AI vs. GDPR

Co si můžeme dovolit s osobními údaji pacientů při využití AI nástrojů?

Bezpečné nasazení AI v nemocničním prostředí

Jiří Benedikt, DPO Krajské nemocnice Liberec

Nařízení GDPR (EU) 2016/679 · Zákon č. 110/2019 Sb. · AI Act

Agenda

01 **Jak fungují velké jazykové modely (LLM)?**

Proč AI samo o sobě není nepřítel

02 **Kde skutečně leží riziko?**

Cloud, přenos dat, ztráta kontroly

03 **Nové hrozby: Prompt injection a další**

Konkrétní scénáře ve zdravotnictví

04 **Právní rámec: GDPR, AI Act, MDR**

Co nám legislativa ukládá

05 **Smluvní zajištění zpracovatelů**

Jak vybírat AI poskytovatele bezpečně

06 **Kritéria pro výběr bezpečných nástrojů**

Praktický checklist pro nemocnici

07 **Role DPO a AI governance v nemocnici**

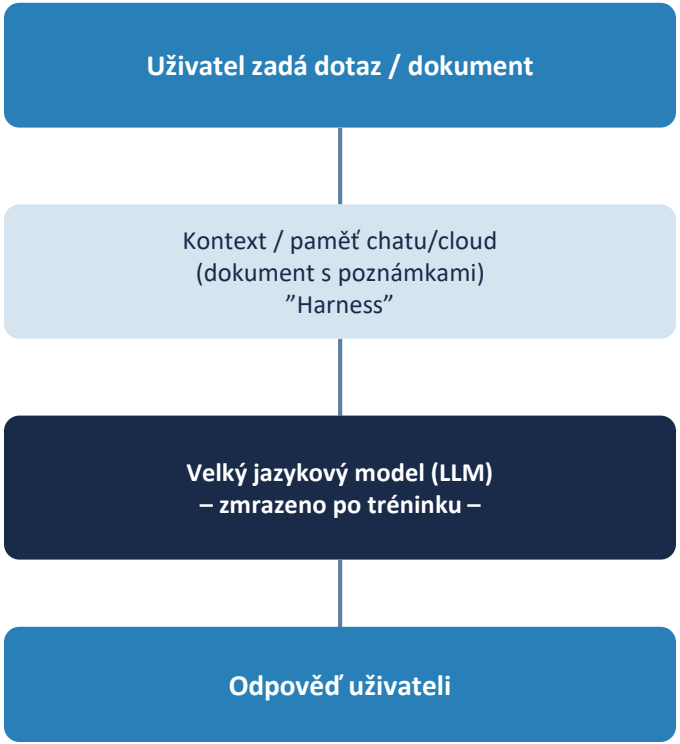
Kdo nese odpovědnost?

08 **Doporučení a závěr**

Co dělat hned zítra

Jak fungují velké jazykové modely?

- LLM jsou po dokončení tréninku zmrazeny – nerozvíjejí se dál z vašich vstupů
- Model si nemůže zapamatovat data od jednoho uživatele a vyzradit je jinému
- "Paměť" chatu = dokument s poznámkami, který se při každé konverzaci předkládá modelu znovu
- Pokud by poskytovatel použil vaše data k dotrénování nového modelu → riziko úniku (malé, ale reálné)
- Používejte nástroje, kde je zakázáno učit se na vašich datech, nebo kde to lze vypnout



⚠ *Data od vás neputují k jiným uživatelům*

Riziko netvoří AI – tvoří ho cloud

Data opouštějí nemocnici

Cloudové AI služby = přenos dat mimo kontrolu zdravotnického zařízení. Platí stejné riziko jako u každé cloudové aplikace.

Nelze ověřit, jak poskytovatel zachází s daty

Bez auditu a smluvního závazku nevíte, co se děje s citlivými daty pacientů na serverech třetí strany.

Akvizice menšího poskytovatele

Pokud menšího AI poskytovatele koupí větší firma, data mohou přejít pod novou jurisdikci nebo politiku zpracování.

Rizikové integrace s dalšími nástroji

Propojení AI s EHR, PACS nebo jinými systémy nemocnice rozšiřuje plochu útoku a potenciál úniku dat.

Závěr: Vybírejte poskytovatele s prokázanou reputací, certifikacemi a přísnou smlouvou (DPA).

Nové typy hrozeb ve zdravotnickém prostředí

Prompt injection – co to je?

Útočník skryje do dokumentu nebo e-mailu instrukce, které AI omylem vykoná jako příkaz.
Příklad: Do propouštěcí zprávy pacienta je vložen skrytý text → AI asistent ho zpracuje a odešle citlivé informace na externí adresu.

Únik do trénovacích dat

Pokud poskytovatel AI dotrénuje model na vašich datech, obsah zpráv a diagnóz se může projevit ve výstupech pro jiné uživatele.

Autoritářský režim

Poskytovatel AI sídlí nebo provozuje infrastrukturu v jurisdikci, kde mají úřady přístup k datům bez soudního příkazu.

Ztráta kontroly při akvizici

Menší AI startup je koupí větší firma se zcela jinou bezpečnostní politikou a sídlem mimo EU.

Právní rámec: co platí pro nemocnice?

Zdravotní údaje = citlivé osobní údaje (čl. 9 GDPR) → podléhají přísné zákonné ochraně

GDPR (EU) 2016/679 + zákon 110/2019 Sb.	Zpracování osobních údajů, souhlas, záznamy zpracování, DPIA, smlouva se zpracovatelem
AI Act	Hodnocení rizikovosti AI systémů, povinná gramotnost (čl. 4), dokumentace, zákaz zakázaných praktik
NIS2 / ZKB	Kybernetická bezpečnost provozovatelů kritické infrastruktury (velké nemocnice)
MDR / IVDR	AI jako zdravotnický prostředek nebo diagnostická pomůcka → dokumentovatelnost, auditovatelnost

⚠ *Perspektiva rizika: AI Act a GDPR hodnotí riziko z pohledu dotčené osoby (pacienta), ne organizace!*

Smluvní zajištění zpracovatele (DPA)

Každý AI nástroj, jemuž předáváte osobní údaje pacientů, musí být smluvně zajištěn jako zpracovatel dle čl. 28 GDPR.

1	**Smlouva o zpracování osobních údajů (DPA / Zpracovatelská smlouva)** Musí být uzavřena před zahájením zpracování. Definuje účel, rozsah, dobu zpracování a povinnosti zpracovatele.
2	**Zákaz využití dat pro trénink modelu** Poskytovatel nesmí vaše data (incl. anonymizovaná) použít ke zlepšování svých modelů bez výslovného souhlasu.
3	**Místo uložení dat – preferenčně EU/EHP** Přenos dat do třetích zemí vyžaduje další záruky (standardní smluvní doložky, adekvátnost).
4	**Auditní právo a transparentnost** Právo provést nebo nechat provést audit u zpracovatele, nebo certifikace dle čl. 42 GDPR.
5	**Povinnost hlášení incidentů** Zpracovatel musí bezodkladně (do 24–72 h) informovat správce o bezpečnostním incidentu.

Jak vybírat AI nástroje pro nemocnici?

Praktický checklist pro odpovědné nasazení

- ✓ Nástroj určen pro firemní / enterprise použití (ne spotřebitelská verze)
- ✓ Smlouva o zpracování dat (DPA) – dostupná a podepsatelná
- ✓ Data se nepoužívají k tréninku modelu (nebo jde vypnout)
- ✓ Datová centra v EU/EHP
- ✓ Certifikace (ISO 27001, GDPR compliance report)

- ✗ Vyhněte se nástrojům bez jasné dokumentace o zpracování dat
- ✗ Vyhněte se free nástrojům pro zdravotnická data bez DPA
- ✗ Vyhněte se nástrojům od poskytovatelů sídlících mimo důvěryhodné jurisdikce

Konkrétní omezení pro nasazení AI ve velké nemocnici

NELZE / ZAKÁZÁNO	PODMÍNĚNĚ POVOLENO
✗ Nahrávat identifikovatelné záznamy pacientů do spotřebitelských AI nástrojů	→ Zpracování anonymizovaných dat – s řádnou anonymizací
✗ Používat AI pro automatické rozhodování o léčbě bez lidského dohledu (čl. 22 GDPR)	→ AI podpora diagnostiky - jako second opinion, vždy s dohledem lékaře
✗ Sdílet data s AI poskytovatelem bez platné DPA	→ Administrativní AI (propouštěcí zprávy, kódování) – se schváleným DPA a záznamem zpracování
✗ Používat AI nástroje klasifikované jako 'nepřijatelné riziko' dle AI Actu	→ Interní AI řešení – bez přenosu dat mimo nemocniční infrastrukturu
✗ Profilovat pacienty způsobem, který je diskriminační (pohlaví, etnický původ, diagnóza)	→ Edukační a výzkumné využití – s etickým schválením a anonymizací

Role DPO a AI governance v nemocnici

AI evangelista ≠ AI governance officer – jsou to dvě protichůdné role

	AI evangelista	AI Governance / DPO
Cíl	Prosazovat a rozvíjet adopci AI	Kontrolovat, řídit rizika, zajišťovat soulad
Přístup	Rychlá implementace, inovace	Kritický odstup, 2. linie obrany
Střet zájmů?	Motivován výsledky	ANO, pokud rozhoduje o nasazení AI
Nezávislost	Není vyžadována	Garantována zákonem (čl. 38 GDPR)

Proč je DPO ideálním AI Governance Officerem?

Ze zákona nezávislý · Přímý přístup k vedení · Zná toky dat v organizaci · Dosažitelný pro subjekty údajů · Přenositelné znalosti z GDPR do AI Act

⚠ DPO nesmí rozhodovat o způsobu využití AI – to by ohrozilo jeho nezávislost!

Praktická doporučení pro nemocnici

1 **Zmapujte, jaké AI nástroje jsou v nemocnici AKTUÁLNĚ používány**

Zahrnuje i neoficiální / shadow IT použití zaměstnanci

2 **Nastavte interní politiku přípustného použití AI**

Co smí kdo používat, s jakými daty a za jakých podmínek

3 **Pro každý nástroj uzavřete DPA se zpracovatelem**

Bez DPA = porušení GDPR; ani anonymizace vás plně neochrání

4 **Zajistěte AI gramotnost personálu (čl. 4 AI Actu)**

Vzdělávání v oblasti rizik, rozpoznání prompt injection, reportování incidentů

5 **Jmenujte AI Governance Officera (ideálně DPO)**

Jasná odpovědnost, 2. linie obrany, nezávislá kontrolní funkce

6 **Zvažte on-premise nebo privátní cloud AI řešení**

Maximální kontrola nad daty, žádný přenos mimo nemocniční infrastrukturu

Závěr

"Žádná technologie není bez rizika.
Cílem je rizikům rozumět a umět je minimalizovat
na úroveň, kterou jsme ochotni akceptovat."

- AI samo o sobě vaše tajemství neprozradí
- Riziko tvoří cloud a přenos dat mimo kontrolu nemocnice
- Legislativa: GDPR, AI Act, MDR (Medical Device Regulation – nařízení EU č. 2017/745 o zdravotnických prostředcích)
- Smluvní zajištění každého zpracovatele je povinností
- Jasná governance = jmenovaný AI Officer (ideálně DPO)