CYBERLAWYER

PRÁVNÍ PRŮŠVIHY PŘI NASAZOVÁNÍ AI NÁSTROJŮ

Praktické zkušenosti aneb Když se to nepovedlo (2. část)

Jindřich Kalíšek
Advokát a řídící partner CYBERLAWYER | CEO regfor

Kongres Právní prostor 2026 | Seč | 29. 4. 2026

WHOIS?

JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/E CIPM FIP

- Advokát a zakladatel CYBERLAWYER
- Hlavní architekt a zakladatel regfor
- Vysokoškolský učitel na Právnické fakultě UK

- Člen Sekce pro umělou inteligenci a nové technologie České advokátní komory
- Člen Spolku pro ochranu osobních údajů
  - > Předseda Komise pro kyberbezpečnost

TAKOVÝ NORMÁLNÍ COMPLIANCE PROJEKT

- **Klient:** Jedno z největších tuzemských zdravotnických zařízení
  - 50+ klinických pracovišť
  - 3 000+ zaměstnanců
  - 50 000+ pacientů ročně

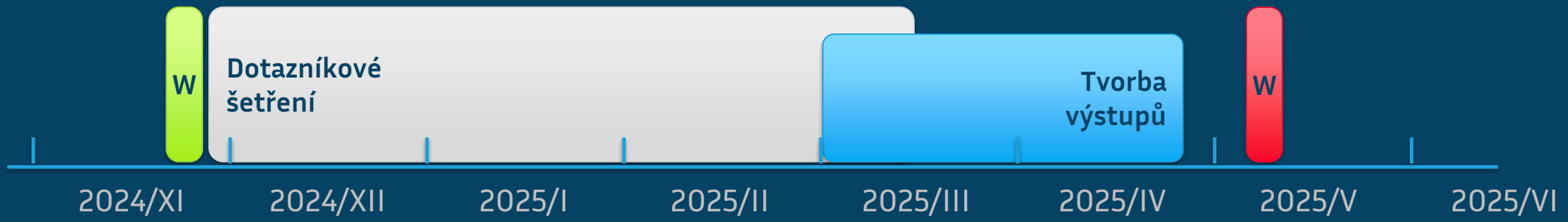
- **Předmět služeb:** Úvodní studie nasazení a využívání nástrojů AI v prostředí zdravotnického zařízení
  - Právní a compliance omezení při zavádění AI nástrojů ve zdravotnickém zařízení
  - Identifikace požadavků oborové regulace (regulace AI, ochrana soukromí a osobních údajů pacientů, informační a kybernetická bezpečnost apod.), které bude nutné naplnit pro řádný provoz nástrojů
  - Posouzení již známých záměrů na implementaci
  - Identifikace rizik a neshod

TAKOVÝ NORMÁLNÍ COMPLIANCE PROJEKT

– Výstupy:

> Úvodní workshop s managementem a klíčovými specialisty
> Souhrnné compliance memo k AI Actu a jeho dopadech pro zdravotnické zařízení
> Check-list povinností a pre-imp dotazník pro posouzení využitelnosti AI nástroje ve FNP
> Analýza výstupů dotazníkového šetření a hodnocení už zavedených nástrojů
> Závěrečný workshop s managementem a klíčovými specialisty

– Timing:

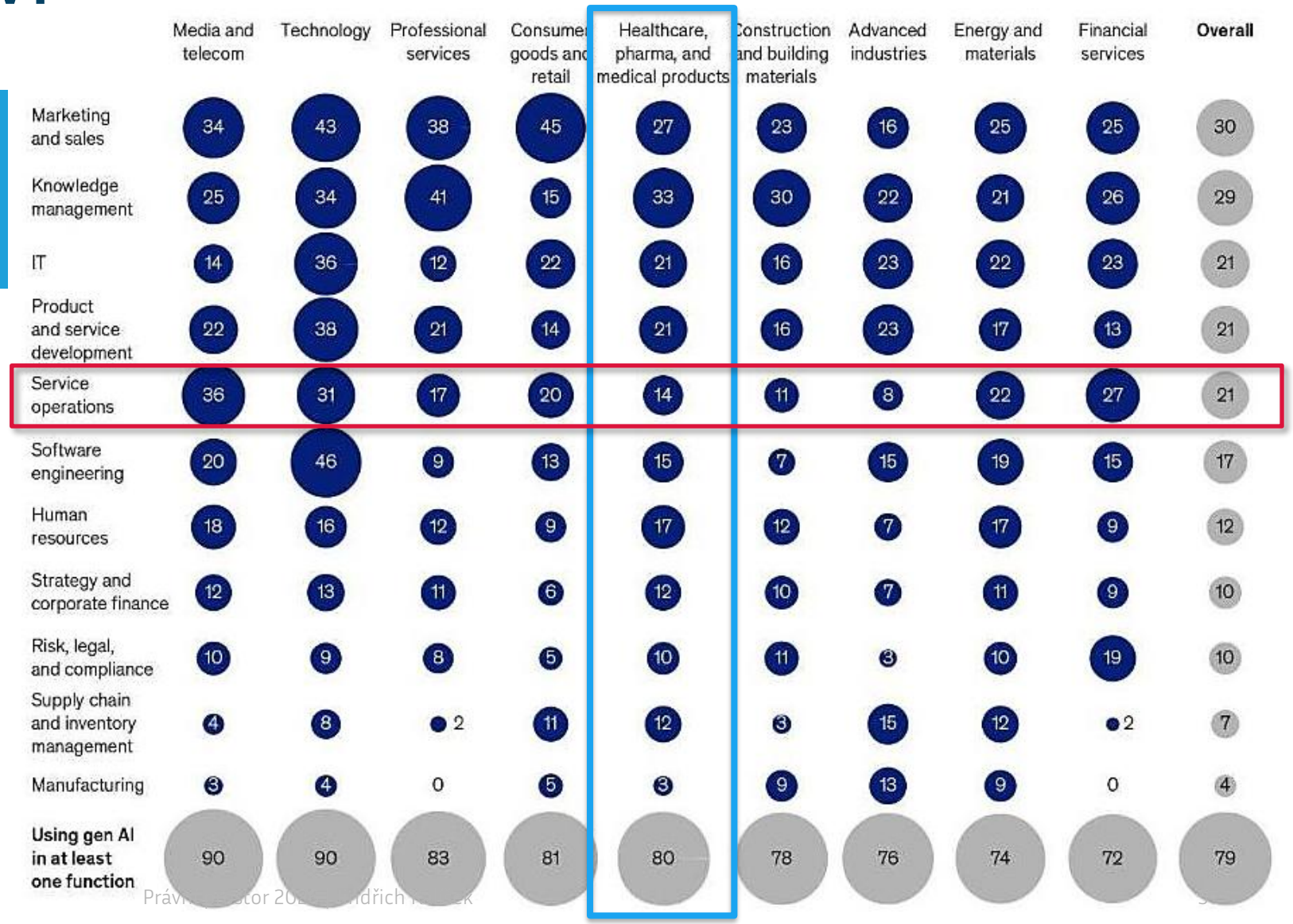


AI VE ZDRAVOTNICTVÍ

McKinsey & Company

Nejčastější využití AI →

- Marketing
- Znalostní management
- IT



	Media and telecom	Technology	Professional services	Consumer goods and retail	Healthcare, pharma, and medical products	Construction and building materials	Advanced industries	Energy and materials	Financial services	**Overall**
Marketing and sales	34	43	38	45	27	23	16	25	25	30
Knowledge management	25	34	41	15	33	30	22	21	26	29
IT	14	36	12	22	21	16	23	22	23	21
Product and service development	22	38	21	14	21	16	23	17	13	21
Service operations	36	31	17	20	14	11	8	22	27	21
Software engineering	20	46	9	13	15	7	15	19	15	17
Human resources	18	16	12	9	17	12	7	17	9	12
Strategy and corporate finance	12	13	11	6	12	10	7	11	9	10
Risk, legal, and compliance	10	9	8	5	10	11	3	10	19	10
Supply chain and inventory management	4	8	2	11	12	3	15	12	2	7
Manufacturing	3	4	0	5	3	9	13	9	0	4
Using gen AI in at least one function	90	90	83	81	80	78	76	74	72	79

KRÁSNÝ NOVÝ SVĚT V ČÍSLECH

9 / 2*	Počet rutinně používaných AI nástrojů v prostředí klienta (* - počet AI nástrojů založených na veřejných LLM modelech)
6	Počet AI nástrojů s chybějící anebo zjevně nedostatečnou dokumentací podle MDR / IVDR a AI Actu
2,5 hod.	Průměrná úspora času jednoho zaměstnance u opakujících se úkolů (administrativní činnosti, e-maily, reporty apod.)
10 / 30 %**	Odhad průměrného nárůstu produktivity (** - na specializovaných klinických pracovištích)

Zdroj: Dotazníkové šetření provedené u klienta v rámci akce MZ ČR

KRÁSNÝ NOVÝ SVĚT V ČÍSLECH (NEPŘÍLIŠ LICHOTIVÝCH)

58 % Podíl zaměstnanců, kteří používají AI nástroje k pracovním úkolům pravidelně

70 % Podíl zaměstnanců, kteří používají veřejně dostupné verze AI nástrojů

48 % Podíl zaměstnanců, kteří do AI nástrojů nahrávají citlivá data a osobní údaje

66 % Podíl zaměstnanců, kteří se při práci spoléhají na výstupy AI, aniž by je kriticky hodnotili anebo ověřovali vůči více zdrojům

Zdroj: A Global Study, University of Melbourne, KPMG International , publikováno na LinkedIn, 19. 4. 2026

HLAVNÍ VÝSTUPY COMPLIANCE PROJEKTU

— Manažerské AI FOMO existuje

> Zdravotnická zařízení často zavádí AI nástroje nikoliv pod tlakem efektivity či prokazatelně lepší péče, ale na základě marketingu a podle přání managementu (odborného / obecného)

— Zdrojem neshod je nepřipravená a nedostatečná governance a compliance

> Praktické problémy typicky nevznikají v samotném modelu AI, ale v governance, dokumentaci a řízení odpovědností

— Časté problémy v praxi

> Shadow AI
> Nejasná role poskytovatele vs. zavádějícího subjektu
> Absence interních pravidel a schvalovacích procesů
> Nedostatečné vyhodnocení regulatorních dopadů
> Podcenění kybernetických a datových rizik

ROLE ZDRAVOTNICKÉHO ZAŘÍZENÍ PODLE AIA

- Povinnosti nevznikají jen výrobcům AI systémů
- Zdravotnické zařízení bude zpravidla vystupovat jako „zavádějící subjekt“ (deployer)
- Klíčové povinnosti na straně nemocnice:
  - Používání AI v souladu s návodem a určeným účelem
  - Zajištění lidského dohledu
  - Evidence a uchovávání logů
  - Monitoring incidentů a reporting
  - AI gramotnost zaměstnanců
  - Spolupráce s dozorovými orgány

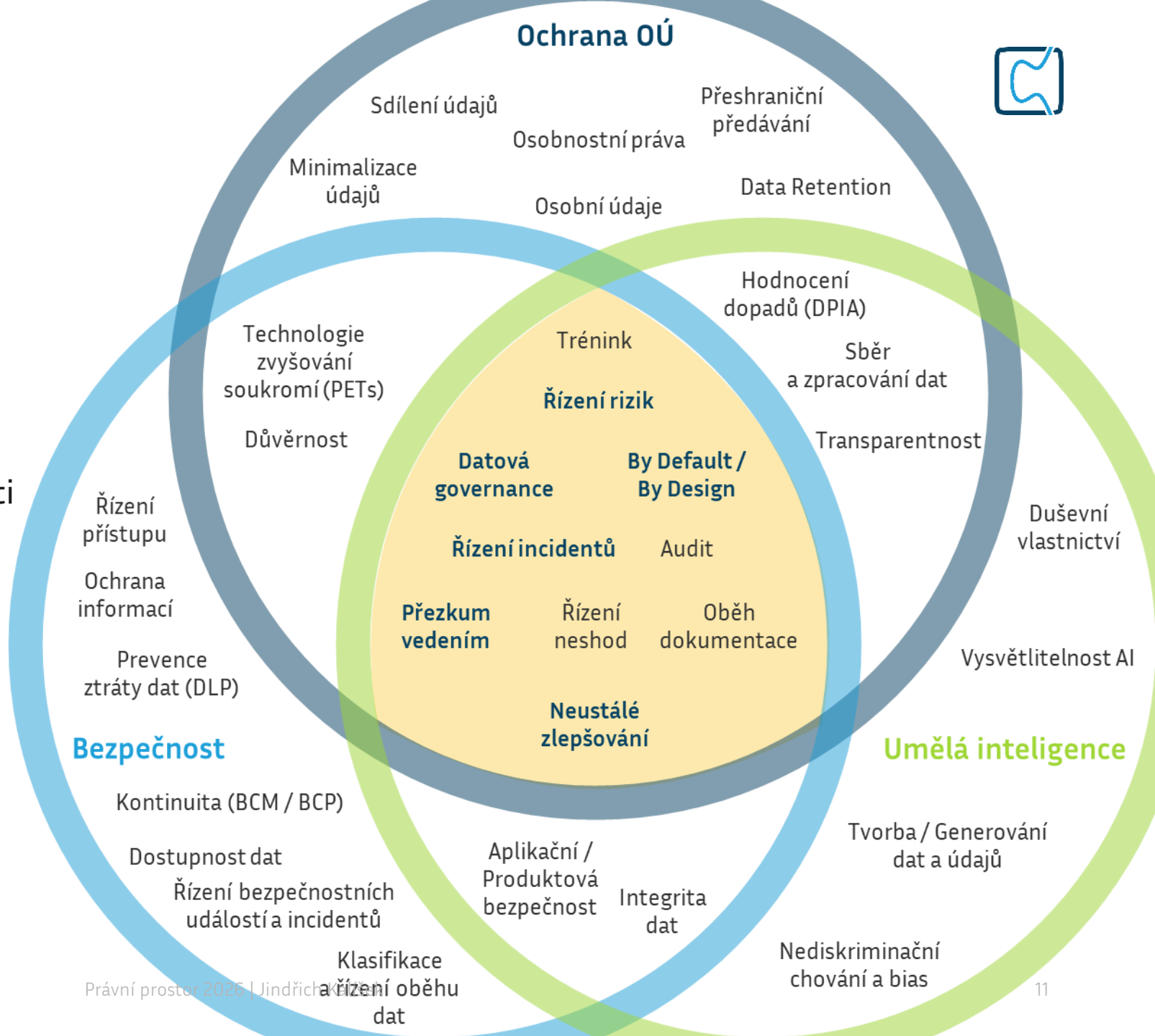
NEJVĚTŠÍ PRAKTICKÉ PROBLÉMY PŘI IMPLEMENTACI

- **AI governance bývá fragmentovaná a AI compliance nezdokumentovaná**

- **Typické problémy identifikované při workshopech a analýzách**
  - Zaměstnanci používají veřejné generativní AI nástroje a vkládají do nich chráněná data
  - Neexistuje centrální evidence AI nástrojů
  - Není určeno, kdo schvaluje, monitoruje a vyhodnocuje použití AI
  - Chybí proces klasifikace AI systémů a proces ex ante / pre-imp vyhodnocování jejich rizik
  - Smluvní dokumentace dodavatelů neodpovídá požadavkům AIA / MDR / IVDR
  - Není provedeno DPIA / FRIA
  - AI compliance je řešena odděleně od kyberbezpečnosti a GDPR

PŘEKRYV REGULACÍ

- **Čtyři vertikály digitální compliance**
  - > Tvoří jednotný prostor regulace
  - > Jsou propojeny přes klíčové procesy a liniové činnosti



PŘEKRYV REGULACÍ: AIA NENÍ VÁŠ JEDINÝ PROBLÉM

- Implementace AI ve zdravotnictví vytváří překryv více regulatorních režimů

- Vedle AIA je nutné řešit zejména:
  - MDR / IVDR
  - GDPR a ochranu citlivých zdravotních údajů
  - Zdravotnickou dokumentaci a odpovědnost za péči
  - NZKB (NIS2) a kybernetickou bezpečnost
  - Informační bezpečnost a řízení přístupů
  - Smluvní odpovědnost a vztahy vůči dodavatelům

CO MUSÍ MÍT NEMOCNICE PŘIPRAVENO

— **Bez kvalitní interní governance nelze AI bezpečně zavádět**

— **Doporučené dokumenty a procesy**

> AI strategie a governance framework
> Interní AI politika a pravidla používání
> Proces schvalování a klasifikace AI nástrojů
> Metodika DPIA / FRIA
> Pravidla práce se zdravotními daty
> Proces hlášení incidentů
> Školení zaměstnanců (*AI literacy*)

AI COMPLIANCE JAKO PROVOZNÍ DISCIPLÍNA

- **Největší riziko není samotná AI, ale nekoordinované zavádění AI do provozu**

- AI governance ve zdravotnictví musí propojit
  - Management zdravotnického zařízení
  - Odborný zdravotnický personál
  - Právní oddělení a compliance (DPO)
  - CISO a kyberbezpečnost

- **AI compliance není jednorázový projekt, ale kontinuální provozní disciplína**
  - Důraz na transparentní, informované a etické využívání AI nástrojů

ZÁVĚREČNÁ DOPORUČENÍ

AI governance musí být součástí rutinního řízení nemocnice

- > AI není izolovaný IT projekt
- > Zavádění AI musí propojit management, právní oddělení, compliance, DPO, CISO a zdravotnický personál
- > Každý AI nástroj musí mít vlastníka, odpovědnost a schvalovací proces
- > Bez evidence AI systémů nelze efektivně řídit rizika ani regulatorní povinnosti

Největší problém není AI, ale chaos kolem ní

- > Nekontrolované používání AI zaměstnanci vytváří právní i bezpečnostní rizika
- > AI governance musí být kontinuální proces, ne jednorázový projekt
- > Investice do AI literacy a interních pravidel budou levnější než řešení incidentů

COMPLIANCE LZE AUTOMATIZOVAT

www.regfor.cz

BEZPEČNOSTNÍ COMPLIANCE

BEZPEČNOST DODAVATELSKÉHO ŘETĚZCE

AUTOMATIZACE

CERTIFIKACE

TRÉNINK, ŠKOLENÍ

AUDIT, KONTROLA

DISKUSE (Q&A)

DOTAZY?
PŘÍPOMÍNKY?
NADŠENÍ / ZKLAMÁNÍ?

Jindřich Kalíšek

kalisek@cyberlawyer.cz
kalisek@regfor.cz