

# Compliance, GDPR a kybernetická bezpečnost při využívání AI/Legal Tech

**František Nonnemann, Myriad AI**

Legální kód: AI & Legal Tech Workshop

Praha, 6. února 2026



# O čem si budeme povídat?

- Jak začít s compliance u AI/LegalTech nástrojů?
- Strategická a operační rizika AI
- Akt o umělé inteligenci
- Osobní údaje a AI
- Kybernetická bezpečnost a provozní odolnost
- Sektorová regulace s dopadem na využití AI
- Řízení (compliance) rizik v praxi

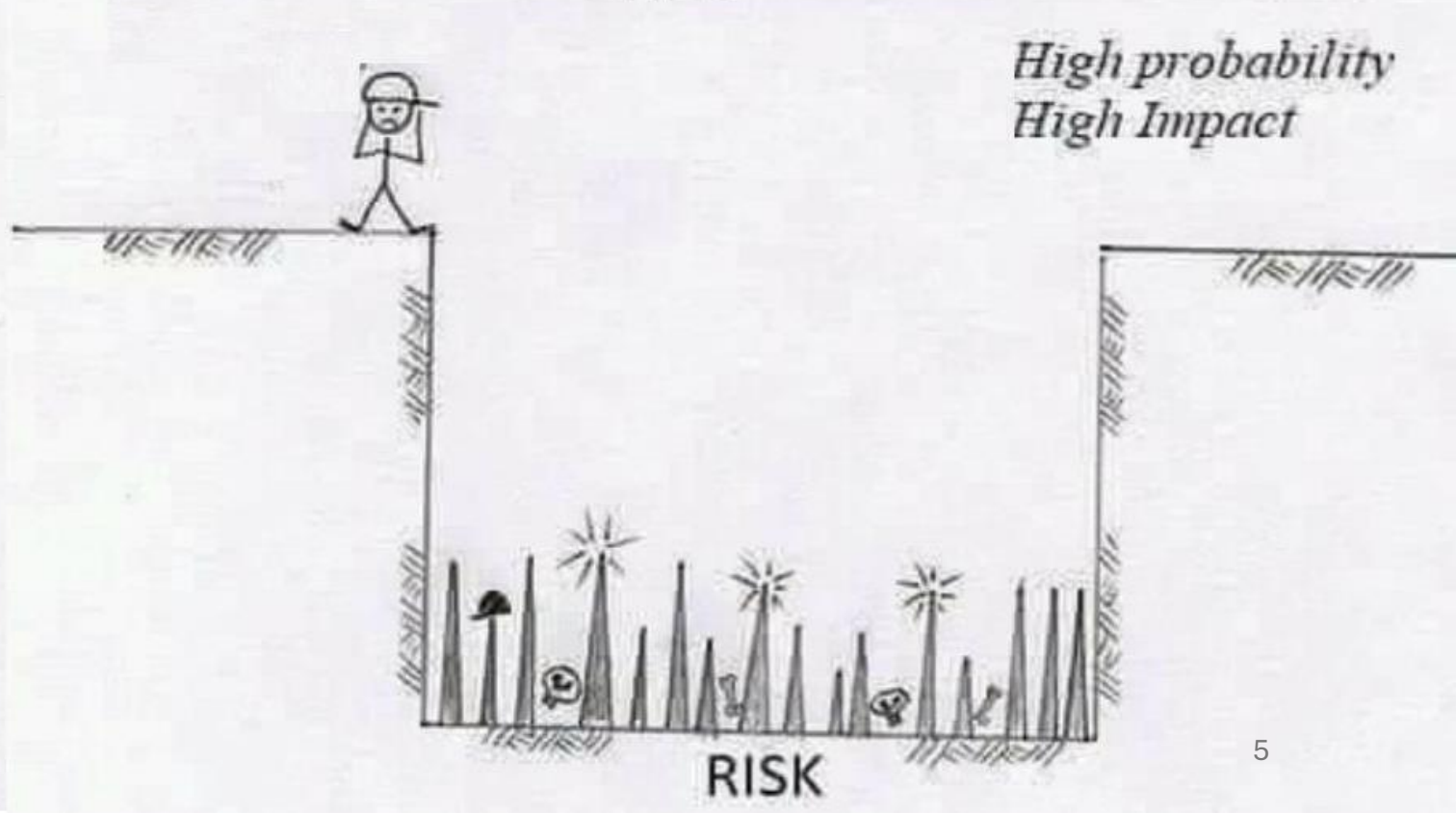
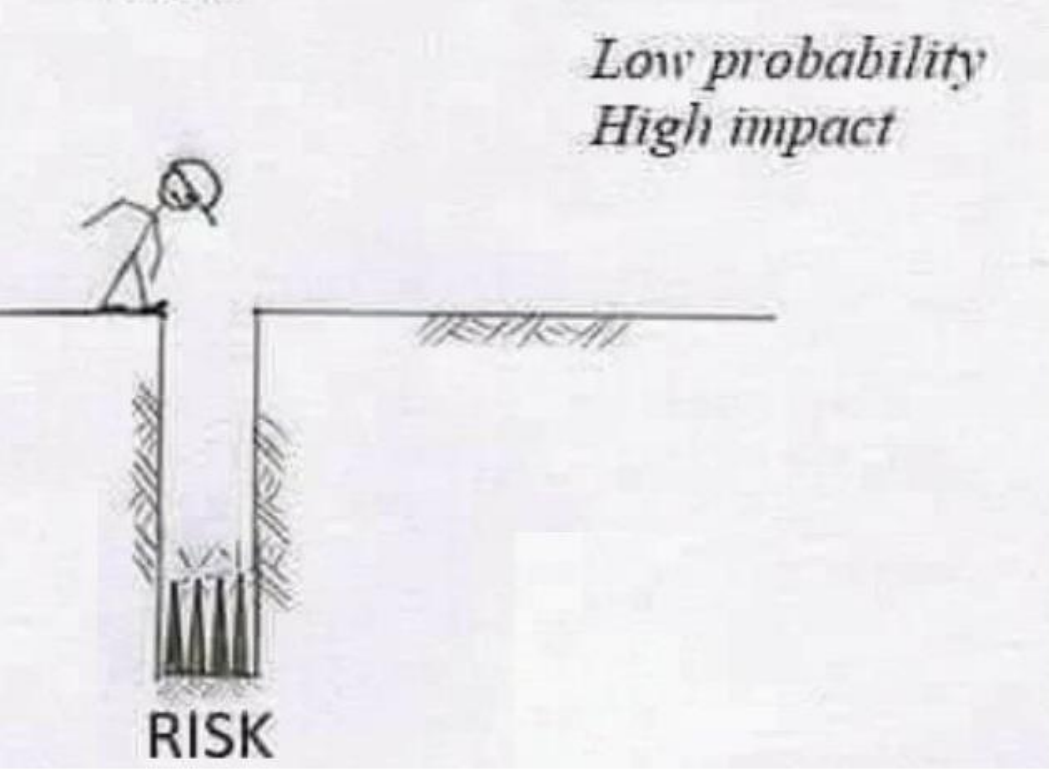
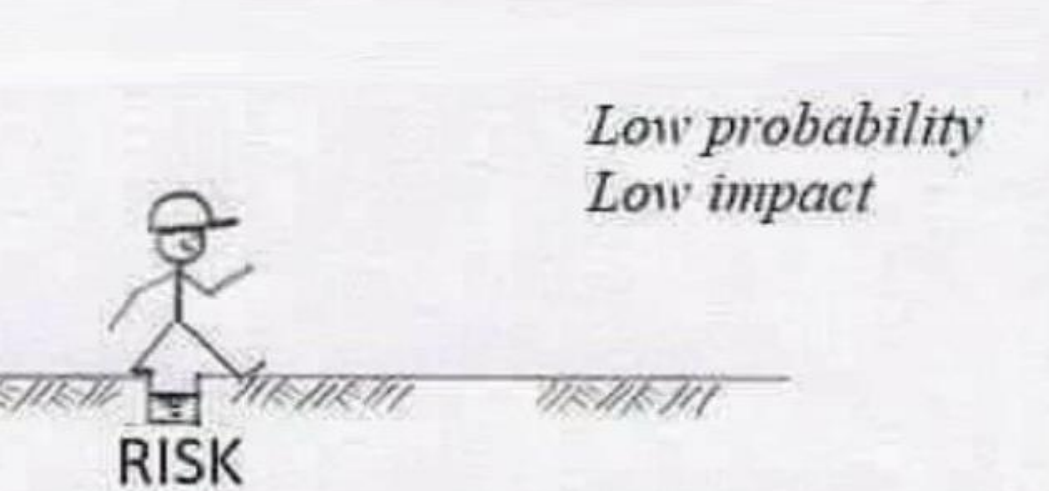
# Riziko je základ!

- Když se chceme chránit, musíme vědět, co a proti čemu chráníme
- Riziko? Možnost, že se v budoucnu stane něco špatného...
  - S určitou pravděpodobností (ne zcela hypoteticky) nastane událost, která bude mít negativní dopad na chráněný zájem, např. peníze, důvěrné informace, kybernetickou bezpečnost, provozní odolnost, dodání projektu, klienty, existenci společnosti, dodržování regulace...
- Informační aktivum → zranitelnost → hrozba → riziko
- Klientské údaje → Free verze AI nástroje → únik dat k provozovateli nebo dalšímu uživateli (prompt injection) → porušení GDPR

# Trocha teorie nikoho nezabije...

- Jak se měří "velikost" rizika? Kombinace pravděpodobnosti a dopadu
- Pravděpodobnost: Jak pravděpodobné je, že se riziko materializuje?
  - 1x za rok, 1x za 5 let, 1x za 20 let?
- Dopad: Jak významný bude dopad realizovaného rizika?
  - Náklady na náhradní řešení, přímá ztráta, náklady na opravu, pokuta, reputace...
- Možné ošetření rizika
  - Zmírnění, akceptace, přenesení, odstranění

# Visualizing Risk



# Není riziko jako riziko!

- Strategická a operační rizika?



# Strategická rizika



# Operační rizika

- Compliance rizika
- Informační bezpečnost
- Právní rizika
- Provozní rizika (odolnost)
- Finanční rizika
- ...

# Compliance rizika

- Akt o umělé inteligenci
- GDPR
- Sektorová regulace

# Akt o umělé inteligenci

- Vyhlášen v Úředním věstníku dne 12. července 2024
- Účinnost postupně:
  - 2. února 2025: Obecná ustanovení zákaz vysoce rizikových systémů, povinné školení zaměstnanců
  - 2. srpna 2025: Zahájení činnosti dozorových úřadů, dozor na úrovni EU a pravidla pro obecné modely AI
  - 2. srpna 2027: Zbytek, včetně pravidel pro vysoce rizikové systémy
- Digitální omnibus?

# Rizikovost AI podle AI Actu

- Čtyři kategorie rizikovosti AI pro dotčené osoby
- Nepřijatelné (čl. 5), např.:
  - Podprahové či manipulativní techniky
  - Zneužívání zranitelnosti skupiny osob
  - Sociální scoring
- Vysoké riziko (čl. 6 a příloha III), např.:
  - Biometrická identifikace na dálku, rozpoznávání emocí
  - Kritická infrastruktura (směrnice CER a nový zákon o kritické infrastruktuře)
  - Rozhodování v HR oblasti
  - Přístup k dárkám
  - Posuzování úvěruschopnosti
  - Rozhodování v oblasti životního a zdravotního pojištění
- Omezené riziko (zvukový, obrazový nebo video obsah podobný realitě)
- Minimální riziko - ostatní

# High-risk systémy

- Poskytovatelé a provozovatelé vysoce rizikových AI systémů musejí plnit řadu povinností, mj. zavést systém řízení rizik
- Čl. 9/2/a AI Actu: Systém řízení rizik je chápán jako nepřetržitý opakující se proces plánovaný a prováděný v rámci celého životního cyklu vysoce rizikového systému AI, který vyžaduje pravidelný systematický přezkum a aktualizaci. Zahrnuje následující kroky: ... identifikaci a analýzu známých a rozumně předvídatelných rizik, která může vysoce rizikový systém AI používaný v souladu se zamýšleným účelem představovat pro zdraví, bezpečnost nebo základní práva.

# AI rizika pro organizaci

- Je řízení rizik podle AI Actu pro organizaci dostatečné?
- Ochrání dostatečně sama sebe proti všem (operačním/compliance) rizikům?

# Není riziko jako riziko II

- GDPR a AI Act řeší **rizika pro práva a svobody dotčených osob**
- Na finančním trhu, v rámci ISMS, projektového řízení, kritické infrastruktury, řízení obchodních rizik atd. identifikujeme a snižujeme **rizika pro organizaci**

# Co s tím? Řídit AI rizika z pohledu organizace

1. Porozumění specifikům a potřebám organizace
2. Jasný přístup a závazek vedení k etickému a transparentnímu využívání AI
3. Přijetí interní strategie pro využití umělé inteligence
4. Určení rolí a odpovědností
5. Proces pro identifikaci a hodnocení rizik plynoucích z využití umělé inteligence
6. Nastavení opatření a kontrol ke snížení nepřijatelně vysokých rizik
7. Zajištění kvalifikace, odborné přípravy a dostatečných zdrojů pro zaměstnance podílející se na využití AI
8. Proces pro pravidelné hodnocení AI rizik, dostatečnosti kontrol a celého AIMS, průběžné vylepšování
9. Dostupná dokumentace celého systému a všech jeho důležitých kroků

\* inspirace ISO ISO/IEC 42001:2023: Systém řízení umělé inteligence

# Osobní údaje a AI

- Osobní údaj: prakticky vše, co lze reálně spojit s fyzickou osobou (vč. veřejně dostupných dat, pseudonymizovaných dat atd.)
- Zpracování: operace či sestava operací prováděná s osobními údaji automatizovaně (nebo manuálně s rejstříkem)
- Zpracování osobních údajů → GDPR

# GDPR rizika

- Vývoj AI modelu s využitím osobních údajů
  - Kdo je odpovědný za zpracování osobních údajů?
  - Právní titul a další GDPR povinnosti/odpovědnosti
- Zpracování osobních údajů při provozu AI
  - Odpovědnost organizace: správce a zpracovatel, předání dat mimo EU, transparentnost, automatizované rozhodování
  - Bezpečnost a integrita → kyberbezpečnost

# Kyberbezpečnost - compliance rizika

- Organizace je v režimu NIS2 (ZkB) nebo DORA
- Externí aplikace → povinnosti pro řízení dodavatelského řetězce (výběr a hodnocení dodavatele, smlouva, evidence, kontrola)
- Interní aplikace → součást IT prostředí, tzn. řízení změn, přístupová oprávnění, aktualizace, evidence, incidenty...

# Kybernetická rizika

- Únik důvěrných informací
  - Provozovatel systému, další uživatelé (úmysl, náhoda/chyba)
  - Osobní údaje, bankovní tajemství, obchodní tajemství (know-how, kód, ceny, plánované produkty)
- Ohrožení provozu a dostupnosti
  - Zavlečení slabiny, chyba při testingu, monitoringu, provozu, řízení výkonu
- Oslabení kybernetické bezpečnosti a provozní odolnosti
  - Bezpečnostní chyba, selhání bezpečnostního nástroje, nezachycení/špatné vyhodnocení alertu, bypassing řízení přístupů a rolí
- Autenticita
  - Generované výstupy nejsou ověřitelné (halucinace), neschopnost auditovatelnosti konkrétního závěru, doporučení, manipulace vstupních dat pro ovlivnění modelu

# Sektorová regulace

- Finanční regulace (AML, obezřetnost, distribuce produktů):
  - Dokumentovatelnost a rekonstruovatelnost postupů a činností
  - Dohledový benchmark ČNB č. 2/2023 K provádění kontroly klienta prostřednictvím systému k monitoringu transakcí, část VI. AML monitoring s využitím umělé inteligence (AI): ověření kvality vstupních dat, dokumentovatelnost, možnost průběžné kalibrace, řízení rizik, testování, bias, transparentnost
  - Lze zobecnit pro další povinnost dle finanční regulace
- Zdravotnictví
  - AI Act neřadí využití AI ve zdravotnictví mezi vysoce rizikové systémy, protože existuje samostatná regulace
  - Nařízení č. 2017/745 o zdravotnických prostředcích + nařízení č. 2017/746 o diagnostických zdravotnických prostředcích in vitro, vztahují se mj. na přístroje, zařízení, software či systém využívaný k získání některé informací např. o vrozeném postižení, predispozici k určitému zdravotnímu stavu nebo nemoci nebo pro stanovení bezpečnosti a kompatibility s možnými příjemci atd.
  - Požadavky na řízení systému (podobné AI Actu): Zajistit bezpečnost a výkonnost AI nástrojů a tyto nástroje evidovat, hodnotit jejich rizikovost, mít k dispozici aktuální a úplnou technickou dokumentaci, zavést systém řízení kvality, oznamovat závažné incidenty atd.

# Jak rizikům přecházet?

- Riziko ShadowAI → školení + "zbraňová amnestie"
- Řešit jednotlivé případy využití AI individuálně: proces + nástroj (model, verze, podmínky) = rizika → opatření
- Pravidelně aktualizovat, rychleji než v jiných procesech
- Celková governance (alespoň základní strategie, role, povinnost, vazba na další předpisy)

# Příklady opatření

- Provoz a dostupnost
  - Kontrolovat výstupy (manuálně, automaticky?), ověřit spolehlivost v omezeném rozsahu (pilot), výběr spolehlivého dodavatele
- Compliance (a právní) rizika
  - Znat podmínky externího nástroje (vč. sledování změn), výběr vhodné licence, školení, aplikace sektorové regulace
- Důvěrné informace
  - Interní klasifikace informací, výběr vhodné licence (nesdílet data s ostatnímu uživateli, data lokace), pseudonymizace, šifrování dat, školení

# AI je fajn, ale...



A jako AI



B jako  
bezpečnost



C jako  
compliance

frantisek@myriad.company