BARCAMP · 11. DUBNA 2026

AI ve firmách a organizacích

Mezi hype a realitou. Co skutečně funguje?

Pavol Hejný · Promptbook

Dva extrémy, se kterými se potkávám

„AI máme hotové"

„Před 3 lety jsme udělali školení na ChatGPT."

- Jednou za čas někdo použije chat
- Žádná integrace do procesů
- Žádná pravidla, žádná strategie
- „My už AI děláme" = jeden prompt měsíčně

„AI nahradí všechny"

„Vyhodili jsme polovinu programátorů a účetní oddělení."

- Slepá víra v AI bez kontroly
- Žádné guardrails, žádné review
- Výstupy nikdo nekontroluje
- Incidenty jsou jen otázkou času

Realita je složitější. A paradoxně často není o samotných AI modelech.

Model vs. Harness

Realita je složitější. A paradoxně často není o samotných AI modelech.

Přeceňujeme hype, podceňujeme dlouhodobý efekt

Zbytečný tlak na rychlost v aplikacích

Nové formy softwaru

Je to o všem okolo

AI model je motor. Ale auto potřebuje volant, brzdy a pravidla silničního provozu.

🔒 Ochrana dat
Kam tečou vaše data? Kdo k nim má přístup? Co říká GDPR?

✅ Spolehlivost
Jak poznáte, že výstup je správný? Kdo kontroluje kvalitu?

👥 Oprávnění
Kdo smí co používat? Kdo vidí jaká data?

> *Nejdůležitější otázka není „jaký AI model použít?"*
> *ale „jak zajistit, že výstupy budou správné, bezpečné a pod kontrolou?"*

Ochrana dat: Kam tečou vaše informace?

Když zaměstnanec vloží interní dokument do ChatGPT:

- Data jdou na servery OpenAI (USA)
- Mohou být použita pro trénink modelu
- Nemáte kontrolu, kdo k nim má přístup
- **GDPR compliance = otázka za milion**

Totéž platí pro Google Gemini, Microsoft Copilot a další cloudové služby.

Otázky, které si musíte položit:

- Kde běží model? (cloud / on-prem)
- Co se děje s daty po zpracování?
- Máte smlouvu o zpracování dat?
- Jsou data šifrovaná at rest i in transit?
- Můžete data smazat na požádání?

Pokud neznáte odpovědi, nemáte AI strategii. Máte risk.

Spolehlivost a kontrola kvality

AI hallucinuje. To není bug, to je vlastnost.

Typické problémy:

- AI vymyslí zákon, který neexistuje
- Shrne dokument, ale vynechá klíčový odstavec
- Odpoví sebevědomě, ale špatně
- Výstup se liší pokaždé, i na stejný vstup

Bez kontroly kvality riskujete:

- Právní problémy
- Poškození reputace
- Špatná rozhodnutí na základě špatných dat

Jak kontrolovat kvalitu:

1. **Human-in-the-loop** – člověk vždy schvaluje kritické výstupy
2. **Pravidla a guardrails** – AI má explicitní omezení
3. **Testování** – automatické kontroly výstupů
4. **Audit trail** – kdo se na co ptal, co AI odpověděla
5. **Verzování** – co se změnilo a proč

> *Důvěřuj, ale prověřuj. Vždy.*

Management oprávnění

Ne každý ve firmě potřebuje přístup ke všemu.

Kdo smí co?

Role	Přístup
Vedení	Strategické reporty, KPI
HR	Personální data, smlouvy
Právní	Smlouvy, compliance dokumenty
Marketing	Veřejná data, kampaně
Zákaznická p.	FAQ, historie komunikace

AI nástroj musí respektovat stejná oprávnění jako vaše interní systémy.

Co se stane bez řízení oprávnění?

- Marketingový stážista se přes AI dostane k finančním datům
- AI asistent prozradí interní strategii
- Zákaznická podpora vidí personální záznamy

Řešení:

- Role-based access control (RBAC)
- Oddělené knowledge bases per tým
- Logování všech dotazů
- Pravidelný audit přístupů

Jak si vybírat AI nástroje?

Kritéria výběru:

Kritérium	Proč
Kde běží?	Cloud vs. on-prem, jurisdikce
Data retention?	Jak dlouho si nechává vaše data?
Compliance?	SOC2, ISO 27001, GDPR
Vendor lock-in?	Můžete snadno přejít jinam?
Integrace?	Napojení na vaše stávající systémy
Cena?	Per-seat, per-token, per-organizace

Červené vlajky:

- ❌ „Data neukládáme" bez důkazu
- ❌ Žádná smlouva o zpracování dat
- ❌ Nemožnost on-prem deploymentu
- ❌ Proprietární formát bez exportu
- ❌ Žádný audit log

Zelené vlajky:

- ✅ Transparentní data flow
- ✅ SOC2 / ISO certifikace
- ✅ On-prem možnost
- ✅ API s dokumentací
- ✅ Export dat kdykoliv

Jak nahrazovat a automatizovat lidskou práci?

Nenahrazujte lidi. Nahrazujte drudgery.

Co automatizovat:

- Třídění emailů a prvotní odpovědi
- Kontrola dokumentů proti interním pravidlům
- Generování reportů z dat
- FAQ a zákaznická podpora (level 1)
- Sumarizace dlouhých dokumentů

Co NEautomatizovat:

- Finální rozhodnutí s právním dopadem
- Komunikaci s klíčovými klienty
- Strategické plánování
- Krizový management

Postup nasazení:

1. **Zmapujte procesy** – kde lidé tráví čas rutinou?
2. **Vyberte pilotní projekt** – malý, měřitelný, nízké riziko
3. **Nastavte metriky** – jak poznáte, že to funguje?
4. **Spusťte pilot** – 1 tým, 1 proces, 1 měsíc
5. **Vyhodnoťte** – čas, kvalita, spokojenost
6. **Škálujte** – co funguje, rozšiřte dál

> *Nejlepší AI projekt není ten nejsložitější.*
> *Je to ten, který ušetří nejvíc času s nejmenším rizikem.*

Vlastní knowledge base a kontext

Generické AI neví nic o vaší firmě. **To je problém i příležitost.**

Co dát AI k dispozici:

- Interní dokumentace a postupy
- FAQ a často řešené problémy
- Šablony a vzory dokumentů
- Pravidla a compliance požadavky
- Historické case study

Jak to udělat správně:

- Verzované dokumenty (ne zastaralé)
- Strukturovaná knowledge base
- Pravidelná aktualizace
- Oddělení veřejných a interních dat

Příklad: Praha 13

Městská část Praha 13 používá Promptbook s vlastní knowledge base:

- Interní dokumentace a předpisy
- Informace pro občany
- Pravidla pro zpracování žádostí

Výsledek:

Senior expert, který není programátor, si sám vytvořil virtuálního asistenta ze své dokumentace.

> *„Neprogramátoři mohou vytvářet a nasazovat virtuální asistenty ze své vlastní dokumentace."*
> *– Jakub Svoboda, Praha 13*

Rulesety: Pravidla, která AI dodržuje

AI bez pravidel je zaměstnanec bez onboardingu.

```
Právní expert firmy XY

PERSONA Profesionální, detail-oriented.
         Pouze české právo.

KNOWLEDGE firemni-prirucka.pdf
KNOWLEDGE gdpr-smernice.docx

RULE Nikdy neraď mimo českou jurisdikci.
RULE Cokoliv vyžadující soud eskaluj
     na {Vedoucí právního}.
```

Pravidla jsou **explicitní, verzovaná a auditovatelná**.

Proč jsou pravidla klíčová:

- AI ví, co smí a co nesmí
- Konzistentní výstupy napříč dotazy
- Auditovatelnost – můžete dokázat, proč AI odpověděla tak, jak odpověděla
- Škálovatelnost – jeden expert nastaví pravidla, stovky lidí je používají

Typy pravidel:

- 🚫 **Zákazy** – co AI nesmí dělat
- ✅ **Požadavky** – co musí vždy udělat
- 🔄 **Eskalace** – kdy předat člověku
- 📋 **Formát** – jak má výstup vypadat

Shrnutí: 7 kroků k AI ve firmě

1. **Zmapujte procesy** – kde je rutina, kde je hodnota?
2. **Vyřešte data** – kde běží, kdo má přístup, GDPR
3. **Nastavte oprávnění** – ne každý potřebuje všechno
4. **Vytvořte knowledge base** – dejte AI kontext vaší firmy
5. **Definujte pravidla** – co AI smí, co nesmí, kdy eskaluje
6. **Spusťte pilot** – malý projekt, měřitelné výsledky
7. **Kontrolujte kvalitu** – human-in-the-loop, audit, testy

> **AI není kouzlo. Je to nástroj. A nástroj potřebuje proces.**

Nová forma softwaru?

AI Agent jako zaměstnanec s vlastní "Subjektivitou"?

Díky za pozornost!