



Bezpečné používání AI ve firmě.

Rizika, která vznikají, když tým začne AI používat, a pravidla, která je ošetří. Bez strašení pokutami a bez zákazů, které nikdo nedodrží.

RIZIKA	DATA	PRAVIDLA	START
Pět typových Jak vypadají a co s nimi.	Tři úrovně Co kam smí a co nikdy.	Osnova o deseti bodech Šablona k vyplnění, ne teorie.	Prvních 30 dní Konkrétní kroky v pořadí.

OBSAH CO V PODKLADU NAJDETE

01	Pět rizik podrobně	str. 02
02	Kam data smí a kam ne	str. 03
03	Firemní AI pravidla	str. 04
04	Přístupy a incident	str. 05
05	Prvních 30 dní	str. 06

FAKT ODKUD RIZIKO SKUTEČNĚ PŘICHÁZÍ

Nebezpečná není AI. Nebezpečné je nemít pravidla.

R / 01

Data ven

Interní podklady
v neschváleném nástroji.

R / 02

Podvržený příkaz

Instrukce schovaná
v dokumentu, kterou nástroj
vykoná.

R / 03

Rozjeté přístupy

Nástroj vidí víc, než na svou
úlohu potřebuje.

R / 04

Stínové AI

Používání na vlastní účty,
mimo dohled firmy.

Páté riziko je nejtišší · nekontrolovaný výstup, který se použije jako fakt. Podrobně na následující straně

Pět rizik, jak vypadají a co je ošetří.

01 TYPOVÁ RIZIKA PRÁCE S AI

RIZIKO	JAK TO VYPADÁ V PRAXI	OPATŘENÍ
01 Firemní data ve veřejných nástrojích	Někdo vloží ceník nebo smlouvu do bezplatného nástroje, aby to měl rychleji.	Schválený nástroj se smlouvou, klasifikace dat a seznam toho, co se nikdy nevkládá.
02 Podvržené instrukce v dokumentech	V souboru nebo na webu je schovaný příkaz. Nástroj ho vykoná, jako by přišel od vás.	Obsah se nikdy nebere jako příkaz. Žádná akce navenek bez potvrzení člověkem.
03 Agenti s neschválenými přístupy	Nástroj má přístup k poště, disku nebo CRM, protože to bylo pohodlné.	Nejmenší nutný rozsah, oddělený účet, přehled schválení a revize.
04 Stínové používání AI	Lidé pracují na soukromé účty, protože firma nenabídla legální cestu.	Nabídnout schválenou cestu dříve než zákaz. Evidence nástrojů a proškolení.
05 Nekontrolovaný výstup	Číslo nebo citace se použije bez ověření, protože zněly přesvědčivě.	Údaj bez dohledatelného zdroje se nepoužívá. Kontrola je součástí úlohy.

4 TŘI KROKY, KTERÉ NESTOJÍ NIC

ZJISTIT, CO SE DNES POUŽÍVÁ

SEPSAT, CO SE NIKDY NEVKLÁDÁ

URČIT ODPOVĚDNOU OSOBU

Co tato rizika spojuje

Ani jedno nevzniká z technologie, ale z chybějícího rozhodnutí: co je schválené, kdo to kontroluje a kam data patří. Řeší se pravidly a školením, ne nákupem nástroje.

Co nefunguje

Plošný zákaz. Firmy, které AI zakázaly, ji mají v provozu dál, jen o tom nevědí. Zákaz bez alternativy vyrábí přesně to riziko, kterému měl zabránit.

Není to výčet všech myslitelných hrozeb, ale pět, které se v českých firmách opakují nejčastěji.

Kam data smí a kam v žádném případě.

Udrží se jen jednoduché pravidlo. Tři úrovně, každá s jasným seznamem. Kdo neví, kam co patří, ptá se předem.

Úroveň 01

Veřejné

Co je už dnes venku: texty z webu, ceník, tisková zpráva, rejstřík.

Kde smí: kterýkoli schválený nástroj

Úroveň 02

Interní

Postupy, nabídky, zápisy, neveřejná čísla. Vaše know how.

Kde smí: jen nástroj se smlouvou a bez učení z vašich dat

Úroveň 03

Chráněné

Osobní údaje, mzdy, zdravotní informace, data klientů pod mlčenlivostí, hesla.

Kde smí: jen po písemném posouzení, zpravidla vůbec

02 TYPICKÉ SITUACE A ZAŘAZENÍ

SITUACE	ÚROVEŇ	POZNÁMKA
01 Text na web nebo sociální síť	Veřejné	Bez omezení, výstup se jen kontroluje.
02 Vzorová smlouva bez jmen	Interní	Jména a částky se před vložením odstraní.
03 Nabídka konkrétnímu klientovi	Interní	Jen ve schváleném nástroji, ne v bezplatné verzi.
04 Životopisy uchazečů	Chráněné	Osobní údaje. Bez posouzení a právního titulu ne.
05 Mzdové podklady	Chráněné	Do externího nástroje nepatří.
06 Data klienta pod mlčenlivostí	Chráněné	Rozhoduje smlouva s klientem, obvykle to vylučuje i schválený nástroj.
07 Přístupové údaje a klíče	Chráněné	Nikdy, za žádných okolností, ani pro test.

Zařazení je vodítko, ne právní posouzení · u osobních údajů rozhoduje GDPR a smlouva s poskytovatelem, u dat klientů vaše smlouva s klientem.



Firemní AI pravidla na dvě strany.

Dokument, který lidé přečtou. Deset bodů, každý s konkrétní odpovědí. Osnovu vyplňujeme společně na školení.

A RÁMEC

- 01 Komu pravidla platí**
Zaměstnanci, brigádníci i externisté. Kdo pracuje s firemními daty.
- 02 Schválené nástroje a účty**
Jmenovitý seznam. Co na něm není, se nepoužívá pro pracovní účely.
- 03 Klasifikace dat**
Tři úrovně z předchozí strany, doplněné o vaše specifické případy.
- 04 Pravidla pro výstup**
Co se kontroluje, co potřebuje zdroj a co se označuje jako AI výstup.
- 05 Co AI nerozhoduje**
Výslovný seznam: lidé, ceny nad limit, právní stanoviska, cokoli bez podpisu.

B PROVOZ

- 06 Přístupy nástrojů**
Kdo je schvaluje, v jakém rozsahu a jak často se prověřují.
- 07 Osobní údaje**
Odkaz na vaši GDPR dokumentaci a jmenování odpovědné osoby.
- 08 Zákazníci a třetí strany**
Kdy je informujete, co máte ve smlouvách a co vyžadují oni.
- 09 Hlášení incidentu**
Komu a do kdy se hlásí únik. Bez sankce za nahlášení.
- 10 Evidence a revize**
Kdo byl proškolen a kdy se pravidla posuzují znovu.

Pravidla, která nikdo nečetl, nikoho nechrání.

Deset bodů projednaných s týmem funguje lépe než třicetistránková směrnice, kterou všichni odklikli. Doložitelnost stojí na tom, že se podle nich pracuje.

KRÁTKÉ A KONKRÉTNÍ

PROJEDNANÉ, NE ROZESLANÉ

S DATEM A REVIZÍ



C PŘÍSTUPY NÁSTROJŮ · PRINCIP NEJMENŠÍHO OPRÁVNĚNÍ

01

Jen na svoji úlohu

Nástroj na nabídky nepotřebuje vidět mzdy ani celou poštu.

02

Oddělený účet

Ne osobní účet zaměstnance. Přístup jde odebrat bez dopadu na jeho práci.

03

Čtení dřív než zápis

Většina úloh si vystačí se čtením. Právo měnit a odesílat je výjimka.

04

Přehled a revize

Seznam povolených přístupů se prochází po každé změně a pravidelně.

D KDYŽ SE NĚCO STANE

01

Zastavit, ne zakrývat

Odebrat přístup nebo vypnout postup, teprve pak řešit, co se stalo. Za nahlášení se nikdo netrestá, jinak se příště nedozvíte nic.

02

Zjistit rozsah

Jaká data se toho týkají, kdo je vložil a kam odešla.

03

Posoudit ohlašovací povinnost

U osobních údajů platí lhůty podle GDPR. Posuzuje odpovědná osoba nebo advokát, ne ten, kdo incident způsobil.

04

Upravit pravidlo, ne jen člověka

Opakovatelný incident znamená chybějící pravidlo. Poučení patří do dokumentu, ne do e-mailu.

! STÍNOVÉ AI · JAK HO PODCHYTIT

ZEPTAT SE

Anonymní otázka „co dnes používáte“ odhalí víc než audit.

NABÍDNOUT CESTU

Schválený nástroj a účet placený firmou. Bez toho zůstanou soukromé účty, jen skrytější.

ZAPSAT STAV

Kdo, co a k čemu používá. Zároveň první část evidence podle AI Actu.

Co udělat během prvního měsíce.

Pořadí je záměrné. První tři body nestojí nic a odstraní většinu rizika. Nákup nástroje je až pátý krok.

✓ CHECKLIST

☐ Zjistit, co se ve firmě dnes používá a k čemu.

☐ Sepsat, co se nikdy nikam nekládá.

☐ Určit odpovědnou osobu za pravidla.

☐ Vybrat a schválit nástroj pro interní data.

☐ Zavést firemní účty místo soukromých.

☐ Projít přístupy, které už nějaký nástroj má.

☐ Proškolit lidi, kteří s AI pracují.

☐ Založit složku s evidencí školení.

☐ Nastavit termín revize pravidel.

↳ CO K TOMU DODÁVÁME MY

01 Bezpečnostní blok ve výuce

Rizika na příkladech, ne na paragrafech. Součást každého školení.

02 Šablona firemních pravidel

Deset bodů z předchozí strany, vyplněných společně s týmem.

03 Evidence pro doložitelnost

Listina, osnova, materiály a potvrzení od zapsaného ústavu.

→ DALŠÍ KROK

Projdeme, co se u vás dnes reálně používá.

Bez auditu a hledání viníků. Zjistíme stav a řekneme, které tři kroky mají u vás největší efekt.

Kontakt

Český Institut pro AI a Data, z. ú.
Příčná 1892/4, 110 00 Praha 1

office@ciad.cz
ciad.cz

Informační podklad. © 2026 Český Institut pro AI a Data, z. ú., IČO 297 52 736, Příčná 1892/4, Nové Město, 110 00 Praha 1. Všechna práva vyhrazena. **Autorská práva a licence.** Tento dokument, jeho struktura, metodika i konkrétní formulace jsou autorským dílem CIAD ve smyslu zákona č. 121/2000 Sb. Adresátovi se poskytuje nevýhradní a nepřenositelná licence užití dokumentu pro vlastní vnitřní potřebu. Rozmnožování, zpřístupnění třetí osobě, zveřejnění, prodej ani vytváření odvozených děl nejsou bez předchozího písemného souhlasu CIAD dovoleny. **Omezení odpovědnosti.** Uvedená rizika, klasifikace a opatření jsou obecným rámcem dobré praxe. Nenahrazují posouzení podle GDPR, smluvních závazků vaší firmy ani stanovisko advokáta ke konkrétní situaci.