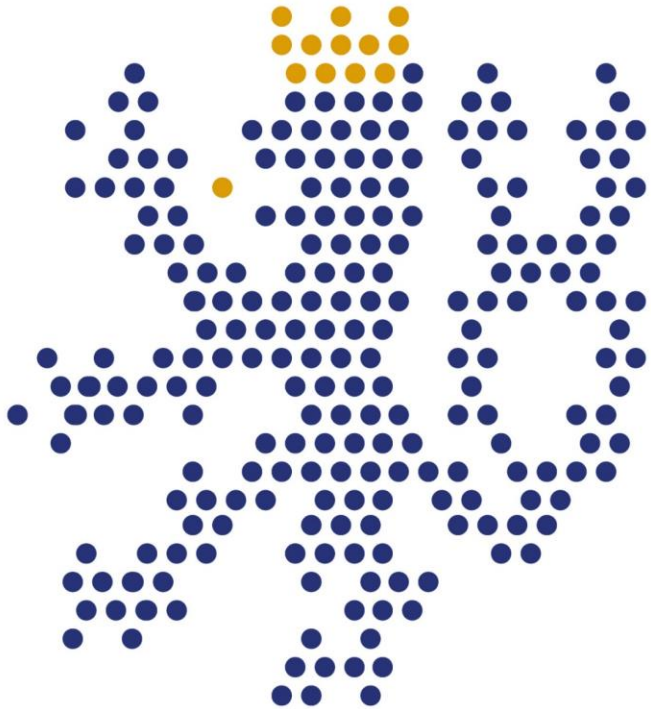


Úřad pro ochranu osobních údajů

AI a ochrana osobních údajů

Mgr. Jaromír Kuba

10. dubna 2025

Obsah

- Regulační rámec AI a ochrany údajů
- Rizika "šedého využití" AI
- Přenos údajů mimo EU
- Rizika
- Praktická doporučení

Regulační rámec

- AI Akt (Akt o umělé inteligenci)
  - Nařízení přímo účinné
  - Český zákon v přípravě
  - V tuto chvíli jen některé povinnosti (AI s nepřijatelným rizikem)

- AI a GDPR
  - Český zákon účinný od 24. 4. 2019 (skoro výročí)
    - V tandemu s GDPR
  - AI často pracuje s osobními údaji
  - Je-li služba zdarma, zboží jste vy!

Umělá inteligence a GDPR

- AI může zpracovávat obrovské objemy osobních údajů
- GDPR se vztahuje na všechny systémy, které pracují s osobními údaji
- Na co nezapomenout:
  - Transparentnost
  - Zásada minimalizace
  - Omezení účelu zpracování, právní základ
- Může být třeba vypracovat DPIA (zvláště v případě zpracování biometriky)

AI Akt a jeho dopad

- Kategorizace rizika:
  - Nepřijatelné (sociální scoring, podprahové věci, zranitelnosti)
  - Vysoce rizikové systémy – celá řada povinností - příloha III
  - Omezené riziko – hlavně transparentnost (AI pro interakci a vytvářející obsah)
  - Minimální riziko – bez extra povinností (většina systémů)
- Obecné AI modely – speciální kategorie, v rámci které se bavíme zejména o LLM (ChatGPT atd.)

Šedé využívání AI v organizacích

- Využití bez vědomí organizace
- Bez pravidel
- Rizika pro subjekty údajů, únik informací z organizace
- Profilace a automatizované rozhodování
- AI se učí a ne vždy lze tyto funkce vypnout!
- Proškolení (ne povinná certifikace!)
- Pravidla využití AI
  - Není-li AI povolena, zaměstnanci hledají cesty v „šedé zóně“

Čínské AI modely

- Přístup státu k datům
- Odlišný přístup k ochraně osobních údajů
- Chybí rozhodnutí o odpovídající ochraně
- V případě použití standartních smluvních doložek může být problém s reálnou nemožností dodržet sjednaný smluvní vztah (vládní přístup k datům)
- AI lze přesto využít k jiným účelům
- Provoz „on-premise“, případně v cloudu v EU – někdy vhodné řešení.

Přenos údajů mimo EU

- Schrems II a neplatnost „Privacy Shieldu“
- Standardní smluvní doložky (SCC)
- Rámec ochrany soukromí EU-USA
  - Budoucnost? (Rámec opět u soudu – případ T-553/23)
- Vliv na cloudové služby a LLM modely (většina LLM z USA)
- Evropské modely
- Provoz on-premise (český jazyk přestává být problém)

Rizika AI

- AI je dobrý sluha, ale zlý pán
- Halucinace, hodně se zlepšuje
- Dezinformace (nelze vyloučit, ale provozovatelé mají účinná protiopatření)
- Vládní narrativ (Čína)
- Ke strašení není důvod
  - Katastrofické scénáře pro IT profese šíří zejména lidé bez reálných zkušeností z IT branže.
  - Ubývá otrocké a nezáživné práce, AI opravuje chyby, které jsme si v kódu sami vyrobili. ☺

Rizika AI

- Deepfake, umělou inteligencí generovaný obsah
  - Již nemůžeme věřit svým očím
  - Nové výzvy v oblasti posuzování pravosti dokumentů a fotografií, staré metody detekce přestávají být účinné
  - Aplikace typu „změna fotky, aby vypadala jako panenka…“ – nahráváte svou fotografii a minimálně e-mail – dobrovolné ztotožnění
- Kde jsou ta data?
  - Historie chatů, přístup provozovatele/vlády, prodej dat, učení AI
- Prompty typu „Vygeneruj fotografii ve stylu seriálu …“
  - Služby nelze kvůli přetížení využívat k legitimním účelům

AI a zločin

- Podvodné e-maily s chybami úplně nezmizí
  - Kriminálník preferuje člověka, který skočí i na hůře připravený podvod, neboť u něj je větší šance, že peníze skutečně pošle
- AI pomáhá s přípravou velmi dobře okopírovaných webů a e-mailů bez chyb
- Modely s vypnutými omezeními (píšou viry, připravují exploity), někdy ale stačí „správně se zeptat“.
- Zpracování výstupů z bezpečnostních nástrojů, pomáhá i obráncům (detekce anomálií v síťovém provozu atd.)

AI mění pravidla hry

- Anonymizace zvuku složitější
  - Lze identifikovat i některé formy pozměněného hlasu
- Nestačí jen lehce „rozkostičkovat“ obličej
  - AI umí dle kostiček „odhadnout“ možný původní vzhled
- 3D tisk klíče z fotografie
  - Hlavně u jednodušších klíčů, ale vývoj jde dopředu
  - Využití AI ke konverzi 2D objektu na 3D, služby pro generování STL pro 3D tisk
  - Nenechávejte přístupové karty a klíče bez dozoru, ne fotky na sociální sítě (kopírování přístupových karet – „Magic Cards“)

Ai odhadne původní vzhled







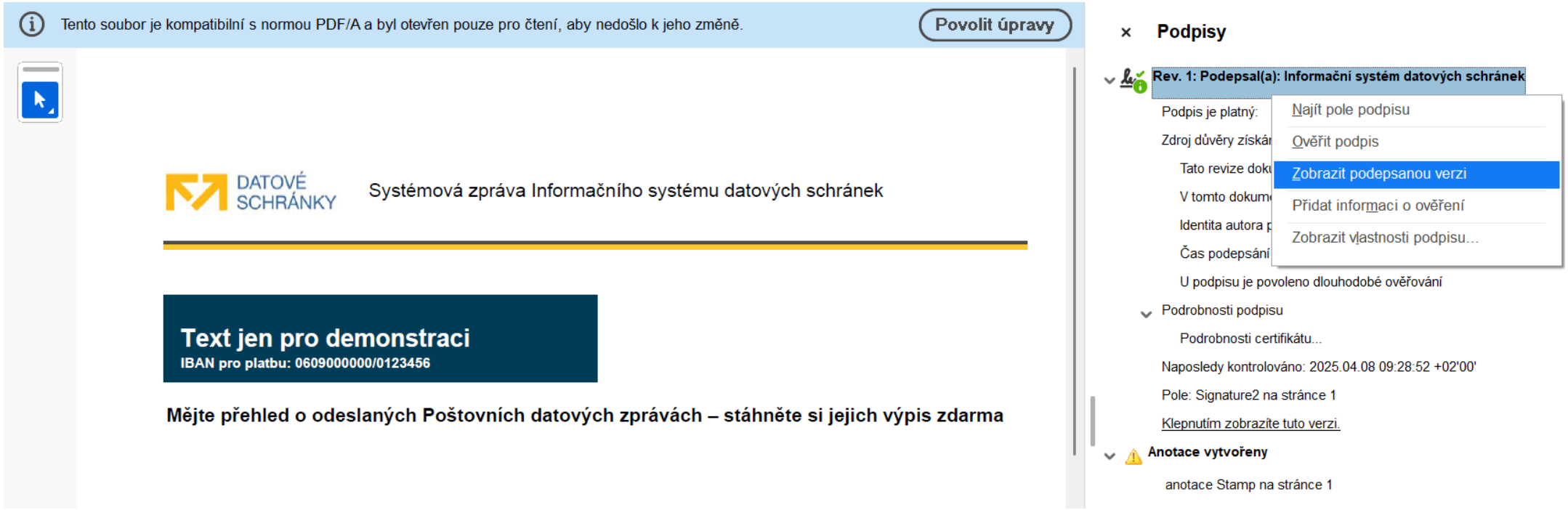
Doporučení

- Hledejte cesty, jak AI maximálně využít
  - Skvělý juniorní programátor k ruce
  - Ověřujte tvrzené informace (prompt „Když nevíš, tak to řekni“)
  - AI = konkurenční výhoda,

- Většina služeb jde přepnout do režimu, kdy se neučí ze zadaných dat
- Provoz modelů on-premise (např. přes program Ollama)
- Soulad s legislativou je nutnost
- Etické využívání AI

Pozvánka na Workshop

- Budeme upozorňovat i na metody pozměňování PDF a jak je rozpoznat



Děkuji za pozornost

jaromir.kuba@uoou.gov.cz