Vytvoření interní AI politiky – praktický návod pro firmy

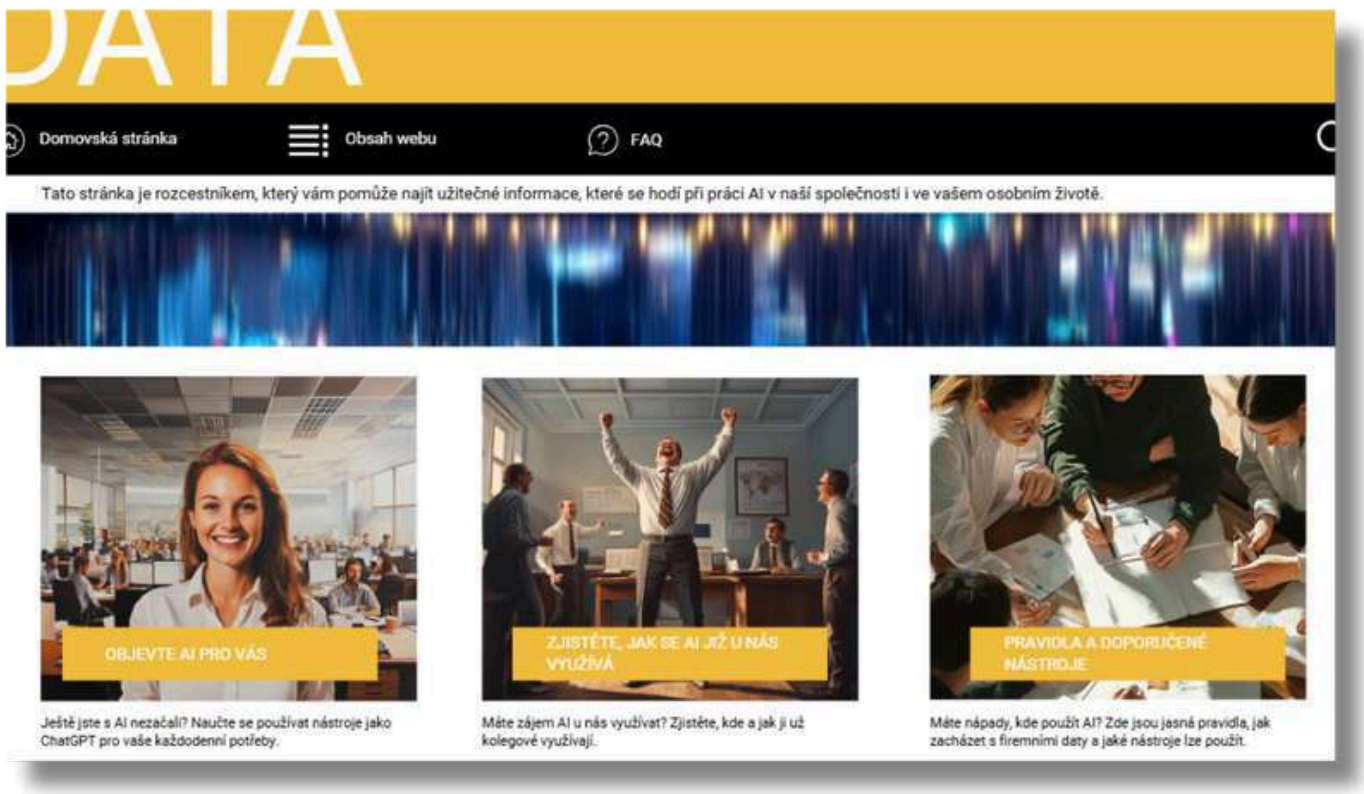
Implementace AI do firemních procesů přináší nejen příležitosti, ale i rizika, pokud nejsou nastavena jasná pravidla a postupy. Interní AI politika pomáhá zaměstnancům pochopit, jak AI využívat bezpečně, efektivně a v souladu s firemními hodnotami. Tato kapitola vám poskytne konkrétní kroky, jak takovou politiku ve vaší firmě vytvořit.

1. Založte AI Portál

AI Portál slouží jako centrální místo, kde zaměstnanci najdou veškeré informace týkající se používání AI ve firmě. Může jít o interní webovou stránku nebo portál, který bude obsahovat:

- **Pravidla a zásady pro používání AI** (včetně toho, co smí být sdíleno ve veřejných AI nástrojích).
- **Návody a příklady využití AI** (use cases z praxe, specifické pro vaši firmu).
- **Seznam schválených AI nástrojů pro firemní účely.**
- **Kontaktní osoby** – AI Navigátoři, kteří jsou k dispozici pro dotazy a pomoc.

Tím zajistíte, že všichni zaměstnanci budou mít přístup k jednotným informacím a pravidlům, která je snadné najít.



2. Určete AI Navigátory (AI průvodce)

Ve firmě je důležité mít konkrétní osoby, které budou zodpovědné za dohled nad implementací a používáním AI technologií. Tito AI Navigátoři jsou klíčoví pro zajištění toho, aby všichni zaměstnanci věděli, jak AI správně využívat a na koho se mohou obrátit v případě dotazů.

Jejich úkoly zahrnují:

- **Vzdělávání zaměstnanců**: AI Navigátoři jsou zodpovědní za proškolení ostatních zaměstnanců o tom, jak používat schválené AI nástroje, jak správně třídit data dle jejich citlivosti a jak chránit firemní informace.
- **Poskytování podpory:** Zaměstnanci se na AI Navigátory mohou obracet, pokud mají otázky ohledně konkrétního využití AI, nebo pokud si nejsou jisti, zda jejich data splňují pravidla pro práci s AI nástroji.
- **Monitorování a implementace**: AI Navigátoři sledují, jak jsou AI nástroje ve firmě používány, a pomáhají při jejich správné implementaci. Pravidelně vyhodnocují jejich efektivitu a případně navrhují úpravy či nové nástroje.
- **Zajištění souladu s politikou:** AI Navigátoři dohlíží na to, aby všichni zaměstnanci dodržovali pravidla stanovená interní AI politikou, a řeší případné porušení zásad.

AI Navigátoři tak slouží jako **hlavní kontaktní osoby** pro všechny otázky týkající se AI a pomáhají firmě využívat AI zodpovědně a efektivně. Každý zaměstnanec by měl vědět, kdo je jejich AI Navigátor a jak se s ním spojit.

3. Stanovte pravidla pro práci s různými úrovněmi citlivosti dat

Rozdělte citlivost dat například do pěti stupňů a jasně stanovte, která data lze využívat v jakých nástrojích. Každý zaměstnanec by měl vědět, co jednotlivé stupně znamenají a kde mohou tato data použít. Zde je příklad, jak můžete jednotlivé úrovně nastavit: (pošlu separé jako tabulku)

Stupeň citlivosti	**Popis**	**Příklady**	**Povolené nástroje a použití**
Stupeň 1 – Veřejná data	Informace, které jsou veřejně dostupné a jejichž sdílení nepředstavuje žádné riziko.	Obecné dotazy týkající se produktů.	Veřejné AI nástroje (např. ChatGPT).
Stupeň 2 – Interní data s nízkým rizikem	Data, která nejsou veřejná, ale jejich sdílení by nezpůsobilo škodu.	Obecná firemní metodologie, marketingové informace.	Interní AI nástroje (např. AI systém na Azure nebo interní firemní AI platforma).
Stupeň 3 – Citlivá data	Informace, které obsahují firemní know-how nebo procesy, jejichž únik by mohl způsobit ztrátu konkurenční výhody.	Firemní know-how, interní procesy.	Pouze ve vysoce zabezpečených interních systémech.
Stupeň 4 – Vysoce citlivá data	Finanční údaje, strategické plány, citlivé projekty.	Finanční údaje, strategické plány.	Pouze s vysoce zabezpečenými nástroji a za přísných podmínek.
Stupeň 5 – Přísně tajná data	Osobní údaje zákazníků, obchodní tajemství, důvěrné smlouvy.	Osobní údaje, obchodní tajemství.	Nelze používat v žádných AI nástrojích.

4. Definujte jasně, co AI je a co není

Pro zaměstnance je důležité pochopit, jaké technologie spadají pod AI a jaké ne. Vysvětlete jednoduchým způsobem, jaké funkce AI ve firmě plní a co od ní mohou očekávat. Příkladem může být:

- **AI nástroje**: Nástroje na analýzu dat, chatboty, predikční modely apod.
- **Ne-AI nástroje**: Jednoduché automatizace nebo systémy, které nejsou založeny na strojovém učení či pokročilých algoritmech.

4. Stanovte, na co AI používat smíte a na co ne

Vytvořte přehled povolených a zakázaných aktivit spojených s používáním AI. Každý zaměstnanec by měl vědět, co je pro firemní účely přípustné:

- **Povolené aktivity**: Automatizace rutinních úkolů, analýza anonymizovaných dat, zákaznická podpora.
- **Zakázané aktivity**: Používání AI k manipulaci s osobními údaji bez svolení, automatické rozhodování o důležitých firemních otázkách (např. propouštění) bez lidského dohledu.

Dále stanovte, co zaměstnanci mohou používat pro osobní účely.

Například: Je povoleno používat veřejné AI nástroje jako ChatGPT pro osobní projekty, pokud se nepracuje s firemními daty.

5. Přidejte přehled konkrétních firemních use cases

V AI Portálu by měl být k dispozici přehled konkrétních příkladů, jak AI využít ve firmě. Ukažte zaměstnancům, jak mohou AI používat v jejich každodenní práci. Například:

- **Marketing**: Analýza zákaznických preferencí a predikce budoucí poptávky.
- **HR**: Náborový proces s pomocí AI asistence (vylučování předsudků při výběru kandidátů).
- **Výroba**: Optimalizace výroby na základě predikce poptávky.

Tímto způsobem získají zaměstnanci inspiraci a praktické návody, jak AI zapojit do svých aktivit.

5. Ochrana dat při používání AI

Zajistěte, aby zaměstnanci věděli, jak chránit data při práci s AI, zejména s veřejnými nástroji.

Například:

- **Vypnutí tréninkového módu:** Při používání nástrojů, jako je ChatGPT, vypněte možnost, aby data byla využívána pro další trénink modelů (pokud nástroj tuto funkci umožňuje).
- **Anonymizace dat**: Pokud pracujete s veřejnými nástroji, ujistěte se, že data, která sdílíte, jsou anonymizovaná, aby nedošlo k úniku citlivých informací.

7. Pravidelná revize a aktualizace politiky

AI technologie se rychle vyvíjejí, a proto je důležité, aby vaše firemní politika byla pravidelně aktualizována. Stanovte pravidlo, že politika bude kontrolována minimálně jednou ročně, a přizpůsobujte ji novým technologiím a bezpečnostním rizikům.

"Zaveďte pravidelná školení zaměstnanců o používání AI – to zajistí lepší pochopení nástrojů a ochrání vaši firmu před nesprávným použitím."

Vzorová směrnice

Interní směrnice pro používání umělé inteligence ve „FIRMĚ“

1. Úvod

Tato směrnice stanovuje pravidla a postupy pro bezpečné a etické používání umělé inteligence (AI) ve „FIRMĚ“. Jejím cílem je zajistit efektivní a odpovědné využívání AI technologií v souladu s firemními zásadami, právními normami a ochranou dat. Směrnice vymezuje pravidla, která zaměstnancům pomohou pochopit, co AI je, jak ji používat, a jak minimalizovat rizika spojená s jejím používáním.

2. Definice

- **Umělá inteligence (AI)**: AI je technologie simulující lidské myšlení, schopná učení, rozhodování a zpracování jazyka. Ve „FIRMĚ“ se to týká nástrojů, které slouží například k automatizaci procesů, analýze dat a zákaznické podpoře.
- **Citlivá data**: Jakákoli data, která obsahují osobní údaje, obchodní tajemství, finanční informace nebo jiná důvěrná data, která by mohla způsobit škodu při neoprávněném přístupu nebo použití.

3. Zodpovědnosti a transparentnost

- **AI Navigátoři:** Jmenovaní zaměstnanci, kteří mají za úkol poskytovat podporu v oblasti používání AI, organizovat školení a zajišťovat, že pravidla této směrnice jsou dodržována.
- **Zaměstnanc**i: Každý zaměstnanec, který používá AI, je odpovědný za její správné a bezpečné používání v souladu s touto směrnicí. Zaměstnanci jsou také zodpovědní za kontrolu výstupů AI a hlášení jakýchkoli nesprávných výsledků nebo incidentů.
- **Transparentnost:** AI Navigátoři zajistí, že všichni zaměstnanci budou informováni, kdy a jak jsou AI nástroje ve firmě používány. Veškeré relevantní informace budou k dispozici v interním **AI Portálu** (např. na intranetu).

4. Klasifikace a použití dat

Pro ochranu dat zavádíme klasifikaci dat do 5 úrovní citlivosti. Každý zaměstnanec je povinen dodržovat tato pravidla:

- **Stupeň 1 – Veřejná data**: Informace dostupné veřejnosti, jako jsou obecné údaje o produktech nebo veřejné reporty. Mohou být používány v jakýchkoli AI nástrojích včetně veřejných (např. ChatGPT).
- **Stupeň 2 – Interní data s nízkým rizikem:** Data, která nejsou veřejná, ale jejichž únik nezpůsobí výrazné škody (např. obecná firemní metodologie). Mohou být používána v interních nástrojích (např. AI systém na Azure).
- **Stupeň 3 – Citlivá data:** Informace týkající se firemního know-how, které nesmí být sdíleny s veřejnými AI nástroji. Mohou být používána pouze v interních AI nástrojích s přísnými bezpečnostními opatřeními.
- **Stupeň 4 – Vysoce citlivá data**: Citlivé finanční údaje, strategické plány nebo projekty. Musí být chráněna šifrováním a nesmí být sdílena prostřednictvím AI nástrojů bez schválení vedení.
- **Stupeň 5 – Přísně tajná data**: Osobní údaje, důvěrné smlouvy a obchodní tajemství. Tato data se nesmí používat v žádných AI nástrojích.

5. Postupy pro používání AI

5.1. Povolené aktivity:

- AI lze používat k automatizaci rutinních úkolů, analýze anonymizovaných dat nebo zlepšení zákaznické podpory, pokud jsou dodržena pravidla pro ochranu dat dle klasifikace.
- Pro osobní účely mohou zaměstnanci používat veřejné AI nástroje, pokud se nepracuje s firemními daty vyšších stupňů (Stupeň 3–5).

5.2. Zakázané aktivity:

- Není povoleno používat AI k automatickému rozhodování o závažných otázkách (např. nábor, propouštění) bez lidského dohledu.
- Nesmí být používána k manipulaci dat, šikaně nebo diskriminaci.

5.3. Nové AI nástroje:

- Před nasazením nového AI nástroje musí být provedeno hodnocení rizik a schválení od AI Navigátorů a IT oddělení.
- Každý nový nástroj musí projít kontrolou, zda splňuje interní pravidla ochrany dat a bezpečnosti.

5.4. Školení:

- Všichni zaměstnanci, kteří pracují s AI, musí projít pravidelným školením o používání AI a ochraně dat. Školení je povinné jednou ročně a musí zahrnovat praktické ukázky, jak správně AI používat.

6. Bezpečnostní pravidla a ochrana dat

6.1. Anonymizace a šifrování dat:
Všechna data vyššího stupně citlivosti (Stupeň 3–5) musí být anonymizována a šifrována, pokud jsou používána s AI nástroji.

6.2. Ochrana přístupu:
Přístup k datům vyššího stupně je omezen pouze na autorizované osoby. Přístup k AI nástrojům musí být zabezpečen dvoufaktorovou autentizací.

6.3. Bezpečnostní incidenty:
V případě úniku dat nebo nesprávného použití AI je nutné okamžitě informovat AI Navigátory a řídit se akčním plánem pro řešení incidentů (viz Akční plán).

7. Kontrola výsledků a pravidelný audit

7.1. Kontrola výsledků:
Výstupy z AI nástrojů musí být pravidelně kontrolovány za účelem identifikace případných nepřesností nebo zaujatosti (bias). Každý tým musí provádět kontrolu alespoň jednou měsíčně.

7.2. Audity:
Interní AI nástroje budou podrobeny pravidelným auditům, aby byla zajištěna jejich funkčnost, bezpečnost a etické používání. Audity provádí IT oddělení společně s AI Navigátory minimálně jednou ročně.

8. Revize a aktualizace

8.1. Pravidelná revize:
Tato směrnice bude revidována každoročně na základě technologického vývoje a legislativních změn. Za revizi je odpovědné vedení společně s AI Navigátory.

8.2. Zlepšování na základě zpětné vazby:
Zaměstnanci jsou povzbuzováni k poskytování zpětné vazby o používání AI a směrnice. Na základě jejich podnětů budou pravidla upravována a doplňována.

9. Závěr
Všichni zaměstnanci „FIRMĚ“ jsou povinni tuto směrnici dodržovat. Porušení pravidel může vést k disciplinárním opatřením. Pravidla používání AI jsou nezbytná pro zajištění bezpečnosti, etiky a efektivity naší firmy.

Datum platnosti: