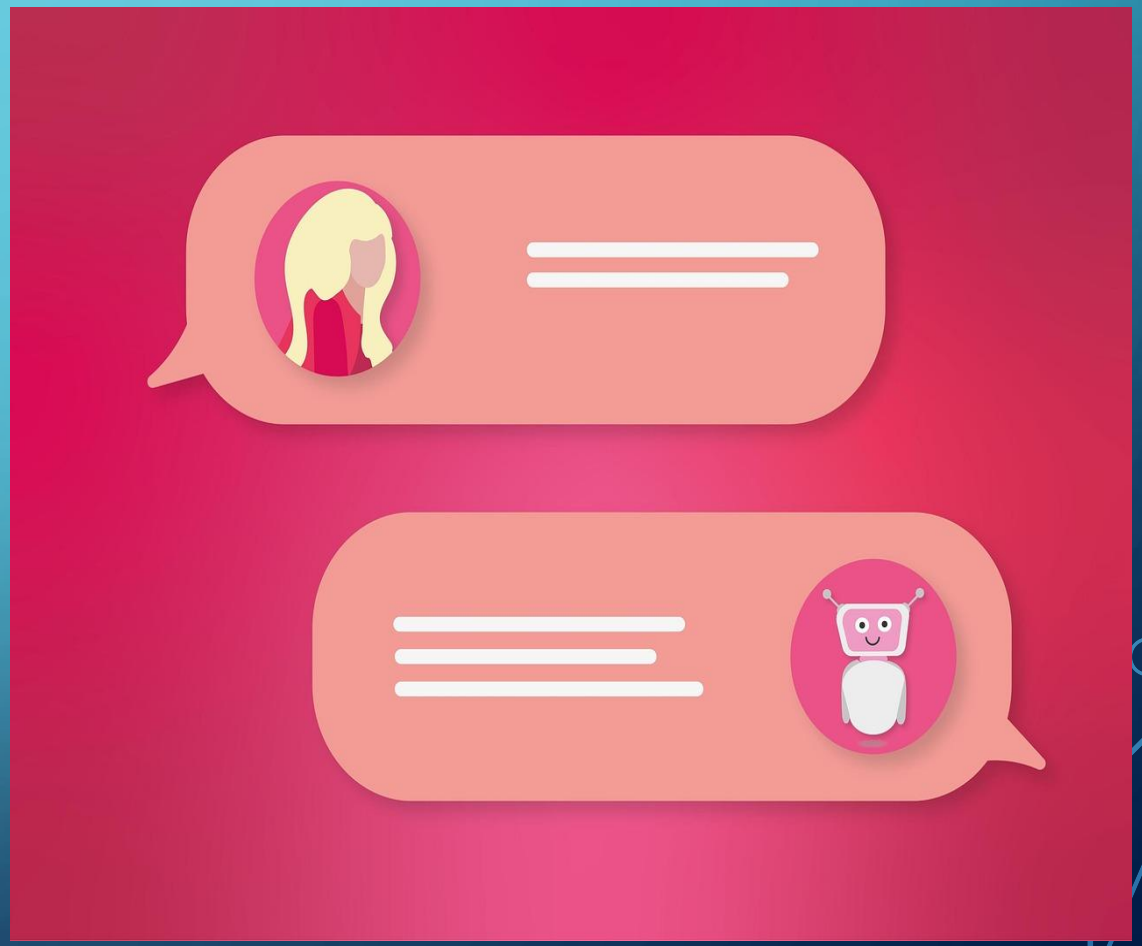
SHADOW AI – ADATVÉDELEM ÉS FELELŐSSÉG AZ ELLENŐRIZETLEN MI-HASZNÁLAT KORÁBAN

Dr. Necz Dániel (LL.M.) ügyvéd,

megbízott oktató (KRE-ÁJK)

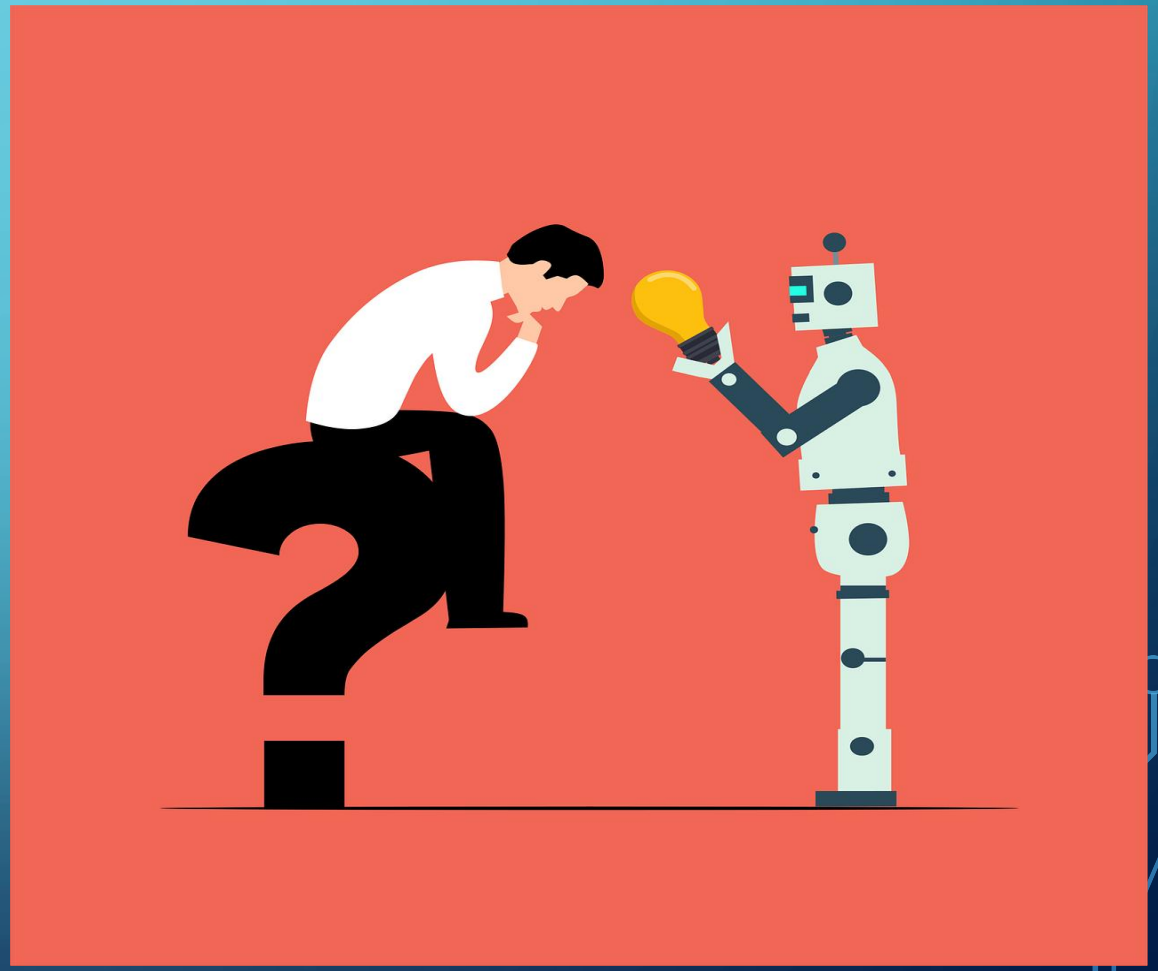
Mi az a shadow AI?

- Nem jóváhagyott AI-használat a cégen belül
- Gyakran munkavállalók saját eszközeire/eszközeiről való adatfeltöltés
- Gyakran privát fiók használata
- Ügyféladatok, munkatársak adatainak megadása (pl. kik vettek részt egy adott meetingen, miről szólt)



Milyen problémákat okoz a shadow AI?

- Kontrollálatlan adatáramlás
- Személyes, gyakran szenzitív adatok kiszivárgása (pl. e-mail szövegek írása, dokumentumok feltöltése, chatbot-al beszélgetés szenzitív témában)
- Jogszabályi és compliance kockázatok
- Gyakran etikai, PR szempontok (pl. HR-es pályázók, orvos betegek adatait adja meg)



A shadow AI-al kapcsolatos adatvédelmi kockázatok

- Személyes adatok jogosulatlan kezelése
- Adatbiztonsági problémák / sérülékenység
- Adatvédelmi incidens kockázata
- Külső AI szolgáltató bevonása

Incidenskezelés

- AI-használat gyakran nem észlelhető
- Incidensforrás nehezen visszakövethető
- Reakció éppen ezért késleltetett lehet
- Elsőre problémásnak nem tűnő AI használat is incidenshez vezethet (pl. notetaker tool nem megfelelő használata)

Hozzáférés az adatokhoz

- Prompt = adatátadás harmadik félnek
- Nem mindig ismert, hova kerül az adat
- Tanulóadatként, személyre szabáshoz való felhasználás
- Privát fiók adataival való keveredés (pl. családtagok is hozzáférhetnek)

A felelős meghatározása

- GDPR szerinti felelősség: adatkezelő / adatfeldolgozó
- AI Act szerinti felelősség: szolgáltató / alkalmazó
- Munkavállaló felelőssége – elsősorban munkajogi, de akár adatkezelőként is felelhet (pl. saját célból vesz át munkahelyéről megszerzett adatokat)

AI Use Policy I.

- Engedélyezett AI eszközök, felhasználási módok, adatkörök listája
- Tiltott eszközök, felhasználási módok, adatkörök meghatározása
- Általános használati keretek
- Alapvető adatvédelmi szabályok

AI Use Policy II.

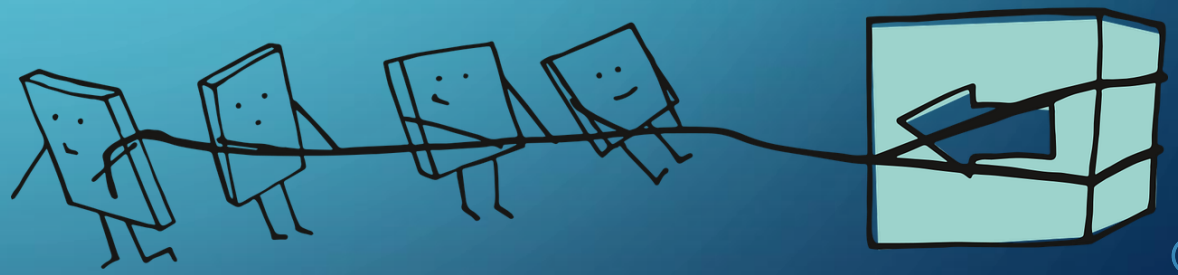
- Promptolási szabályok (jó példák)
- Külső AI-ba való adatbevitel
- Ellenőrzési és jóváhagyási folyamat
- Oktatás és tudatosságnövelés

Mire érdemes még figyelni?

- Shadow AI számos esetben előfordulhat
- Nem elegendő a puszta szabályzat, technikai korlátok
- Emberi viselkedés a kulcstényező

Záró gondolatok

- A shadow AI-al kapcsolatos adatvédelmi problémák nem csak kifejezetten AI-t használó szervezeteket érinthetnek
- Fontos a megfelelő vállalati/szervezeti szabályozás mielőbbi kialakítása
- A megfelelő AI használatra vonatkozó szabályok munkatársak oktatásába való beépítése



KÉRDÉSEK?

KÖSZÖNÖM A FIGYELMET!

Dr. Necz Dániel LL.M. ügyvéd, óraadó

(KRE-ÁJK)

daniel.necz@simplegal.eu