Otázky, bez kterých AI nepoužívejte

Dalibor Kačmář
Ředitel pro technologie a bezpečnost

Gabriela Holíková
Ředitelka pro právní záležitosti

Microsoft Česká republika a Slovensko

Proč si tyto otázky pokládat?

AI neexistuje v právním vakuu.

GDPR, sektorové předpisy i nový EU AI Act platí souběžně.

Cílem je vědět, NA CO se ptát dodavatele i sebe sama — než systém pustíte do produkce.

01

EU AI Act · Regulatorní povinnosti

Jak naplníme povinnosti podle Aktu o umělé inteligenci?

01

ODPOVĚĎ

Akt o umělé inteligenci — jak to vidíme v Microsoftu?

- **Klasifikace use case je úkol deployera**
  Veřejná správa = často zavádějící subjekt vysoce rizikových systémů. Začněte gap analýzou pro každý use case.

- **Microsoft je signatář EU AI Pactu**
  Responsible AI Standard interně předjímá řadu požadavků Aktu.

- **Compliance Manager**
  V Microsoft Purview hotová AI Act assessment template — strukturovaná evidence.

- **AI Foundry & RAI Dashboard**
  Model cards, evaluace, transparency reporty požadované pro high-risk systémy.

- **Rozdělení odpovědnosti**
  Microsoft plní svou část jako poskytovatel (provider); vy plníte svou jako zavádějící subjekt (deployer) — smluvně i technicky podpořeno.

02

GDPR · DPIA · čl. 22

Potřebujeme DPIA a jak ošetříme GDPR u AI?

02

ODPOVĚĎ

GDPR & DPIA — jak na to s Microsoftem

- **DPIA je u AI pravidlo**
  Při zpracování osobních údajů nebo rozhodování s významnými dopady = automatický spouštěč.

- **Microsoft je typicky zpracovatel**
  DPA + Podmínky pro produkty: vaše data zůstávají vaše, netrénují foundation modely.

- **Vzorové posouzení k dispozici v Trust Centru**
  Upravitelná šablona DPIA pro snadnější start.

- **Purview Data Lifecycle Management**
  Retenční politika pro prompty, odpovědi a logy — historie chatu je nová kategorie záznamů.

- **Copilot respektuje přístupová práva**
  Uživateli ukáže jen to, na co už má přístupová práva v M365 — minimalizace v praxi.

03

US CLOUD Act · Digitální suverenita

Mohou k našim datům přistupovat zahraniční orgány činné v trestním řízení?

03

ODPOVĚĎ

Přístup orgánů činných v trestním řízení

- **Cloud Act -** Clarying Lawful Overseas Use of Data (CLOUD) Act (v překladu: *zákon o zákonném užívání údajů v zahraničí*)
  - NEUMOŽŇUJE neomezený, hromadný nebo automatický přístup vlády k údajům zákazníků.
  - NEIGNORUJE zahraniční právo.
  - Žádosti o údaje zahraničních společností podle zákona CLOUD Act NEJSOU běžné.
  - Extrateritoriální přístup orgánů činných v trestním řízení k údajům NENÍ specifikem USA.
- **EU Data Boundary**
  Zpracování dat M365, Azure i Dynamics 365 v evropských datacentrech.
- **Defending Your Data**
  Napadáme nelegitimní žádosti orgánů, notifikujeme zákazníka, finančně kompenzujeme porušení GDPR.
- **Customer Lockbox**
  Microsoft inženýr nemá přístup k vašim datům bez vaší výslovné aprobace — vše auditováno.
- **Customer-managed keys & Confidential Computing**
  Bez vašeho klíče data nedešifruje nikdo — ani Microsoft, ani třetí strana.

04

Duševní vlastnictví · Autorské právo

Kdo vlastní výstup generativní AI — a co když poruší cizí autorská práva?

04

ODPOVĚĎ

Vlastnictví AI výstupu & copyright

- **Podle smlouvy**
  U Copilot a Azure OpenAI: vstupy i výstupy patří zákazníkovi.

- **Vaše data se nepoužívají k trénování**
  Služby Microsoft Generative AI nebudou používat zákaznická data k trénování žádného modelu generativní umělé inteligence, s výjimkou případů, kdy je to v souladu s prokazatelnými pokyny zákazníka.

- **Copilot Copyright Commitment**
  Microsoft obhájí komerčního zákazníka a uhradí přiznané škody za porušení autorského práva způsobeného výstupem Copilotu.

- **Podmínka: guardrails zapnuté**
  Závazek platí, pokud zákazník nepoužije obejití content filtrů a předepsaných guardrails.

- **Podmínka: nejde o záměrné zneužití**
  Zákazník výstup neupravuje, neužívá ani nedistribuuje způsobem, u kterého ví, že by porušoval nebo zneužíval práva třetích stran.

05

AI služby · Provoz

Kdo provozuje AI službu a jazykový model a jakým způsobem? Má to na odpovědnost provozovatele?

05

ODPOVĚĎ

Způsob provozu AI služby

Porozumění dodavatelskému řetězci
Poskytovatel AI služby může být závislý na jednom nebo více subdodavatelích.

Služby a jazykové modely
AI služby budou založeny na více modelech – odbornost, vzájemná kontrola, rozdělení komplexních úloh

Varianty provozu
Nejčastější: LLM poskytovaný provozovatelem, malé modely ve vlastním nasazení, „přeprodej“ služeb (API) 3. strany

Odpovědnost provozovatele
Optimální situace: poskytovatel AI služby přebírá odpovědnost za své subdodavatele; jedny smluvními podmínky.

Microsoft AI služby
OpenAI LLM: provozovány Microsoftem ve vlastních datových centrech, zcela odděleně od společnosti OpenAI
Anthropic LLM: dostupné v Microsoft AI službách, provozovány Anthropic = subdodavatel, Microsoft smluvní záruky
OSS & vlastní SLM: provozuje zákazník sám na pronajatých výpočetních prostředcích

06

Data v AI · Rezidence

Kde budou uložena má data a kde budou zpracovávána? Mohu tuto oblast efektivně řídit?

06

ODPOVĚĎ

Rezidence data a její řízení

Data v neaktivním stavu a při zpracování
Uložení a jejich zpracování se může odehrávat na oddělených místech. Vliv na analýzu rizik a dopadů.

Co si pamatuje AI služba
Vyžadujte „nestavové“ generování odpovědí (inference). Pokud má „paměť“, data vám musí patřit a musíte je řídit.

Řízení rezidence uložení a zpracování dat
Základ - transparence. Ideálně definovat místo v EU. Jinak nutné ekvivalentní záruky: DPF, SCC a jiné.

Microsoft AI služby
Azure AI a M365 Copilot: nabízí možnost plné rezidence v EU/EFTA = záruky Evropské datové hranice (EUDB)
U Anthropic modelů je garantováno uložená dat v EU/EFTA, zpracování probíhá v USA. EUDB ~ přelom 26/27

07

Data v AI · Zpracování a ochrana

Co se může s našimi daty při zpracování AI dít a jak data efektivně chránit?

07

ODPOVĚĎ

Zpracování dat a jejich ochrana

- **Práva poskytovatele služby**
  AI je nákladnou technologií, pozor na služby poskytované „zdarma“ a podmínky poskytování služby.

- **Nutné záruky**
  Zpracování dat pouze pro poskytování služby. Žádné trénování a vylepšování modelu, sdílení s výrobcem modelu.

- **Respektování soukromí a důvěrnosti informací**
  AI služby musí respektovat soukromí a důvěrnost, jejich nastavení je otázkou datových zdrojů. Pozor, týká se i generovaných výstupů.

- **Microsoft AI služby**
  U všech služeb platní „Nutné záruky“.
  M365 Copilot: Respektuje přístupová práva a klasifikaci dokumentů. Umožňuje klasifikaci „není učeno pro AI“.
  M365 Copilot: Chrání výstupy podle úrovně klasifikace vstupů.

08

AI služby · Hrozby a bezpečnost

Jak nás zvolená technologie chrání před novými AI hrozbami?

08

ODPOVĚĎ

Nové hrozby a jejich zmírnění

Nové typy hrozeb

Nadměrné sdílení informací, úniky informací, zneužití a napadení AI systémů.

Sdílená odpovědnost - uživatel

Organizační politiky a jejich vynucení pro ochranu dat. Odpovědný a bezpečný vývoj vlastních řešení. Řízení přístupu k aplikacím. Odpovědné používání koncovým uživatelem.

Sdílená odpovědnost - poskytovatel

Zajištění bezpečného provozu, technologie pro ochranu dat (šifrování), prokázání shody (ISO, SOC, penetrační testy)

Microsoft AI služby

- Microsoft AI služby získaly certifikace podle mezinárodního standardu ISO 42001:2023 pro managment AI systémů: Odpovědné, etické a transparentní řízení AI služeb – řízení, risk management and provozní opatření.
- Implementujeme a sdílíme framework pro Odpovědnou AI, v souladu s NIST AI Risk Management Framework
- Umožňujeme monitorování rizik v reálném čase a včetně rizikového chování (AI služby, Copilot & Agenti)
- Poskytujeme postupy (LLMOps) a nástroje pro vývoj vlastích řešení – organizace dat, experimenty, hodnocení, ochrana promptů, detekce halucinací, hodnocení bezpečnosti, posouzení rizik a bezpečnosti užití.

09

Odpovědnost · Lidský dohled

Kdo nese odpovědnost za rozhodnutí AI a jak zajistit lidský dohled?

09

ODPOVĚĎ

Lidský dohled & odpovědnost

- **Odpovědnost = lidé, ne algoritmy**
  Princip odpovědného nasazení AI: lidé zůstávají odpovědní za výstupy AI.

- **Výbor pro odpovědné řízení umělé inteligence**
  Cross-funkční tým: právní, privacy, IT, bezpečnost, byznys, HR. Pravidelná revize případů použití umělé inteligence.

- **Interní směrnice pro používání umělé inteligence**
  Schválené použití a nástroje, zakázané použití.

- **Nástroj Defender for Cloud Apps**
  Odhalí shadow AI nástroje v organizaci — bez tohoto pohledu nemusíte vidět reálná rizika.

- **Vynucování pravidel a školení zaměstnanců**
  Pravidla: Kdo, na co, s jakými daty může AI použít.

Z Á V Ě R

Soulad není brzda inovace. Je to podmínka důvěry.

Microsoft pomáhá s velkou částí compliance smluvně a technicky — vy se můžete soustředit na vhodné použití a kvalitu služby občanům.

Děkujeme za pozornost.

Dotazy nám posílejte na:
gabriela.holikova@microsoft.com a dalibor.kacmar@microsoft.com