



**AI** Eticky



Příručka  
**Bezpečné  
a správné zavádění  
AI do firem**

Barbora Brabcová

# Proč tahle příručka vznikla?



## Vítejte v příručce.

kteřá vás provede jedním z nejdůležitějších témat současnosti – **etikou v umělé inteligenci**.

Umělá inteligence (AI) dnes proniká do všech oblastí našeho života i podnikání, a s tím přicházejí nejen nové příležitosti, ale také nová rizika.

Cílem této příručky je poskytnout firmám praktický návod, jak zavádět AI zodpovědně, bezpečně a v souladu s etickými zásadami.

Inspirací pro mě vždy byly myšlenky Isaaca Asimova, který ve svých dílech představil koncept „zákonů robotiky“ – pravidel, která měla zabránit robotům v ohrožení lidí.




### **Ale co samotní lidé? Chovají se vždy k technologiím správně?**

Dnes, kdy máme v rukou nástroje jako je AI, si musíme sami položit otázku: „Jak můžeme zajistit, že AI nebude zneužita?“

Etika v AI není jen teoretický koncept – je to praktická nutnost. Pokud firmy chtějí dlouhodobě prosperovat a udržet si důvěru zákazníků, musí zajistit, že jejich AI systémy budou nejen efektivní, ale také bezpečné a transparentní.

Tato příručka vám ukáže, jak na to.

## Kontakt

 Barbora Brabcová  
 barbora.brabcova@bebecon.cz  
 LinkedIn

## Dozvíte se:

- ✓ Proč je etika a bezpečnost v AI klíčová pro váš byznys.
- ✓ Jak identifikovat rizika při používání AI.
- ✓ Jak zavádět AI ve firmě prakticky, bezpečně a transparentně.

Společně objevíme způsoby, jak lze **AI** implementovat tak, aby se stala **nástrojem**, který nejen zlepšuje vaši produktivitu, ale i **chrání vaši značku a zákazníky**.

***Jakou roli hraje etika v technologických inovacích, které denně používáte?***



# OBSAH

1. Proč je etika v AI klíčová pro budoucnost a váš byznys?
2. Příprava na zavedení AI – klíčové otázky
3. Jak identifikovat rizikové oblasti při používání AI
4. Jak správně zavádět AI ve firmě
5. Jak měřit úspěch a efektivitu AI ve firmě
6. Vytvoření interní AI politiky – praktický návod pro firmy
7. Akční plán pro řešení úniku dat nebo nesprávného použití AI
8. Průběžný rozvoj a optimalizace AI ve firmě

# 1. Proč je etika v AI klíčová pro budoucnost a váš byznys?

Tento e-book vznikl jako součást iniciativy „**AI Eticky**“, kterou jsem založila, abych pomohla firmám, jednotlivcům i celé společnosti využívat AI zodpovědně a s ohledem na etické zásady.

V březnu 2023 jsem se jako první v České republice začala intenzivně zabývat otázkou etiky v AI. Sepsala jsem **Etické desatero práce s AI**. Toto desatero se stalo základem mého přístupu k využívání AI ve firmách, na školeních a konzultacích, které vedu.

Implementace AI nabízí obrovské výhody – od zrychlení procesů až po úspory nákladů. Nicméně s těmito přínosy přichází i řada rizik.

## Používáme ale AI eticky a bezpečně?



*"Jak by vaše firma reagovala, kdyby došlo k etickému selhání AI systému? Máte připravený plán?"*

## 3 nejdůležitější důvody, proč potřebujete etickou a bezpečnou AI



### **Zákaznická důvěra a reputace**

Firmy, které veřejně ukazují, že AI používají transparentně a zodpovědně, mají náskok před konkurencí. Navíc jediný incident, kdy AI selže, může poškodit roky budovanou reputaci.



### **Ochrana dat**

AI musí pracovat se zabezpečenými daty, jinak riskujete únik citlivých informací.



### **Dlouhodobá udržitelnost**

Eticky nastavená AI přináší firmě větší odolnost vůči budoucím legislativním změnám a skandálům.

# Jaké přínosy může etická AI firmám přinést?

Etická a bezpečná AI není jen o ochraně před riziky. Správně nastavené principy mohou firmám přinést reálné výhody, které se projeví v dlouhodobém růstu a posílení pozice na trhu.



**Důvěra zákazníků:** Firmy, které aktivně pracují na zodpovědném využívání AI, si budují pevnější vztahy se zákazníky. Transparentnost v používání AI posiluje loajalitu a zlepšuje vnímání značky.



**Snížení právních rizik:** Etické používání AI snižuje pravděpodobnost právních sporů, pokut nebo sankcí, které mohou vzniknout z neetického nebo nezabezpečeného nakládání s daty.



**Zvýšení efektivity:** Pokud je AI dobře nastavena a používána v souladu s etickými zásadami, může firmě výrazně pomoci zefektivnit procesy a zamezit chybám při zpracování dat.



**Konkurenční výhoda:** Firmy, které aktivně komunikují o etickém využívání AI, mohou získat náskok před konkurencí, která tyto aspekty ignoruje.



**Posílení firemní kultury:** Implementace etických zásad pro AI vede k vytvoření pozitivního pracovního prostředí, kde se zaměstnanci cítí odpovědní za svá rozhodnutí a za bezpečné zacházení s technologiemi.



**Minimalizace zneužití:** Pravidla pro používání AI omezují riziko, že zaměstnanci AI využijí nelegitimně nebo neeticky.



**NIKDY NEČEKEJTE, ŽE ODSTRANÍTE VŠECHNA RIZIKA! TO NENÍ MOŽNÉ. VŽDY NĚJAKÉ RIZIKO BUDE. KLÍČEM JE RIZIKA MINIMALIZOVAT.**

# 2. Příprava na zavedení AI – klíčové otázky

Při implementaci AI do firemních procesů je důležité věnovat pozornost několika oblastem, které mohou představovat rizika pro bezpečnost a etiku. Zde jsou klíčové otázky, které byste si měli položit:



## Kde AI zpracovává citlivá data?

Zajistěte, že AI nemá přístup k osobním údajům zaměstnanců nebo zákazníků bez správného zabezpečení.



## Jaká rozhodnutí činí AI?

Ujistěte se, že AI nerozhoduje o citlivých záležitostech (např. nábor, propouštění) bez lidského dohledu.



## Používají vaši zaměstnanci AI správně?

Monitorujte, jak AI využívají vaši zaměstnanci, a zaveďte opatření, aby AI nevyužívali k osobním nebo nelegitimním účelům.



## Pravidelná kontrola a aktualizace zásad pro AI

Sledujte aktuální vývoj legislativy i technologie a pravidelně aktualizujte firemní pravidla, aby odpovídala nejnovějším standardům a minimalizovala rizika.



## Jak jsou zaměstnanci školeni na používání AI?

Zajistěte, že zaměstnanci procházejí pravidelným školením ohledně správného a bezpečného používání AI, aby rozuměli rizikům i etickým pravidlům.



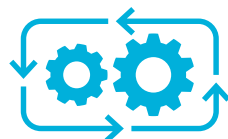
## Jaké nástroje s AI se ve vaší firmě používají?

Udělejte přehled všech nástrojů s AI, které zaměstnanci používají (legitimní i nelegitimní), a zajistěte, že jsou správně nastaveny a bezpečně využívány.



## Jaký přístup mají jednotlivé týmy k AI?

Analyzujte, kdo ve firmě má přístup k AI nástrojům a k jakým účelům je používají. Nastavte jasná pravidla, která oddělují pracovní a osobní použití AI.



## Kontrola výstupů AI

Sledujte výstupy, které AI generuje, aby se předešlo situacím, kdy by AI mohla vytvořit neetický nebo nebezpečný obsah (např. bias v rozhodování, nevhodné návrhy).



## Je AI integrována do firemních procesů správně?

Ověřte, zda jsou AI nástroje implementovány do pracovních procesů způsobem, který odpovídá etickým zásadám a neohrožuje citlivá data.



**Jsou všechna data, která vaše AI zpracovává, dostatečně chráněna?**

# 3. Jak identifikovat rizikové oblasti při používání AI

Jedním z nejdůležitějších kroků při zavádění AI ve firmě je **identifikace rizikových oblastí**.

AI je sice skvělým nástrojem pro automatizaci procesů, analýzu dat nebo zlepšení zákaznické zkušenosti, ale nesprávně nastavená AI může přinést značná rizika – **od porušení bezpečnosti dat po neetické rozhodování**.

Tato kapitola vám ukáže, jak efektivně **identifikovat potenciální rizika spojená s AI**, aby vaše firma mohla tyto problémy včas řešit a předejít tak nežádoucím důsledkům.

## Praktický návod: Jak provést analýzu rizik AI ve firmě

Jedním z nejdůležitějších kroků při zavádění AI ve firmě je **identifikace rizikových oblastí**.

AI je sice skvělým nástrojem pro automatizaci procesů, analýzu dat nebo zlepšení zákaznické zkušenosti, ale nesprávně nastavená AI může přinést značná rizika – **od porušení bezpečnosti dat po neetické rozhodování**.

Tato kapitola vám ukáže, jak efektivně **identifikovat potenciální rizika spojená s AI**, aby vaše firma mohla tyto problémy včas řešit a předejít tak nežádoucím důsledkům.

### 0. Proved'te analýzu rizik před zavedením AI

Pokud se AI ve vaší firmě teprve chystáte zavést, je klíčové už na začátku provést důkladnou analýzu možných rizik. Identifikujte, jaké oblasti by AI ovlivnila, a jaká rizika může její nasazení přinést.

Zvažte:

- Kde bude AI zpracovávat citlivá data nebo rozhodovat o klíčových záležitostech?
- Jaké procesy budou plně automatizované a vyžadují zvláštní pozornost z hlediska etiky a bezpečnosti?
- Jaké bude mít AI přístupy k datům a jaké ochrany budou nutné pro zajištění bezpečnosti?

Provádění této předběžné analýzy vám pomůže předvídat a minimalizovat rizika ještě před samotným nasazením AI.



## 1. Zmapujte, kde a jak se AI již používá

Prvním krokem je pochopit, kde ve vaší firmě již AI pracuje a k jakým účelům se používá.

Proveďte audit všech nástrojů a systémů, které obsahují prvky AI, a odpovězte si na následující otázky:

- Kde je AI implementována v procesech (např. HR, marketing, IT)?
- Které nástroje s AI vaši zaměstnanci používají (interní aplikace, externí software)?

Tímto získáte jasný přehled o tom, kde se AI ve vaší firmě skutečně používá, a kde mohou vzniknout potenciální problémy.

## 2. Identifikujte přístup k datům

Ve firmě se generuje velké množství dat – včetně citlivých osobních údajů nebo obchodních tajemství. Je proto důležité pochopit, jak AI pracuje s daty a zda jsou tato data správně chráněna.

Zeptejte se sami sebe:

- Zpracovává AI citlivá data (osobní údaje zaměstnanců nebo zákazníků)?
- Jsou přístupová práva k těmto datům dostatečně zabezpečena a monitorována?

## 3. Sledujte, jak AI používají vaši zaměstnanci

AI může být zneužita i samotnými zaměstnanci – například využitím neschválených nástrojů nebo sdílením citlivých údajů. Klíčové otázky, které vám pomohou identifikovat toto riziko, jsou:

- Mají vaši zaměstnanci přístup k AI nástrojům, které nejsou oficiálně schválené?
- Existují pravidla a zásady pro používání AI na pracovišti?

Doporučuje se zavést pravidla, která stanoví jasná pravidla použití AI v rámci firmy.

## 4. Zajistěte pravidelnou aktualizaci a kontrolu bezpečnosti

Nástroje s AI se neustále vyvíjejí. Aby byla zajištěna bezpečnost a etika při jejich používání, je nutné pravidelně provádět aktualizace a audity těchto nástrojů.

Odpovězte si na následující otázky:

- Jak často aktualizujete své AI systémy?

Provádíte pravidelné kontroly bezpečnosti a etiky těchto systémů?

## 5. Kontrola výstupů AI

AI systémy mohou produkovat výstupy, které neodpovídají skutečnosti. Důkladná kontrola výstupů AI je klíčová pro zajištění toho, aby se ve firmě využíval obsah, který je nesprávný.

Zeptejte se:

- Jsou výsledky generované AI správné a odpovídají skutečnosti?
- Máte nastavené procesy pro kontrolu a revizi rozhodnutí, které AI činí?

## 6. Školení zaměstnanců

Zajistěte, aby všichni vaši zaměstnanci pravidelně procházeli školením ohledně správného a bezpečného používání AI. To zajistí, že budou rozumět jak rizikům, tak i etickým pravidlům, které jsou při práci s AI nezbytné.

Klíčová otázka:

- Jsou vaši zaměstnanci pravidelně školeni na používání AI?

## 7. Opatření pro snížení rizik

Na základě analýzy rizik je nutné přijmout opatření, která minimalizují možná nebezpečí. Mezi tato opatření patří nastavení přístupových práv, implementace bezpečnostních protokolů, pravidelné audity a revize výstupů AI systémů.

Tímto přístupem můžete zajistit, že **rizika** spojená s používáním AI budou **odhalena včas** a vaše firma se vyhne problémům spojeným s neetickým či nezabezpečeným použitím této technologie. Implementací těchto kroků můžete zaručit, že AI bude sloužit nejen efektivně, ale i bezpečně.



**"Provádějte pravidelné audity datových toků v AI nástrojích, abyste odhalili případné slabiny."**

# 4. Jak správně zavádět AI ve firmě

Úspěšné nasazení AI ve firmě vyžaduje pečlivé plánování, koordinaci a zohlednění etických a bezpečnostních zásad. V této kapitole se zaměříme na konkrétní kroky, které byste měli podniknout při implementaci AI, abyste minimalizovali rizika a maximalizovali přínosy.

## 1

### Stanovte si jasné cíle

Prvním krokem při zavádění AI je definovat, co konkrétně chcete s pomocí AI dosáhnout. Mnoho firem začíná s AI bez jasného záměru, což vede k nejasným očekáváním a možným problémům. Položte si otázky:

- Jaké konkrétní procesy nebo úkoly chcete automatizovat?
- Které oblasti firmy potřebují optimalizaci nebo zrychlení díky AI?
- Jaké problémy nebo nedostatky by AI mohla pomoci vyřešit?

### Identifikujte potřebné nástroje a technologie

Po stanovení cílů je důležité vybrat správné AI nástroje a technologie, které budou vyhovovat potřebám vaší firmy.

Při výběru technologií zvažte:

- Jaké nástroje jsou dostupné na trhu a jaké z nich nejlépe odpovídají vašim cílům?
- Potřebujete vlastní řešení nebo vám postačí standardní nástroje dostupné na trhu?
- Jsou tyto nástroje v souladu s vašimi etickými a bezpečnostními zásadami?

Při výběru AI řešení se nebojte konzultovat s odborníky nebo externími firmami, které se na tuto oblast specializují.

## 2

## 3 Vypracujte plán implementace

Implementace AI není jednorázový krok, ale proces, který vyžaduje pečlivé plánování a přizpůsobení. Vytvořte podrobný plán implementace, který bude zahrnovat následující aspekty:

- **Časový harmonogram:** Stanovte si realistické termíny, kdy a jak bude AI zaváděna do jednotlivých procesů.
- **Zodpovědnosti:** Určete, kdo ve firmě bude za implementaci odpovědný – od IT oddělení až po jednotlivé manažery, kteří budou AI nástroje využívat.

**Zabezpečení:** Zajistěte, že implementované AI systémy jsou řádně zabezpečeny a chráněny před zneužitím nebo kybernetickými útoky.



**Stanovte si realistické termíny pro zavádění AI a vždy zvažte bezpečnostní rizika každé fáze implementace.**

## 4 Školení zaměstnanců

Aby byla AI ve firmě efektivně využívána, je nezbytné zajistit, aby zaměstnanci byli s jejími funkcemi a používáním dobře obeznámeni.

Školení by mělo zahrnovat:

- **Technické aspekty:** Jak používat konkrétní AI nástroje a jak s nimi pracovat ve svých každodenních úkolech.
- **Etické zásady:** Jak používat AI odpovědně a bezpečně, aby nedošlo k neetickým rozhodnutím nebo narušení ochrany dat.
- **Rizika a zneužití:** Jak identifikovat možné nebezpečí a co dělat v případě, že AI nefunguje tak, jak by měla.

## 5 Monitorování a hodnocení výsledků

Implementace AI není nikdy hotová – po jejím zavedení je nutné neustále monitorovat její výkon, sledovat výsledky a přizpůsobovat ji novým výzvám.

Pravidelně analyzujte:

- **Výkonnost AI:** Dosahuje AI očekávaných výsledků a naplňuje vaše cíle? Kde jsou potenciální problémy nebo nedostatky?
- **Bezpečnostní aspekty:** Jsou všechna data zpracovávána bezpečně a v souladu s předpisy? Je AI chráněna proti útokům nebo zneužití?
- **Etika a transparentnost:** Je AI využívána eticky a bez diskriminace? Jsou rozhodnutí AI transparentní a spravedlivá?

# 6

## Aktualizace a údržba AI systémů

Technologie AI se neustále vyvíjí, a proto je důležité zajistit, že AI nástroje budou pravidelně aktualizovány a optimalizovány.

Zvažte:

- **Pravidelné upgrady:** Sledujte nové verze AI softwaru a technologií, které mohou zvýšit efektivitu a bezpečnost.
- **Audit a kontrola:** Pravidelně provádějte audity AI systémů, abyste zajistili jejich správnou funkci a dodržování etických standardů.
- **Zpětná vazba od zaměstnanců:** Získejte od zaměstnanců zpětnou vazbu o používání AI – kde vidí problémy, co funguje a co by mohlo být vylepšeno.



*AI není jednorázová investice. Je to dlouhodobý proces, který vyžaduje pravidelnou kontrolu a údržbu.*

## SWOT analýza zavádění AI

Před implementací umělé inteligence (AI) je zásadní zhodnotit klíčové faktory, které mohou ovlivnit úspěch jejího zavádění.

Tato SWOT analýza vám pomůže rychle porozumět **silným a slabým stránkám, příležitostem a hrozbám** spojeným s AI ve firemním prostředí.

Manažeři a lídři díky tomu získají přehled o tom, jak využít AI pro zlepšení procesů, konkurenční výhodu a optimalizaci rozhodování, zatímco budou moci efektivně čelit případným rizikům a výzvám.

# S

## (Strengths) – Silné stránky

- **Automatizace a efektivita:** AI může zrychlit rutinní úkoly, zefektivnit pracovní procesy a snížit náklady na lidské zdroje.
- **Zlepšení zákaznické zkušenosti:** Personalizace a rychlejší odpovědi vedou ke zvýšení spokojenosti zákazníků.
- **Konkurenční výhoda:** Firmy využívající AI získávají náskok díky lepším datovým analýzám a rychlejšímu rozhodování.
- **Lepší datová analýza:** AI poskytuje firmám hlubší pohled do dat, což podporuje přesnější predikce a strategické plánování.

# W

## (Weaknesses) – Slabé stránky

- **Náklady a investice:** Implementace AI vyžaduje počáteční vysoké investice do infrastruktury, softwaru a školení zaměstnanců.
- **Komplexita integrace:** AI může být obtížně integrována do stávajících procesů, zvláště pokud firma nemá dostatečné IT zázemí.
- **Chybějící dovednosti:** Nedostatek kvalifikovaných odborníků na AI a data science může bránit efektivnímu zavádění AI.
- **Riziko 'AI bias':** Modely mohou být zatíženy zaujatostí (bias), což může ovlivnit rozhodování a poškodit reputaci firmy.

# SWOT

# O

## (Opportunities) – Příležitosti

- **Inovace a rozvoj nových produktů:** AI umožňuje vývoj personalizovaných a inovativních produktů, které mohou firmu odlišit na trhu.
- **Optimalizace operací:** Díky prediktivní údržbě a optimalizaci zásob může AI výrazně snížit provozní náklady.
- **Expanze do nových trhů:** AI může pomoci identifikovat nové tržní příležitosti a přizpůsobit služby různým geografickým oblastem.
- **Partnerská spolupráce:** Firmy mohou využívat externí poskytovatele AI technologií a získat přístup ke špičkovým řešením bez nutnosti interního vývoje.

# T

## (Threats) – Hrozby

- **Riziko narušení soukromí a úniků dat:** Práce s AI může vést k únikům citlivých dat, což může mít právní a reputační následky.
- **Změna právního prostředí:** Rychle se vyvíjející regulace AI a ochrany osobních údajů mohou vyžadovat časté úpravy a dodatečné náklady.
- **Odpor zaměstnanců k implementaci AI:** Zaměstnanci mohou mít obavy z AI kvůli strachu o ztrátu práce, což může snížit efektivitu jejího zavádění.
- **Nedostatek datové infrastruktury:** Chybějící nebo neadekvátní datová infrastruktura může zavádění AI ve firmě značně zpomalit.

## Doporučení na základě SWOT analýzy



**1. Maximalizovat silné stránky** zaváděním automatizace v rutinních činnostech a zlepšováním zákaznické zkušenosti.



**2. Zaměřit se na školení a nábor odborníků** v oblasti datové vědy, aby firma mohla plně využít potenciál AI.



**3. Využít příležitosti pro partnerskou spolupráci** s externími poskytovateli, kteří mohou nabídnout technologie a know-how, které firma nemá interně.



**4. Omezit hrozby zavedením přísných pravidel** pro práci s daty a zajištěním souladu s právními normami.

# 5. Jak měřit úspěch a efektivitu AI ve firmě

Zavedení AI ve firmě je jen prvním krokem. Aby AI přinášela dlouhodobou hodnotu, je důležité neustále sledovat její výkon a měřit její přínos pro firmu. V této kapitole se zaměříme na praktické způsoby, jak hodnotit efektivitu AI systémů, jak identifikovat oblasti pro zlepšení a jaké metriky a nástroje použít pro měření úspěchu.



## 1. Stanovte si klíčové metriky úspěchu (KPI)

Aby bylo možné měřit úspěch AI, je nezbytné definovat konkrétní metriky a ukazatele, které budou sledovat výkonnost AI systémů. Tyto ukazatele (KPI) by měly být jasně propojeny s cíli, které jste si stanovili před zavedením AI.

Mezi nejčastější KPI pro AI patří:

- **Zvýšení produktivity:** Jak AI zefektivnila pracovní procesy? Došlo ke snížení času potřebného na rutinní úkoly?
- **Zlepšení kvality rozhodování:** Produkuje AI lepší a přesnější výsledky než lidský zásah?
- **Snížení nákladů:** Jaké jsou úspory, které AI přináší, například ve formě nižších provozních nákladů nebo nákladů na zaměstnance?
- **Spokojenost zákazníků:** Jak AI přispěla ke zlepšení zákaznické zkušenosti nebo snížení počtu stížností?



## 2. Pravidelné hodnocení ROI (návrtnosti investic)

Implementace AI představuje významnou investici, proto je důležité pravidelně sledovat, jaký má tato technologie dopad na firmu z hlediska návratnosti investic (ROI).

Zvažte následující:

- Jaké byly počáteční náklady na implementaci AI (licence, školení, vývoj)?
- Jaké úspory AI přinesla ve střednědobém a dlouhodobém horizontu (např. zkrácení času, snížení nákladů na lidské zdroje)?
- Jaký je finanční přínos zvýšené efektivity nebo kvality rozhodování díky AI?





### 3. Monitorování výkonnosti AI v reálném čase

AI systémy potřebují neustálý dohled, aby bylo zajištěno, že pracují efektivně a bez problémů. Nastavte monitorovací mechanismy, které budou sledovat klíčové aspekty výkonnosti AI v reálném čase, včetně:

- **Rychlost zpracování dat:** Je AI schopná plnit úkoly v rámci požadovaného času?
- **Kvalita výstupů:** Jsou výsledky, které AI generuje, bez chyb a v souladu s očekávanými?
- **Chybovost a incidenty:** Jak často dochází k výpadkům nebo chybám v AI systému?



### 4. Pravidelné audity a kontroly

Provádějte pravidelné audity AI systémů, abyste ověřili, že nadále splňují své cíle a fungují v souladu s etickými a bezpečnostními zásadami.

Během auditu se zaměřte na:

- **Dodržování etických pravidel:** Je AI stále transparentní, spravedlivá a bezpečná?
- **Bezpečnost dat:** Jsou data, se kterými AI pracuje, stále chráněna před úniky a neoprávněným přístupem?
- **Přesnost a zaujatost:** Produkuje AI nestranné a přesné výsledky, nebo se objevily nové formy zaujatosti (bias)?



### 5. Získávání zpětné vazby od zaměstnanců a zákazníků

Úspěch AI není jen o technologiích – je také důležité, aby AI fungovala dobře pro ty, kteří ji používají. Získejte pravidelně zpětnou vazbu od zaměstnanců a zákazníků, kteří s AI přicházejí do kontaktu, abyste pochopili její silné a slabé stránky:

- **Od zaměstnanců:** Jak se jim pracuje s AI? Cítí se pohodlně s jejími funkcemi? Jaké jsou jejich připomínky nebo návrhy na zlepšení?
- **Od zákazníků:** Zlepšila se zákaznická zkušenost díky AI? Jsou spokojeni s personalizovanými doporučeními nebo rychlostí obsluhy?



### 6. Optimalizace AI systémů na základě výsledků

Na základě zpětné vazby a shromážděných dat je nezbytné průběžně optimalizovat AI systémy, aby nadále přinášely maximální hodnotu. Přizpůsobte algoritmy a procesy AI podle měnících se potřeb firmy a technologických možností:

- **Upravení algoritmů:** Pokud AI přestává dosahovat požadovaných výsledků, zvažte úpravu nebo přeškolení algoritmů.
- **Rozšíření funkcí:** Jakmile AI osvědčí svůj přínos v jedné oblasti, zvažte rozšíření jejího využití do dalších částí firmy.
- **Zavádění nových technologií:** Průběžně sledujte nové AI technologie a nástroje, které by mohly zlepšit výkon vašich současných systémů.

# 6. Vytvoření interní AI politiky – praktický návod pro firmy

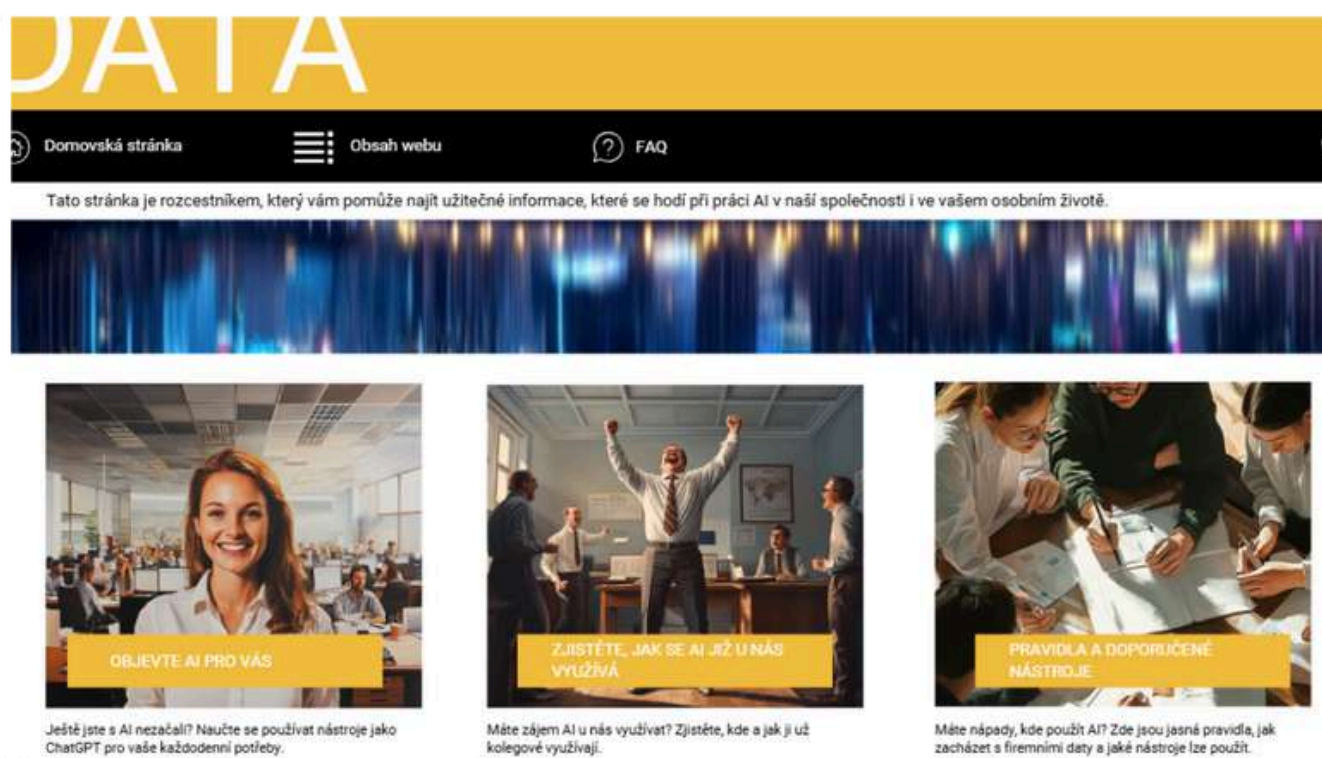
Implementace AI do firemních procesů přináší nejen příležitosti, ale i rizika, pokud nejsou nastavena jasná pravidla a postupy. Interní AI politika pomáhá zaměstnancům pochopit, jak AI využívat bezpečně, efektivně a v souladu s firemními hodnotami. Tato kapitola vám poskytne konkrétní kroky, jak takovou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



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

# 7. Akční plán pro řešení úniku dat nebo nesprávného použití AI

I při důkladné implementaci AI pravidel může dojít k situacím, kdy nástroje nesprávně zpracují citlivá data nebo dojde k jejich úniku. Tento akční plán vám pomůže rychle a efektivně reagovat, minimalizovat dopady a zlepšit pravidla pro budoucí používání AI.



## Omezení přístupu k AI nástroji s následnou analýzou

Namísto okamžitého zakázání AI nástroje je důležité omezení přístupu k nástroji, abyste rychle zajistili kontrolu nad situací. Omezení přístupu může zahrnovat:

- **Dočasné snížení úrovně přístupu k AI nástroji pouze pro relevantní týmy** (IT, bezpečnostní tým, AI Navigátoři).
- **Zamezení přístupu k citlivým datům, ale ponechání přístupu ke zbytkovým funkcím, dokud nebude provedena analýza.**

Tímto způsobem firma minimalizuje dopad incidentu, aniž by nutně úplně zastavila provoz AI nástroje. Analýza se může začít okamžitě, aniž by došlo k vážnému narušení firemních procesů.



## Okamžitá analýza rozsahu problému

Jakmile je přístup omezen, následuje rychlá analýza toho, co se stalo. Tento krok by měl být prováděn okamžitě a prioritně, a to následujícím postupem:

- **Identifikace dotčených dat:** Rychle zjistěte, která data byla zasažena (např. citlivé osobní údaje, firemní know-how). Je důležité, aby analytici věděli, jaká data AI systém zpracovával během incidentu.
- **Hodnocení závažnosti:** Zjistěte, zda se jedná o únik, špatné použití dat, nebo jiný typ incidentu (např. chybné rozhodnutí AI, přístup k nesprávným datům).
- **Interní hlášení:** Proveďte okamžité hlášení odpovědným týmům (IT, bezpečnost, právní oddělení), kteří provedou forenzní analýzu incidentu.

Tip pro praxi: Mějte připravené nástroje pro automatické monitorování AI nástrojů (např. sledování datových přístupů), které mohou okamžitě upozornit na podezřelé aktivity.



## Úprava pravidel pro dočasné používání AI nástroje

V průběhu analýzy můžete upravit pravidla pro používání AI nástroje, aby byl provoz co nejméně narušen. Například:

- **Omezte přístup k citlivým datům** (Stupeň 3–5) a dovolte pouze zpracování méně citlivých dat (Stupeň 1–2), dokud není zcela jasné, co se stalo.
- **Přehod'te některé úkoly na lidské operátory, pokud AI nástroj aktuálně nemůže zpracovávat konkrétní datové sady správně.**

Tím zajistíte, že práce nepřestane, ale rizika budou minimalizována.

## Kontaktování a informování zainteresovaných stran



V případě incidentu je důležité rychle informovat všechny dotčené strany. Tento krok zahrnuje:

- **Interní komunikaci:** Informujte všechny relevantní týmy, zejména ty, které zpracovávají dotčená data. Zároveň zajistěte, aby si ostatní zaměstnanci byli vědomi nových pravidel pro používání AI do doby, než bude incident zcela vyřešen.
- **Externí komunikaci:** Pokud došlo k úniku osobních nebo citlivých dat zákazníků, okamžitě informujte dotčené osoby o tom, jaká data byla zasažena, co firma dělá pro řešení situace a jaká preventivní opatření budou zavedena.

Tip pro praxi: Vypracujte předem připravený šablonový e-mail pro okamžité informování zákazníků, který bude přizpůsobitelný podle typu incidentu.

## Forenzní analýza a zjištění příčiny



V průběhu omezeného provozu AI nástroje probíhá forenzní analýza zaměřená na:

- **Příčinu incidentu:** Byl problém způsoben lidskou chybou (např. nesprávně nastavená přístupová práva), technickou chybou, nebo dokonce záměrným zneužitím?
- **Detailní sledování pohybu dat:** Která data byla skutečně zpracována, kde se nacházela a jak byla chráněna během incidentu?

Výstupy forenzní analýzy budou klíčové pro následná nápravná opatření.

## Úprava AI nástroje a pravidel pro budoucí používání



Na základě forenzní analýzy je třeba provést okamžité úpravy AI systému a interních pravidel. Mezi klíčová opatření patří:

- **Zpřesnění přístupových práv:** Jasně definujte, kdo smí přistupovat k jakým úrovním dat v AI nástroji, a nastavte pevné limity pro automatizovaný přístup.
- **Upravení algoritmů nebo parametrů AI:** Pokud incident souvisí s chybou v rozhodování AI, upravte parametry, aby se tato chyba neopakovala.
- **Doplnění o další bezpečnostní opatření:** Například zavedení dvoufaktorové autentizace pro přístup k vysoce citlivým datům nebo vylepšení šifrování pro všechna data zpracovávaná AI nástroji.

## Zpětná vazba a proškolení zaměstnanců



Po vyřešení incidentu je nezbytné vrátit se k zaměstnancům a zajistit, že si jsou vědomi nových pravidel a změn v používání AI. Proškolení je ohledně:

- Nových opatření, která byla zavedena, aby se incident neopakoval.
- Správného třídění citlivosti dat a vhodného používání AI nástrojů.
- Postupů pro informování AI Navigátorů při podezření na problém.

Zpětná vazba zaměstnanců na nové postupy vám také pomůže odhalit případné mezery v pravidlech.

## Zavedení monitorovacích mechanismů a revize politiky



Na základě analýzy a nových poznatků je nutné vylepšit pravidla a procesy pro používání AI. Mezi klíčové úpravy může patřit:

- **Pravidelná kontrola a audit AI nástrojů:** Nastavte monitoring, který upozorní na podezřelé aktivity nebo potenciální problémy dříve, než dojde k incidentu.
- **Revize AI politiky:** Aktualizujte pravidla pro práci s citlivými daty, upravte směrnice pro sdílení dat a zajistěte, že všechna nová pravidla jsou dostupná a srozumitelná pro zaměstnance.



**Z incidentů, jako byl únik dat u Samsungu (viz příloha), se učíme, že jasná pravidla pro používání AI musí být jasně definována, správně komunikována na zaměstnance a pravidelně aktualizována**



# 8. Průběžný rozvoj a optimalizace AI ve firmě

Nasazení AI je pouze začátek. Aby firma mohla plně využít potenciál této technologie, musí neustále pracovat na jejím rozvoji, přizpůsobování a vylepšování. V této kapitole vám ukážeme, jak zajistit, že AI bude ve vaší firmě vždy aktuální, bezpečná a přizpůsobená vašim rostoucím potřebám.

## 1. Pravidelná aktualizace AI technologií

Technologie AI se neustále vyvíjejí a nové nástroje a funkce přicházejí na trh. Aby vaše firma nezůstala pozadu, je důležité pravidelně sledovat nové trendy a technologie, které by mohly zlepšit současné AI systémy.

Mezi hlavní kroky patří:

- **Monitoring trhu:** Sledujte nové AI nástroje, platformy a inovace, které by mohly zvýšit efektivitu nebo bezpečnost vašich systémů.
- **Testování a pilotní projekty:** Pravidelně vyzkoušejte nové AI technologie na malém vzorku dat nebo procesů, abyste zjistili, zda mají potenciál pro širší nasazení.
- **Plánované upgrady a migrace:** Zajistěte, aby váš tým měl plán na pravidelné aktualizace AI nástrojů a systémů, které jsou ve firmě již implementovány.

## 2. Rozšiřování využití AI

Jakmile AI technologie osvědčí své přínosy v jedné oblasti, může být vhodné rozšířit její použití do dalších částí firmy.

Zvažte:

- **Kde jinde může AI zvýšit efektivitu?** Pokud například AI úspěšně optimalizovala marketingové procesy, může být nasazena i v oblasti HR, financí nebo logistiky.
- **Personalizace procesů:** AI může pomoci při personalizaci interních i zákaznických procesů – od přizpůsobení produktů zákazníkům až po individualizaci školení zaměstnanců.
- **Automatizace rutinních úkolů:** Po implementaci základních AI procesů můžete zkoumat další oblasti, kde lze ušetřit čas a zdroje automatizací každodenních úkolů.

### 3. Adaptace na nové legislativní požadavky

AI technologie jsou stále více pod dohledem regulatorních orgánů a právních předpisů. Je důležité sledovat změny v legislativě, aby firma zůstala v souladu s právními předpisy týkajícími se ochrany osobních údajů, etiky AI a bezpečnosti dat.

Doporučujeme:

- **Pravidelná kontrola legislativy:** Sledujte nové právní předpisy týkající se AI a ochrany dat (např. GDPR, evropská regulace AI), abyste zajistili, že vaše AI systémy jsou stále v souladu s požadavky.
- **Právní poradenství:** Pracujte s právníky nebo experty na ochranu osobních údajů, kteří vám pomohou pochopit a implementovat změny v legislativě do vašich AI politik.

### 4. Měření dlouhodobé efektivity AI

Pravidelné hodnocení a revize výkonu AI je klíčové pro zajištění dlouhodobých přínosů.

Zvažte následující kroky pro optimalizaci efektivity AI:

- **Opakované měření klíčových metrik:** Pravidelně revidujte klíčové ukazatele výkonnosti (KPI), abyste viděli, jak se zlepšuje produktivita, snižují náklady nebo zlepšuje spokojenost zákazníků.
- **Zpětná vazba od zaměstnanců:** Zajistěte, že zaměstnanci, kteří AI používají, poskytují pravidelně zpětnou vazbu, která vám pomůže přizpůsobit AI jejich potřebám a vylepšit její funkce.

### 5. Vytvoření AI strategie na 3–5 let

Aby AI skutečně přinesla dlouhodobou hodnotu, je nutné mít jasně definovanou strategii rozvoje na několik let dopředu.

Doporučujeme:

- **Definování dlouhodobých cílů:** Stanovte si cíle, kterých chcete v horizontu 3–5 let dosáhnout s pomocí AI. Například zvýšení automatizace, zlepšení zákaznické zkušenosti nebo snížení provozních nákladů.
- **Pravidelné revize a úpravy strategie:** Plánujte revizi AI strategie alespoň jednou ročně, abyste zajistili, že zůstává v souladu s novými trendy, technologiemi a potřebami firmy.



**Rozvoj AI vyžaduje nejen technologické inovace, ale i přizpůsobení firemních procesů.**

## 4. Přílohy

1. Vzorová směrnice
2. Konkrétní příklady, kde AI selhala
3. Související dokumenty
4. Doporučené odkazy
5. Zajímavé údaje o Česku
6. Naše Etické desatero na vaši nástěnku
7. Index připravenosti na umělou inteligenci

# PŘÍLOHA 1:

## 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.
- **Zaměstnanci:** 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**

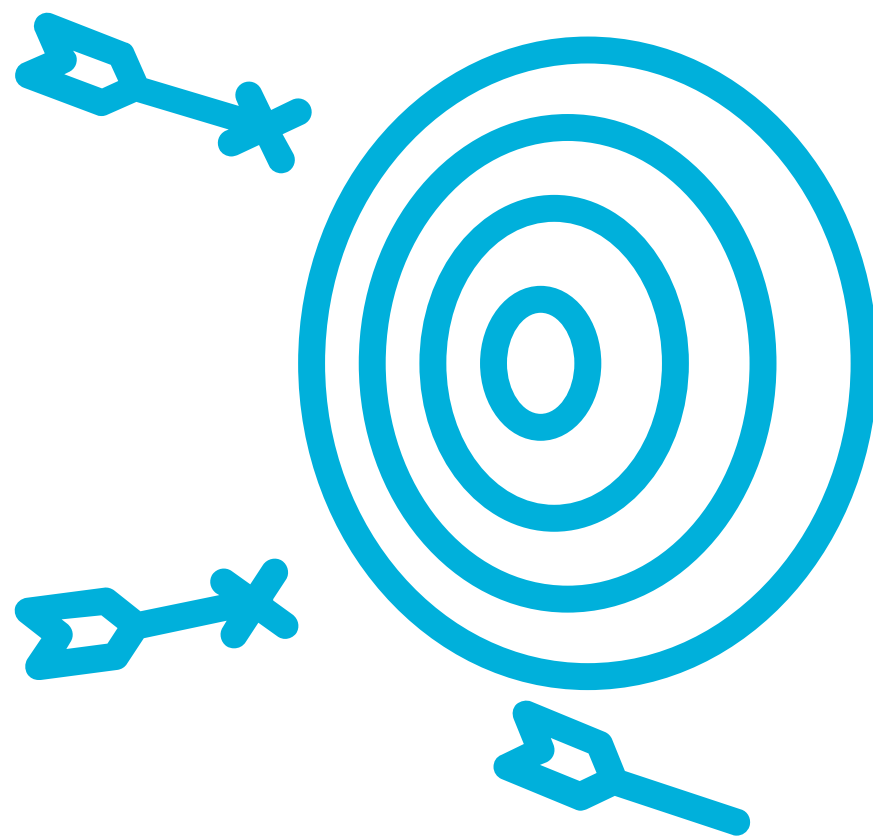
Všichni zaměstnanci „FIRMĚ“ jsou povinni tuto směrnici dodržovat. Porušení pravidel může vést k disciplinárním opatřením. Pravidla používání AI jsou nezbytná pro zajištění bezpečnosti, etiky a efektivity naší firmy.

Datum platnosti:

# PŘÍLOHA 2:

## Konkrétní příklady, kde AI selhala

Případ	Co se stalo	Jak to ovlivnilo firmu	Odkaz na článek	Zjištění
<b>Amazon – náborový software</b>	AI diskriminovala ženy na základě historických dat, která preferovala muže.	Stahování náborového softwaru, poškození pověsti a interní vyšetřování.	Reuters	Firmy by měly pravidelně revidovat data a algoritmy, které AI používají, aby se předešlo diskriminačním výsledkům. Transparentnost v používání AI je zásadní, aby byly jasně stanoveny zodpovědnosti za případná selhání.
<b>iTutorGroup – náborový software</b>	AI automaticky diskriminovala kandidáty na základě jejich věku, čímž porušila zákony o diskriminaci v zaměstnání.	Kolektivní žaloba zaměstnanců v USA, ohrožení reputace společnosti, právní důsledky.	The U.S. Equal Employment Opportunity Commission (EEOC)	
<b>Deepfake útok na firmu v Hongkongu</b>	Útočníci použili deepfake technologie k vytvoření realistických nahrávek hlasu vedoucího pracovníka firmy, čímž oklamali zaměstnance a přesvědčili je k neautorizovaným převodům.	Ztráta ca 25 milionů dolarů kvůli finančnímu převodu na základě deepfake útoku, což vedlo k také ke ztrátě důvěry investorů.	CNN	Je třeba zavést důkladné ověřovací mechanismy a školit zaměstnance, jak rozpoznat a reagovat na možné deepfake útoky. Ochrana citlivých firemních informací vyžaduje nejen technologická opatření, ale i zvyšování povědomí mezi zaměstnanci.
<b>Právníci použili výstupy ChatGPT v soudní argumentaci</b>	Dva právníci předložili soudu argumenty založené na smyšlených citacích vytvořených ChatGPT, aniž by ověřili jejich pravdivost.	Ztráta důvěry v právníky, vyšetřování, možné disciplinární opatření vůči právníkům.	CBS News	AI by měla být považována za podpůrný nástroj, ale nikdy za hlavní zdroj rozhodování v oblastech, kde mohou chybné informace způsobit vážné následky. Firmy by měly zajistit, aby zaměstnanci byli školeni, jak správně interpretovat AI výsledky a jak je ověřovat.
<b>Samsung – únik dat přes konverzační AI</b>	Zaměstnanci Samsungu nahráli citlivé informace do veřejného nástroje ChatGPT, což vedlo k úniku firemních dat.	Následkem toho společnost omezila používání AI nástrojů a zahájila interní vyšetřování. Tento incident odhalil závažné problémy v ochraně dat.	Forbes	Firmy musí zavést jasná pravidla pro používání AI, zejména veřejných nástrojů. Zaměstnanci by měli být proškoleni v tom, jak zacházet s citlivými informacemi a jaké nástroje jsou bezpečné pro jejich zpracování.



*Co myslíte?  
Jednalo se vážně  
vždy o selhání AI?*

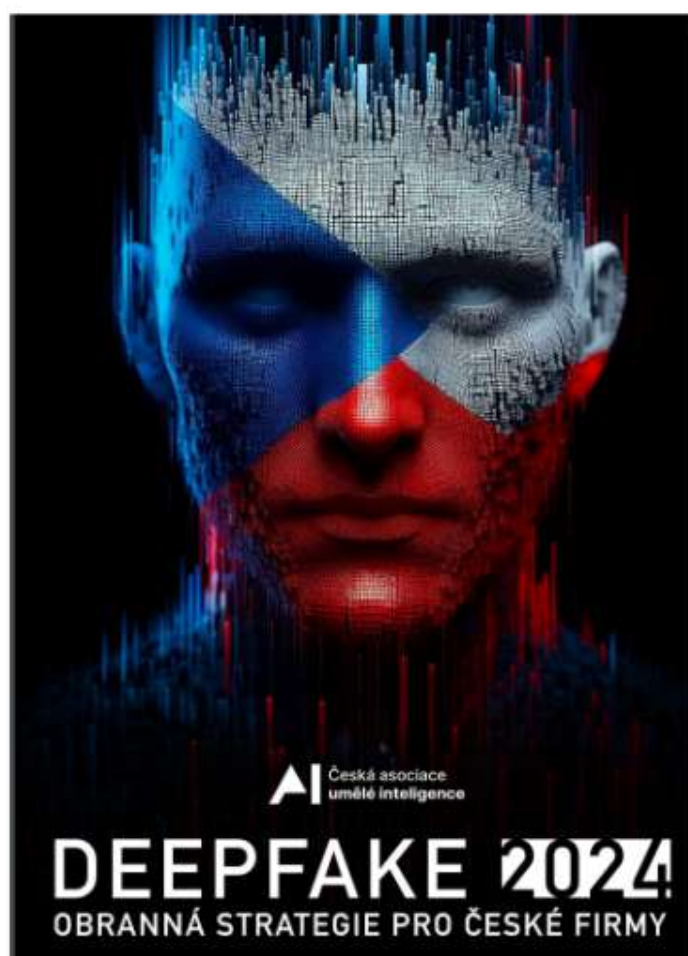
---



# PŘÍLOHA 3: Související dokumenty

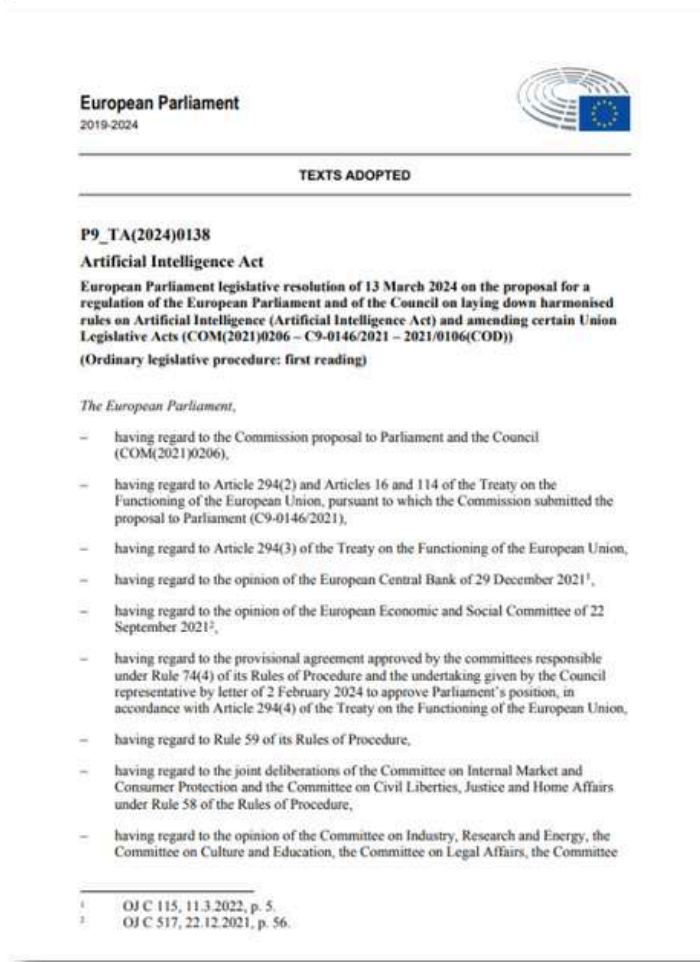
## Deepfake manual od CAUI

Odkaz na dokument [zde](#).



# AI Act

Odkaz na dokument [zde](#).



# Národní strategii umělé inteligence ČR

Odkaz na dokument [zde](#).



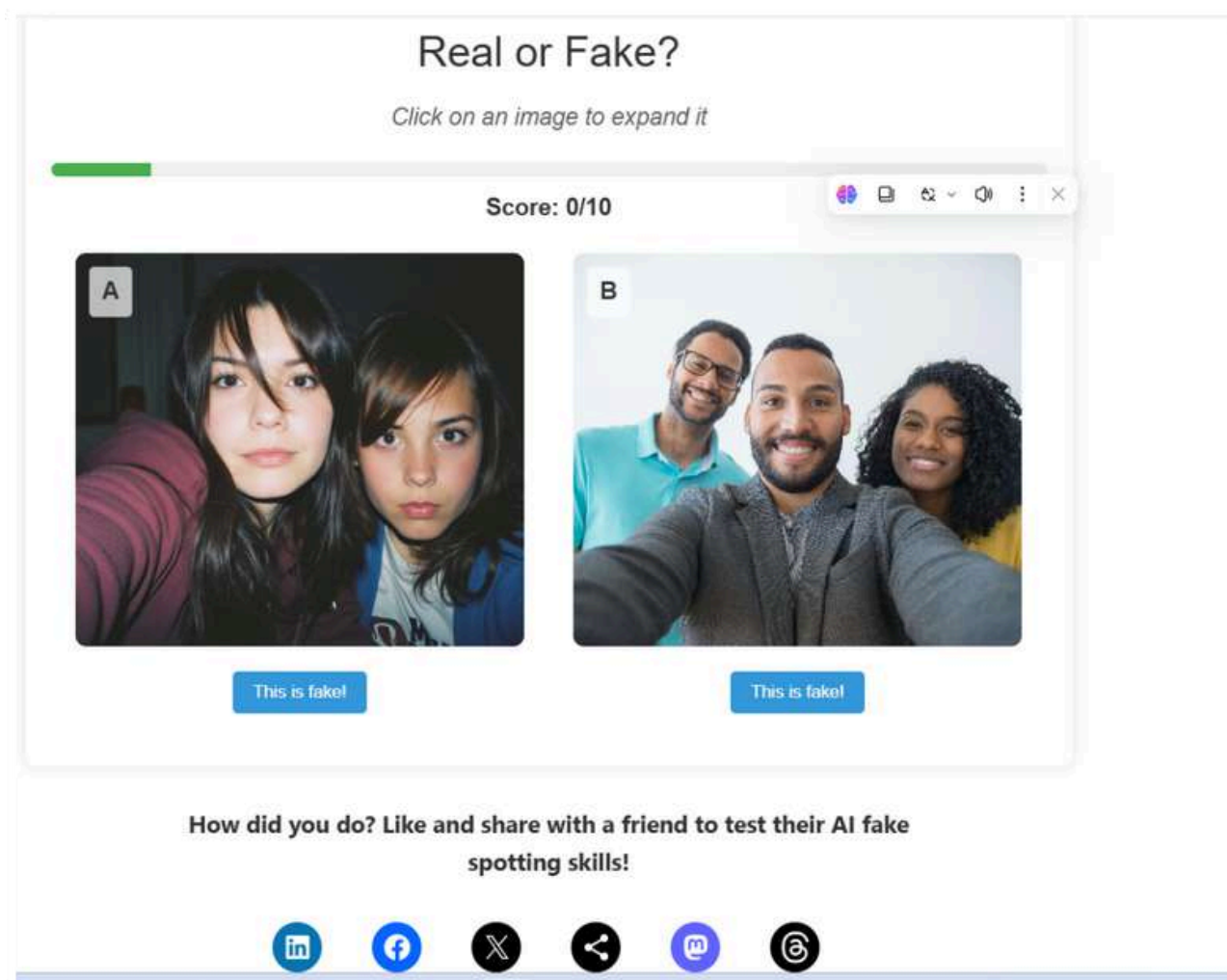
# PŘÍLOHA 4:

## Doporučené odkazy

Vyzkoušejte, jak si stojíte v rozpoznávání Deepfake

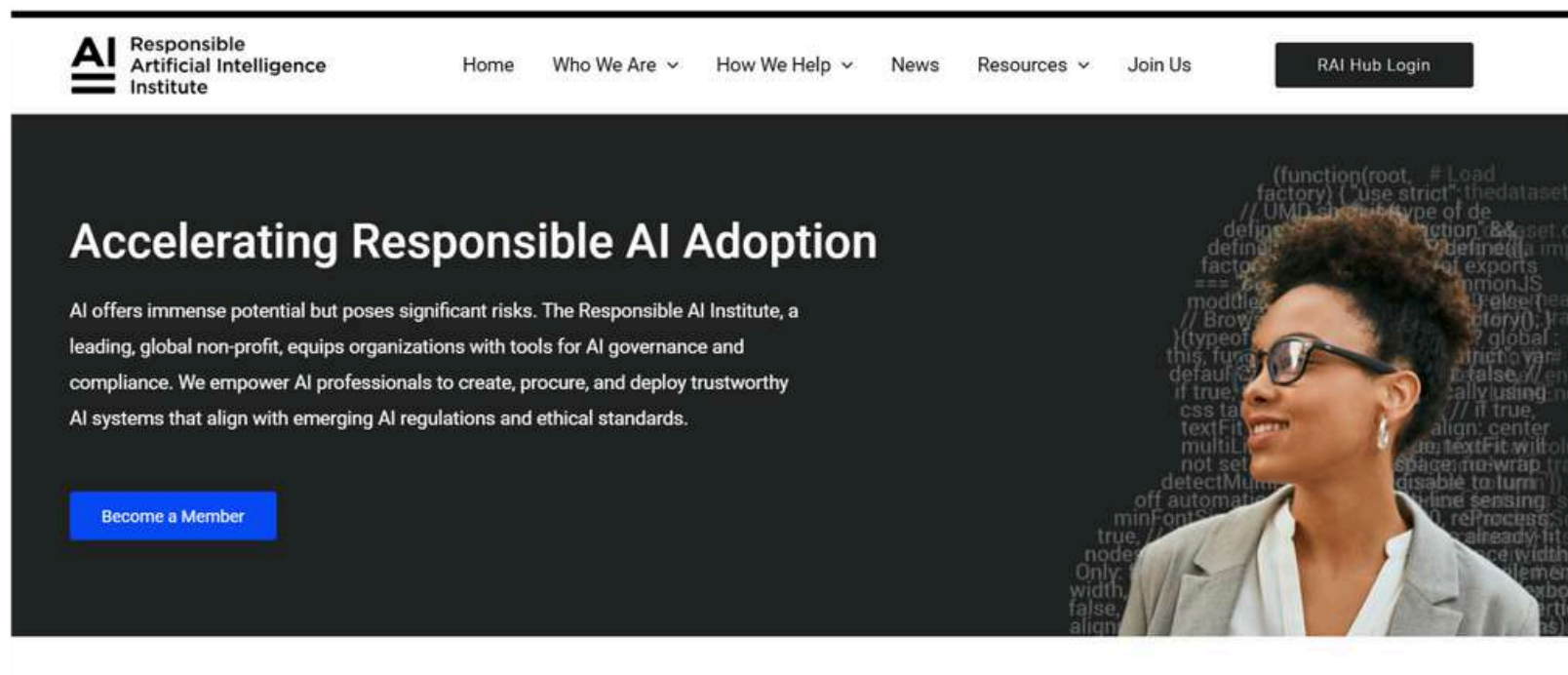
### Skutečné nebo falešné? Hra AI Deepfake

Rozpoznávání falešných obrázků a videí je čím dál těžší, zkuste svůj postřeh v této hře

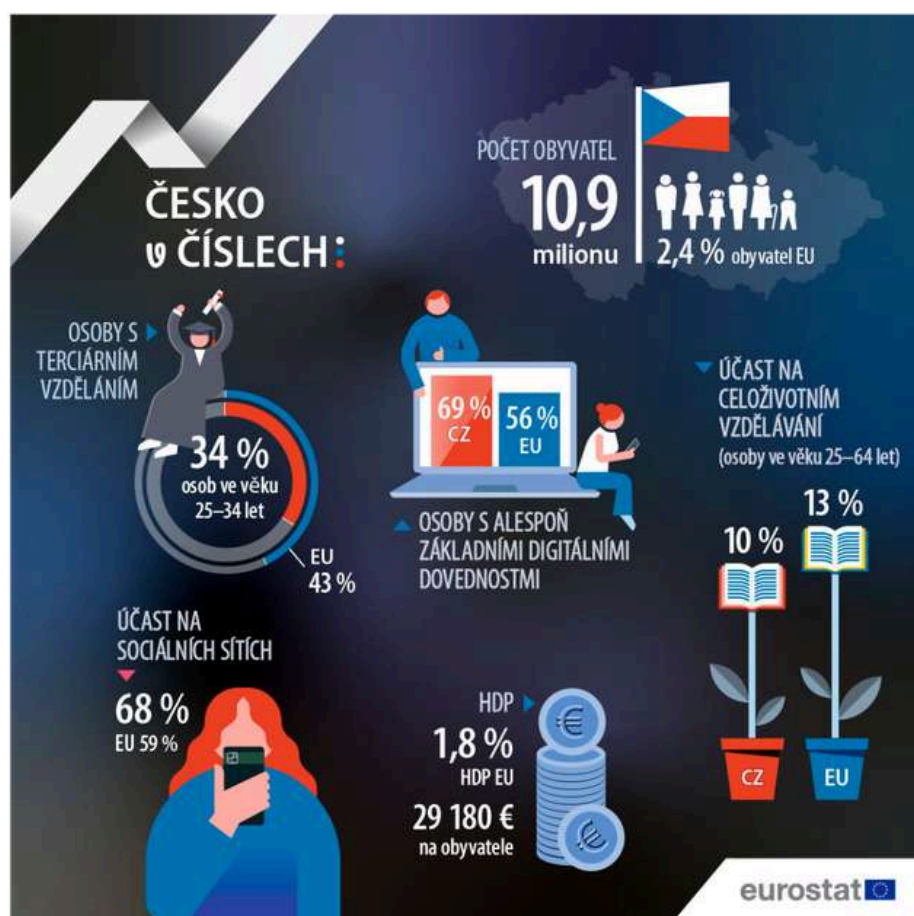


# Responsible Artificial Intelligence

Odkaz [zde.](#)



# PŘÍLOHA 5: Zajímavé údaje o Česku



**ČESKÝ  
STATISTICKÝ  
ÚŘAD**

Podniky s přístupem na internet celkem

Rok 2024

97 %

Datum zveřejnění: 30. 10. 2024

Podniky s přístupem na internet přes mobilní síť

Rok 2024

84 %

Datum zveřejnění: 30. 10. 2024

Zaměstnanci podniků, kteří mají v práci přístup na internet

Rok 2024

56 %

Datum zveřejnění: 30. 10. 2024

Zaměstnanci podniků, kteří mají v práci přístup na mobilní internet z přenosného zařízení

Rok 2024

35 %

Datum zveřejnění: 30. 10. 2024

Podniky s webovými stránkami

Rok 2024

84 %

Datum zveřejnění: 30. 10. 2024

Podniky, které prodávaly přes webové stránky, mobilní aplikace nebo online tržiště

Rok 2023

20 %

Datum zveřejnění: 30. 10. 2024

Podniky s účtem na sociálních médiích

Rok 2024

54 %

Datum zveřejnění: 30. 10. 2024

Podniky používající technologie umělé inteligence

Rok 2024

11 %

Datum zveřejnění: 30. 10. 2024

**PŘÍLOHA 6:**  
**Naše Etické desatero**  
**na vaši nástěnce**





# ETICKÉ DESATERO PRÁCE S AI NÁSTROJI

# 1



## Nepodporujte nezákonné aktivity

Nikdy **nepoužívejte AI** k podpoře, plánování nebo uskutečňování **nezákonných či nemorálních činností**.

# 6



## Nepoužívejte AI k šíření nenávistných a diskriminačních projevů

AI **nesmí být využívána** k vytváření nebo šíření obsahu, který podněcuje **nenávisť, diskriminaci** nebo polarizaci společnosti.

# 2



## Respektujte soukromí

Nikdy **nevkládejte do AI** modelů žádné **citlivé informace** o sobě, jiných osobách nebo firmách bez jejich výslovného souhlasu, aby byla zajištěna ochrana osobních údajů a dodržování předpisů, jako je GDPR.

# 7



## Dodržujte pravidla používání ve vztahu k dětem

Některé AI aplikace mají pro děti věková omezení a tato pravidla by měla být respektována. Smysluplné a bezpečné využití AI však má smysl podporovat se **správným vedením** i u mladších **dětí**.

# 3



## Ověřujte informace

Před sdílením informací od AI si **ověřte** jejich **správnost a zdroje**, z nichž čerpá, zejména pokud se jedná o fakta, data nebo čísla.

# 8



## Používejte AI hlavně jako inspiraci

AI je skvělým nástrojem pro vytváření návrhů, struktury nápadů a inspirace, ale je důležité, aby byl **vždy doplněn lidský prvek**.

# 4



## Omezte šíření dezinformací

**Zamezte** tomu, abyste se nevědomky stali **šířitelem nepravdivých** nebo **zavádějících informací** tím, že budete pečlivě ověřovat informace generované AI.

# 9



## Odpovědné sdílení

Sdílejte výsledky vytvářené AI zodpovědně a **vždy** jasně **uvádějte, že** byly **vytvořeny umělou inteligencí**.

# 5



## Dodržujte autorská práva

Výstupy AI mohou zasahovat do autorských práv a práv duševního vlastnictví. **Ne vždy máte plná autorská práva** k vytvořenému **obsahu**.

# 10



## Vzdělávejte sebe a druhé

Sledujte vývoj v oblasti AI a **sdílejte své znalosti s ostatními**, aby se zvýšila úroveň povědomí a znalostí.

# PŘÍLOHA 7:

## Index připravenosti na umělou inteligenci

### AIRI – Index připravenosti na umělou inteligenci

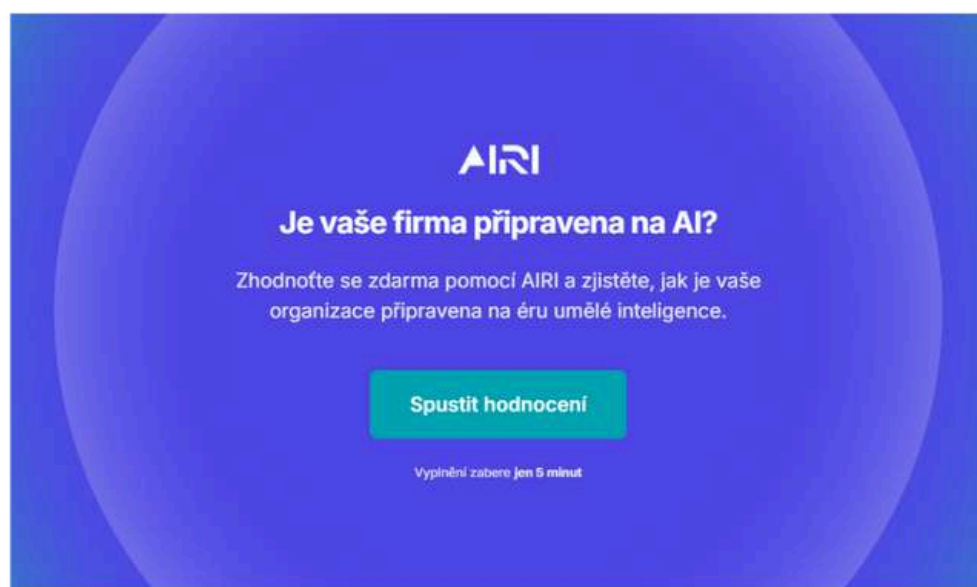
V České republice se stále více firem zajímá o zavádění umělé inteligence do svých procesů. Tento krok však často naráží na otázky, **jak připravená je daná organizace na efektivní a bezpečné používání AI.** Jedním z užitečných nástrojů, který může manažerům a lídrům pomoci zhodnotit tuto připravenost, je **Index připravenosti na AI (AIRI).**

AIRI je **hodnotící systém**, který umožňuje firmám získat komplexní pohled na jejich schopnosti a **připravenost pro implementaci AI.**

Index posuzuje klíčové aspekty jako datovou infrastrukturu, technické dovednosti, etiku a bezpečnost, čímž firmám poskytuje nejen hodnocení aktuální úrovně, ale i jasnou představu o oblastech, které je třeba zlepšit. Tento přístup pomáhá organizacím zjistit, zda jsou dostatečně připraveny na AI a kde by mohly efektivněji využít zdroje k posílení své konkurenceschopnosti.

Pro zájemce z řad firem je hodnocení prostřednictvím **AIRI dostupné zdarma**, což představuje ideální příležitost získat cenný vhled do připravenosti organizace na AI. Podrobnosti o systému AIRI a možnostech hodnocení naleznete na [oficiálních stránkách AIRI](#).

Použití tohoto indexu může být klíčovým krokem pro firmy, které se chtějí ujistit, že jsou na správné cestě k bezpečnému a efektivnímu využívání umělé inteligence.





# Napište mi!

Barbora Brabcová

- ❖ Specialistka na firemní nákup
- ❖ Krotitelka procesů
- ❖ Lektorka

✉ [barbora.brabcova@bebecon.cz](mailto:barbora.brabcova@bebecon.cz)

[in](#) Barbora Brabcová | LinkedIn

