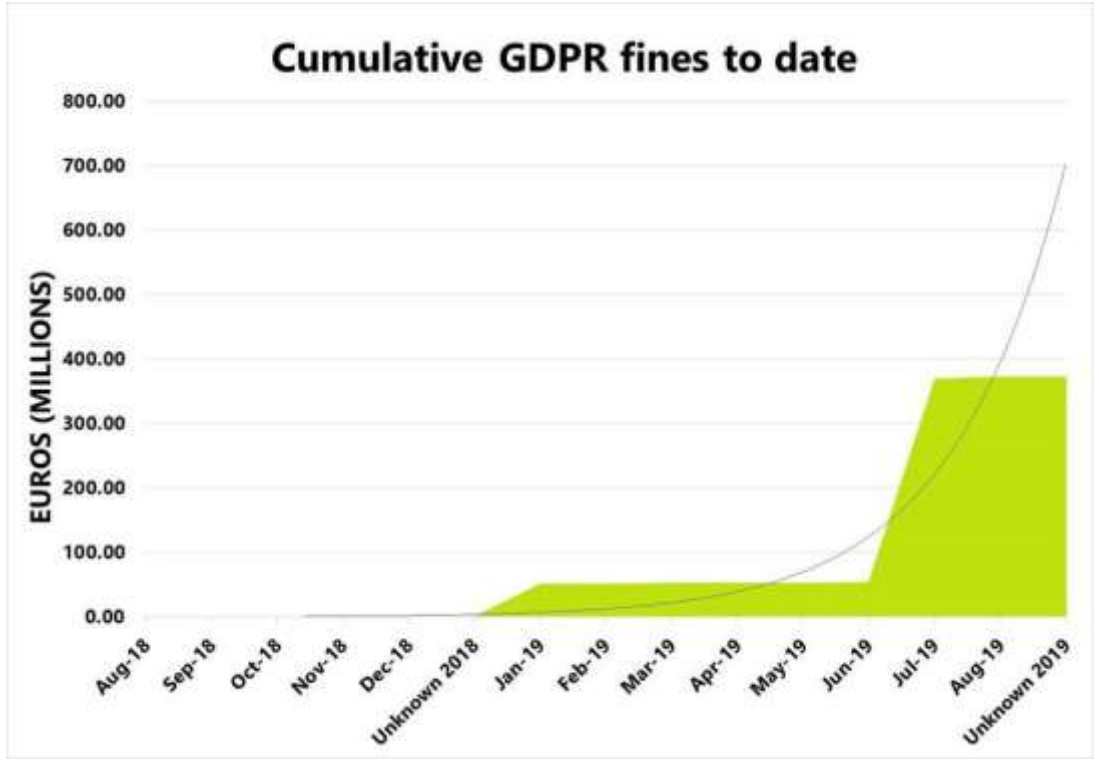
Forrás: https://www.gdpr.info.hu/gdpr-rendelet-szovege

# NEMZETKÖZI (EURÓPAI) HELYZET

Bírságok 2019 augusztus-szeptemberéig:

~120 milliárd forintnak megfelelő büntetés

~Magyarországon kb. 49-50 millió forint




Forrás: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

Forrás: https://blog.crosssec.com/infografika-gdpr-birsagok-europaban

# NEMZETKÖZI (EURÓPAI) HELYZET – PORTUGÁL KÓRHÁZ ESETE

A portugál adatvédelmi hatóság (CNPD) szerint a **Centro Hospitalar Barrerio Monitjo kórház** jogsértést követett el mivel nem megfelelően tárolta a betegek adatait és a hozzáférés szabályozása sem volt megfelelő.

985 felhasználó – orvosi jogosultság szintű hozzáféréssel -> 296 orvos dolgozott akkor

A felhasználók korlátozás nélkül fértek hozzá a betegek összes adatához

400.000 Euro büntetés

**2018**

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Forrás: http://medicalonline.hu/eu_gazdasag/cikk/korhazat_birsagoltak_a_gdpr_megsertese_miatt

# NEMZETKÖZI (EURÓPAI) HELYZET – BRITISH AIRWAYS

„Az emberek személyes adatai pont ilyenek - személyesek. Ha egy szervezet képtelen megvédeni az elvesztéstől, megsemmisítéstől vagy lopástól, akkor ez több, mint kellemetlenség. A törvény ezért egyértelmű - mert amikor személyes adatok feldolgozásával bíznak meg, akkor azokat gondosan kell kezelni.”

Elizabeth Denham

Az ICO közleménye szerint egy kibertámadás részeként a British Airways honlapját a támadók hamis holnapra irányították át és ezáltal az utasok ide feltöltött adatait ellopták. Számítások alapján 500.000 utas adata került illetéktelenek kezébe, ami miatt 66 milliárd forintnyi bírság kiszabását javasolták.

Forrás: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

# NAIH HATÁROZATOK EGÉSZSÉGÜGYI TÉMÁBAN

2012-es határozat (GDPR előtt!)

2013-as határozat (GDPR előtt!)

2014-es határozat (GDPR előtt!)

2015-ös határozat (GDPR előtt!)

2017-es határozat (GDPR előtt!)

2018-as határozat

2019-es határozat

„A felnőtt magyar lakosság többségét (62 százalék) érdekli saját adatainak védelme, közel ötöde (18 százalék) azonban nem foglalkozik a kérdéssel. Tájékozottság tekintetében megosztottak a válaszadók. 43 százalékuk inkább nem, 24 százalékuk inkább tájékozottnak vallotta magát. Miközben az adatvédelem tartalmával a megkérdezettek 61 százaléka tisztában van, meglepő lehet, hogy az információszabadság tartalmát mindössze 38 százalék ismeri.„ (2013)

Forrás: https://naih.hu/files/adatved-kozvelkut-2013-03.pdf

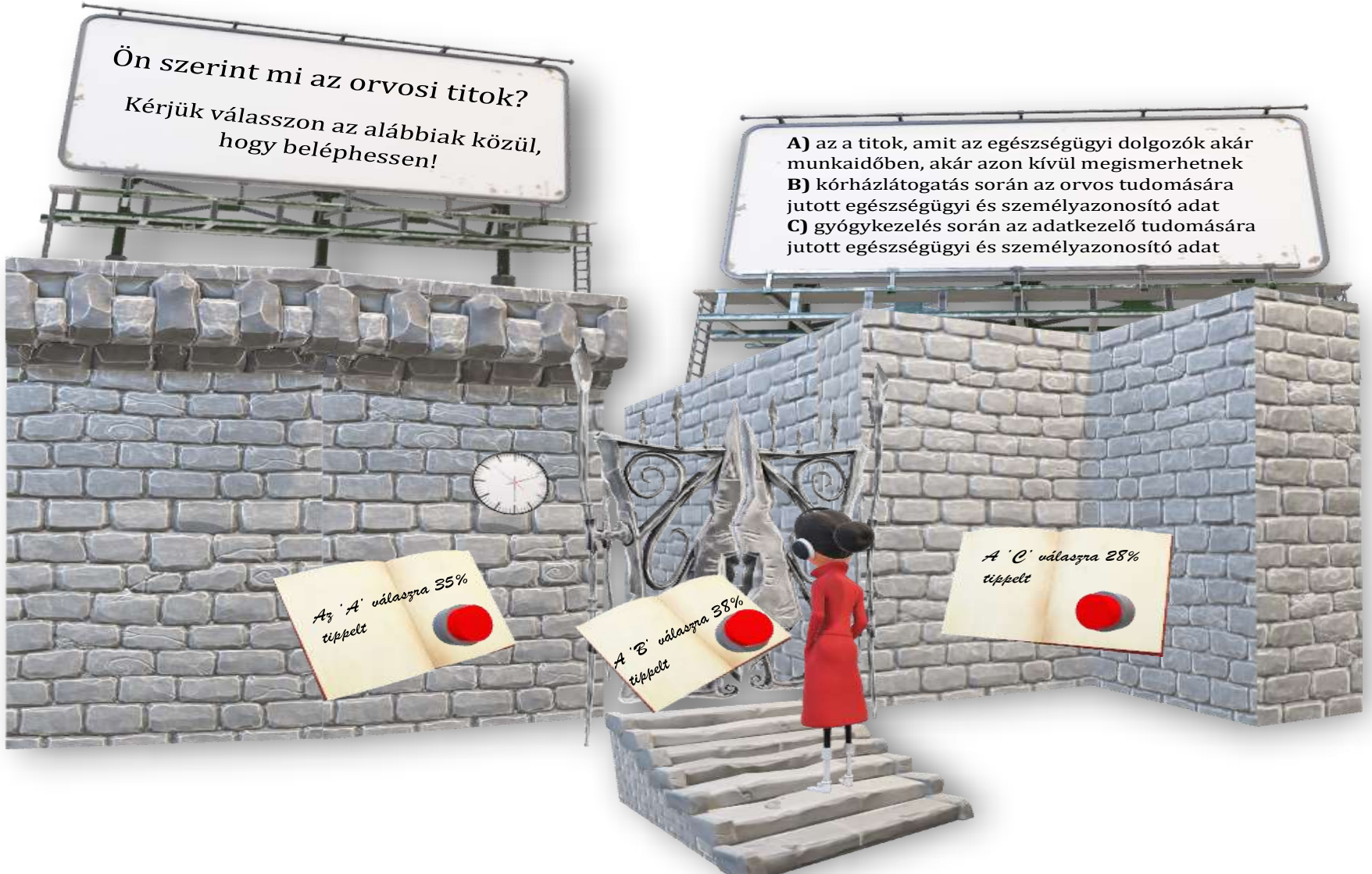
Nemzeti Adatvédelmi és Információszabadság Hatóság

Forrás: https://naih.hu

# MI AZ AMIT VÉDENÜNK KELL? CSAK EGÉSZSÉGÜGYI ADATOKAT?

- **Betegellátásban résztvevők adatai**
- **Betegellátással összefüggésbe hozható adatok**
- **Munkaügyi adatok**
- **Dolgozói adatok (pl.: orvosi alkalmassági)**
- **Szerződésekkel kapcsolatos anyagok, információk**
- **Konkrét beteggel összefüggésbe hozható kutatási anyagok**
- **Kutatási eredmények**
- **Jogszabályokban előírt egyéb adatok és rendszerek védelme**

# TUDATOSÍTÁS



# HA NEM TESZÜNK SEMMIT

# KÖSZÖNÖM A FIGYELMET!