

Fejlesztők kötelezettségei és felelőssége az AI Act és a GDPR alapján

dr. Kóródi Balázs LL.M. ügyvéd

mesterséges intelligencia és technológiai jogi szakjogász,
adatbiztonsági és adatvédelmi szakjogász

tel.: 70/385-3051, dr.korodi.balazs@outlook.com

Miről lesz szó?

- Szabályozás tárgya – a GDPR és az AI Act hatálya
- Paradigmaváltás? – Digital Omnibus
- Szerepkörök
- Kötelezettségek
- Felelősség

GDPR

- Horizontális
- Technológiasemleges
- Extraterritoriális
- Alapjogi jellegű, célja a személyiségi jogok védelme

AI Act

- Horizontális
- Technológiasemleges
- Extraterritoriális
- Szubszidiárius
- Termékbiztonsági, termékfelelősségi kiindulópont
- Kockázatalapú (tiltott, nagy kockázatú, átláthatósági kockázat)

AI Act – MI-rendszer

gépi alapú rendszer, amelyet

különböző autonómiaszinteken történő működésre terveztek, és amely

a bevezetését követően **alkalmazkodóképességet** tanúsíthat,

és amely a kapott **bemenetből** – explicit vagy implicit célok érdekében – **kikövetkezteti**, miként generáljon olyan **kimeneteket**, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket,

amelyek **befolyásolhatják a fizikai vagy a virtuális környezetet**;

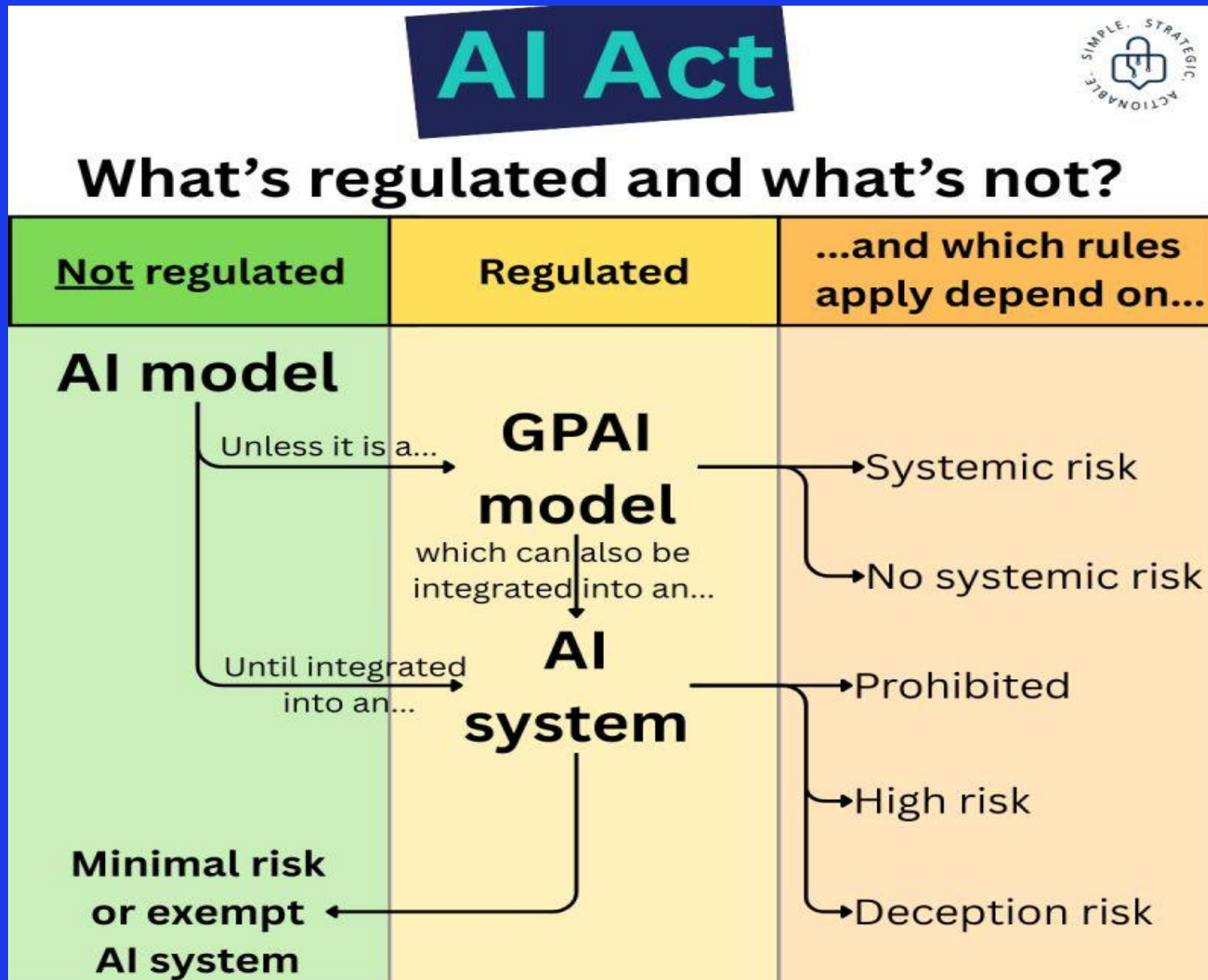
AI Act - Általános célú MI-modellek és MI-rendszerek

„általános célú MI-modell”: olyan MI-modell amely

- jelentős általánosságot mutat,
- különféle feladatok széles körének elvégzésére képes,
- többféle downstream rendszerbe vagy alkalmazásba integrálható,

„általános célú MI-rendszer”: általános célú MI-modellen alapuló MI-rendszer, amely – mind közvetlen felhasználás, mind más MI-rendszerekbe való integráció céljából – többféle célt képes szolgálni

AI Act - A szabályozás logikája



Szerepkörök – AI Act

szolgáltató

- MI-rendszert vagy GPAI-modellt fejleszt vagy fejleszttet,
- a saját neve vagy védjegye alatt forgalomba hozza,
- vagy az MI-rendszert üzembe helyezi (alkalmazónak, vagy saját használatra)

termékgyártó

- bizonyos feltételek esetén: szolgáltató

alkalmazó

- felügyelete alá tartozó MI-rendszert használja
- kivétel: személyes, nem szakmai használat

forgalmazó

importőr

meghatalmazott képviselő

Szerepkörök - GDPR

Adatkezelő

- fejlesztés – tanításhoz, teszteléshez használt adatok
- rendeltetésnek megfelelő finomhangolás
- általánosságban: a használattal járó adatkezelés

Adatfeldolgozó

- support
- SaaS

Változások a szerepkörben

GDPR

- Ha az adatfeldolgozó túlterjeszkedik a kapott utasításokon, adatkezelőnek kell tekinteni.

AI Act

- bármely szereplő szolgáltatóvá válhat, ha
 - nevét, vagy védjegyét elhelyezi az MI-rendszeren, vagy
 - jelentős módosítást hajt végre nagy kockázatú MI-rendszeren, úgy, hogy az továbbra is nagy kockázatú marad, vagy
 - eredetileg nem nagy kockázatú rendszer rendeltetését úgy módosítja, hogy az nagy kockázatúvá válik.

Kötelezettségek – Ai Act

nagy kockázatú MI-rendszer szolgáltatói

- III. fejezetben foglalt követelmények biztosítása:
 - Kockázatértékelés és tesztelés
 - Adatkormányzás és adatkezelés
 - Műszaki dokumentáció
 - Eseményrögzítés (naplózás)
 - Átláthatóság és az alkalmazóknak nyújtott tájékoztatás
 - Emberi felügyelet
 - Pontosság, stabilitás, kiberbiztonság
- Fel kell tüntetni a nevet, címet, védjegyet
- Minőségirányítási rendszer
- Megfelelőségértékelési eljárás
- Megfelelőségi nyilatkozat elkészítése, és a CE jelölés elhelyezése
- Nyilvántartásba vétel
- Korrekciós intézkedések, együttműködés a hatósággal

„deception risk” MI-rendszer szolgáltatói

- közvetlen interakcióra szánt MI rendszerek tervezése
- szintetikus tartalom jelölése géppel olvasható formában

Kötelezettségek - GDPR

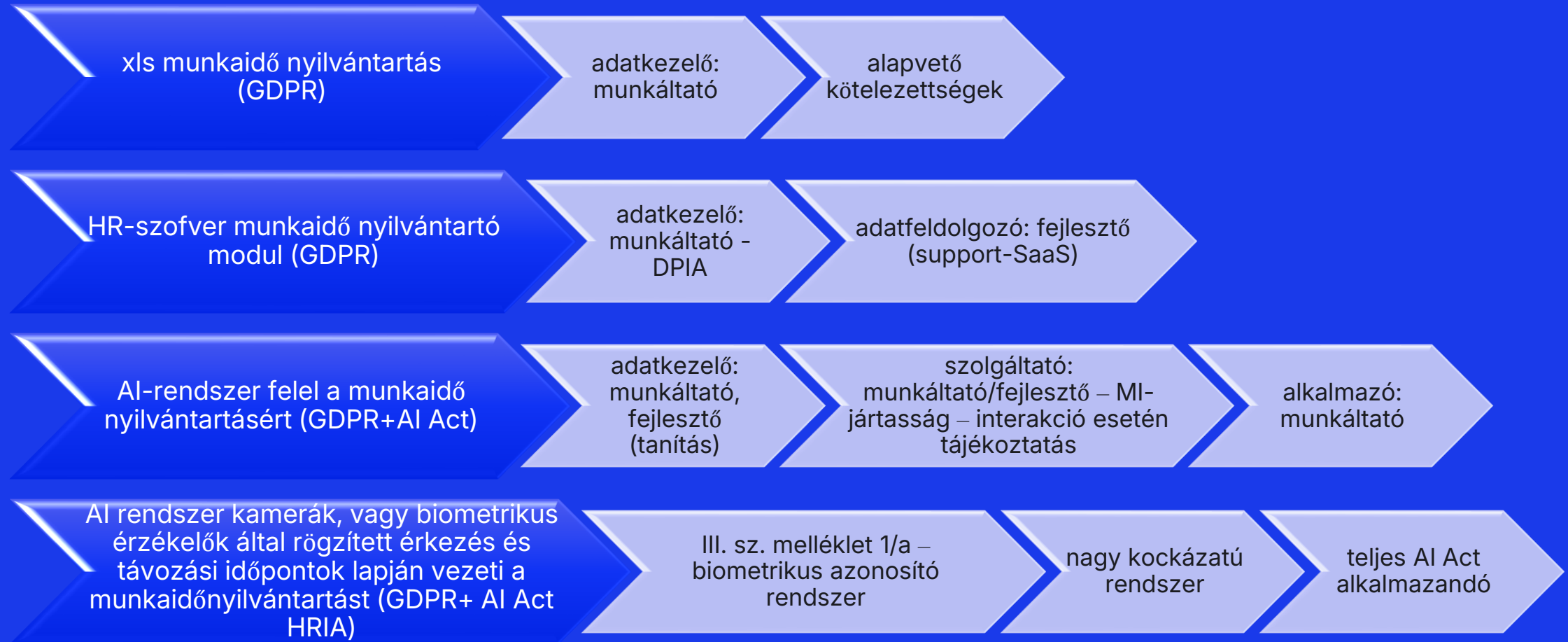
Adatkezelő

- adatkezelési tájékoztató: automatizált adatkezelés ténye, az alkalmazott logika, és annak hatása
- GDPR 22. cikk: automatizált döntéshozatal
- adatbiztonság
- beépített és alapértelmezett adatvédelem
- adatvédelmi hatásvizsgálat

Adatfeldolgozó

- szerződés és utasítás szerinti eljárás
- együttműködés

Egy példa...



Felelősség: új PLD

„termék”
fogalmának jelentős
kiterjesztése

- szoftver (operációs rendszer, appok),
- MI-rendszerek,
- digitális gyártási fájlok (pl. 3D nyomtatási sablonok),
- digitális szolgáltatások (pl. jármű navigációs rendszere),
- energia, gáz, víz.

a hibás termék új
meghatározása

- hibás, ha nem nyújtja a jogosan elvárható biztonságot,
- a folyamatos tanulásra vagy új tulajdonságok szerzésére való képességnek a termékre gyakorolt hatása,
- biztonság szempontjából releváns kiberbiztonsági követelmények,

kiterjesztett
felelősségi kör

- a gyártó, az alkotóelem gyártója, importőr, forgalmazó, meghatalmazott képviselő,
- logisztikai szolgáltató,
- online platform, ha gyártói/importőri szerepet tölt be.
- aki egy terméket lényegesen módosít, és úgy hozza forgalomba, gyártónak minősül.

Záró gondolat

- Anthropic felmérés:
<https://www.anthropic.com/features/81k-interviews>
- A felhasználók azt várják a mesterséges intelligenciától, hogy levegye a vállukról a mindennapi terheket – munkában és magánéletben egyaránt –, hogy több idejük, energiájuk és lehetőségük maradjon egy jobb, teljesebb életre.

Köszönöm a figyelmet!

dr. Kóródi Balázs LL.M. ügyvéd

mesterséges intelligencia és technológiai jogi szakjogász,
adatbiztonsági és adatvédelmi szakjogász

tel.: 70/385-3051, dr.korodi.balazs@outlook.com