

Microsoft 365 Copilot: Mýty a fakta o bezpečnosti

Jak je to doopravdy s ochranou dat,
soukromím a AI ve firmách?

Březen 2026



AI nástroje, jako je Microsoft 365 Copilot, mění svět byznysu přímo před našima očima téměř ze dne na den.

To, co původně začalo jako uzavřené vědecké experimenty se strojovým učením, dnes zasahuje do našich každodenních životů. Od nákupů až po práci, učení nebo kreativní činnost.

Z výhod umělé inteligence těží firmy všech velikostí. Přestože je Microsoft 365 Copilot na trhu jen krátce, data z průzkumu Work Trend Index 2023 od Microsoftu mluví jasně.

70%

uživatelů potvrzuje vyšší produktivitu práce.

71%

uživatelů tráví méně času rutinními úkoly.

68%

uživatelů říká, že díky Copilotovi odvádí kvalitnější práci.

Nelze se proto divit, že

34%

manažerů vnímá AI jako jednu z hlavních priorit a považuje ji za klíč k udržení kroku s dobou a vyšší konkurenceschopnosti byznysu.²

Je úplně přirozené, že raketové tempo inovací budí i určité obavy. Nikdo nechce šlápnout vedle, a tak se často sami sebe ptáme:

- Q Jsou naše data opravdu v bezpečí?**
- Q Zůstane to, na co se AI ptáme, skutečně soukromé?**
- Q A co předpisy a pravidla, které musíme dodržovat?**

Kolem AI dnes koluje spousta mýtů. Internet je plný „zaručených“ zpráv, které občas zbytečně zveličují případná rizika. Vyznat se v tom, co je a co není pravda, tak bývá obtížné.

Proto jsme pro vás připravili přehled nejčastějších otázek a odpovědí a podíváme se, jak je to s bezpečností a soukromím u Microsoft 365 Copilota doopravdy. Ať už o zavedení AI uvažujete, případně jej už máte, ale nejste si úplně jistí všemi bezpečnostními mechanismy, je tu přesně pro vás tento náš stručný průvodce.

Pořídte si licenci
Microsoft 365 Copilot
od Vodafone Business



Generativní AI má obrovský potenciál, ale přirozeně budí otázky ohledně bezpečnosti, a leckdy dokonce i strach o práci. Tyto pochybnosti musíme rozptýlit. AI tu není, aby nás nahradila, ale aby nám uvolnila ruce.

Nedostatečná informovanost kolem AI nás zbytečně brzdí. Často nám brání v rozhodnutích, která by přitom mohla všem usnadnit práci a život.

Pojďme si to nejdůležitější uvést na pravou míru. Posvítíme si na největší mýty kolem Copilota a ukážeme vám jasná fakta, abyste se mohli lépe rozhodovat.

Vyvracíme mýty o AI



Q Dostanou se k našim důvěrným dokumentům kolegové?

A **Ne.** Copilot vždy respektuje stávající nastavení oprávnění v Microsoft 365 ve vaší firmě. Každému uživateli zobrazuje pouze ty dokumenty a informace, ke kterým už má přístup (například na SharePointu). Pokud tedy nemáte právo do určitého dokumentu nahlížet, Copilot vám ho nenabídne. Stejně tak se k vašim důvěrným dokumentům nemohou dostat ani ostatní kolegové – ať už interní, nebo externí.

Q Nedostanou se data nějak k naší konkurenci?

A **Ne.** Copilot vidí jen to, co mu v rámci Microsoft 365 dovolíte. Zároveň pracuje v uzavřeném prostředí vaší firmy. Vaše data tak zůstávají v bezpečí a k jiným organizacím ani ke konkurenci se nedostanou.

Q Budou se na našich datech z Copilota trénovat další AI modely?

A **Ne.** Microsoft 365 Copilot sice využívá vaše e-maily nebo dokumenty, aby vám mohl pomáhat, ale dělá to v zabezpečeném prostředí Microsoft 365. Vaše dotazy, odpovědi ani firemní data se k učení AI modelů nikdy nepoužívají. Všechno vaše know-how tak zůstává v bezpečí.



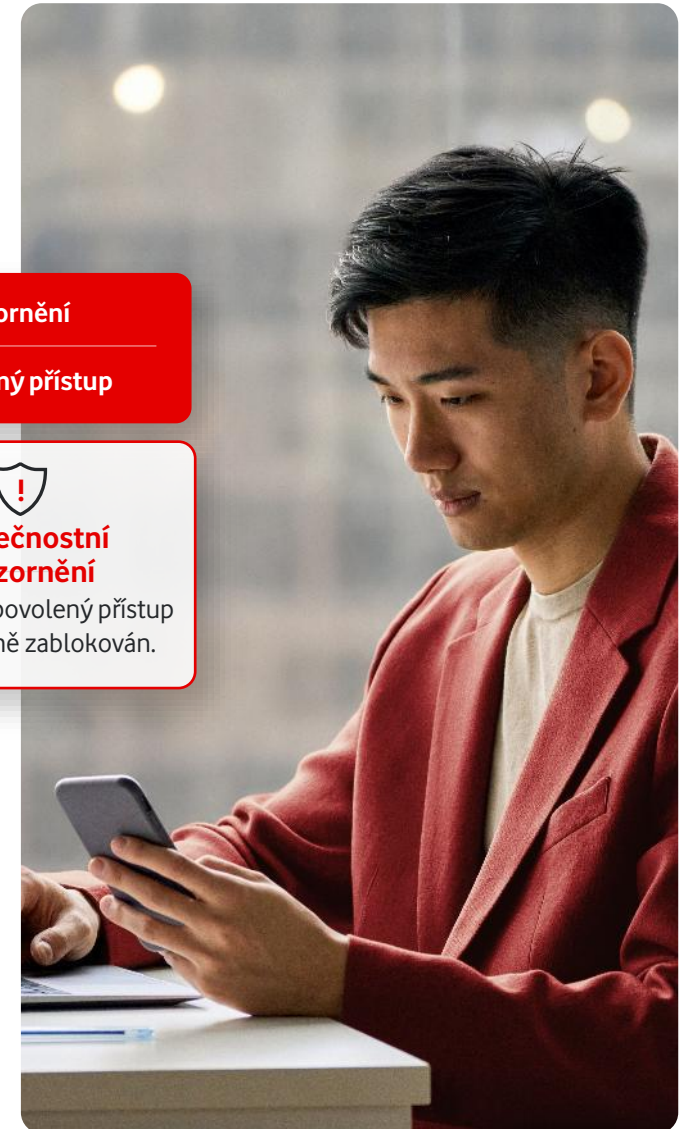
 **Upozornění**

Nepovolený přístup



Bezpečnostní upozornění

Pokus o nepovolený přístup byl úspěšně zablokován.



Q Můžeme Copilota používat, i když pracujeme s citlivými finančními údaji našich zákazníků?

A **Ano.** Microsoft 365 Copilot má hned několik vrstev ochrany, takže je vhodný i pro přísně regulovaná odvětví. K ochraně citlivých finančních údajů využívá systém šifrování a izolaci dat. Obsahuje mechanismy, které blokují škodlivý obsah a brání zneužití informací. AI dokáže detekovat chráněný materiál, což Microsoft garantuje svým závazkem k ochraně autorských práv zákazníků. Díky vestavěnému řízení přístupu a funkcím monitorování se k citlivým datům dostanou pouze autorizovaní uživatelé.

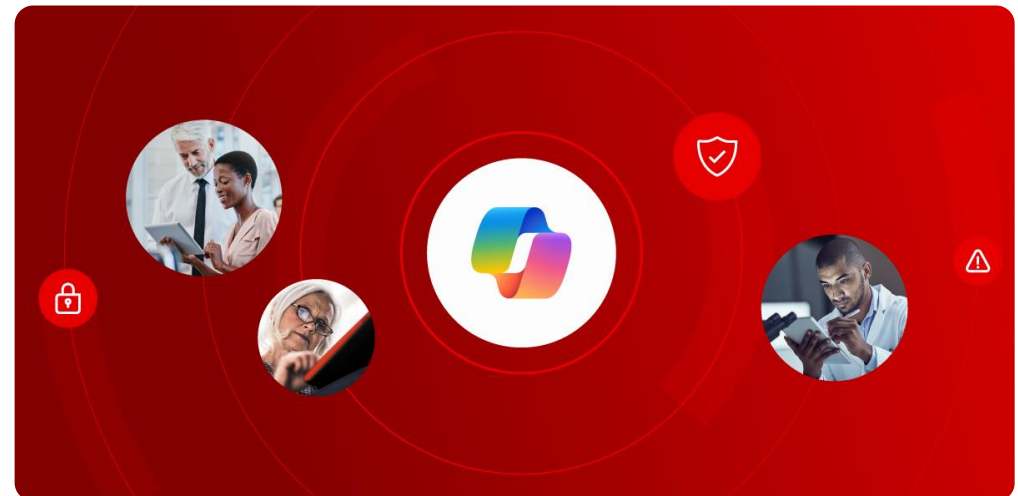
Q Můžeme sledovat, jak se Copilot používá, a prohlížet si historii konverzací?

A **Ano.** V Microsoft 365 Copilotu můžete zapnout automatické zaznamenávání každé interakce uživatelů do auditních protokolů, tzv. logů. Ty vám zobrazí, kdo nástroj použil, kdy a odkud a také ke kterým souborům a zdrojům přistupoval. Tyto záznamy jsou dostupné skrze nástroje jako Microsoft Purview. Vaše organizace tak může snadno monitorovat aktivitu, kontrolovat konverzace z pohledu interních pravidel a shody s předpisy a včas odhalit jakékoli chování v rozporu s pravidly, nevhodný jazyk nebo podezřelé zacházení s daty.

Q Je chat v Microsoft 365 Copilotu bezpečný?

A **Ano.** Firemní verze chatu v rámci Copilota využívá robustní bezpečnostní infrastrukturu Microsoftu, která splňuje ty nejpřísnější firemní nároky. Celé řešení je plně v souladu s nastavením zabezpečení, které už v rámci Microsoft 365 používáte. Systém má bezpečnostní pojistky a šifrování, které chrání vaše data před neoprávněným přístupem. Součástí jsou inteligentní filtry, které automaticky detekují a blokují škodlivý obsah. A to vše plně v souladu s certifikacemi ISO i nařízením GDPR.

Vaše prompty i odpovědi zůstávají v bezpečí v rámci organizace. Nesdílí se s nikým zvenčí a nepoužívají se ani k trénování základního AI modelu Copilota.



Q Může AI vyzradit data našich zákazníků?

A Ne, pokud AI používáte správně a s dobře nastavenými kontrolními mechanismy.

Bezpečnostní riziko většinou pramení ze špatných návyků, jako je zadávání citlivých informací do neschválených nástrojů – tato praktika se nazývá shadow AI. Tento pojem označuje situace, kdy se jednotlivci nebo týmy registrují a používají veřejně dostupné AI asistenty či neoficiální doplňky bez vědomí nebo schválení firmy, což pak vede k absolutní ztrátě přehledu a kontroly nad tím, s jakými informacemi a daty tyto nástroje vlastně pracují a kde tato data končí.

Q Je etické používat AI?

A Ano. Velký důraz se klade hlavně na to, jak se umělá inteligence vyvíjí, nasazuje a následně spravuje. Používání AI s sebou nese velkou zodpovědnost, zejména pokud jde o férovost, transparentnost, udržitelnost a jasné vymezení odpovědnosti. Mnoho organizací proto už dnes vytváří vlastní etické kodexy a vnitřní pravidla, aby tyto hodnoty v praxi skutečně zajistily.

Sám Microsoft si na zodpovědném přístupu k AI zakládá. A protože se technologie i postupy v oblasti AI neustále posouvají dopředu, budou se i tyto strategie dál vyvíjet a přizpůsobovat tak, aby etické používání zůstalo prioritou i v budoucnu.



Q Jak zvládnout zavádění AI bez velkých nároků na IT?

A Existuje hned několik způsobů, jak zavést AI do provozu, aniž by vás to stálo příliš mnoho času a peněz:

Začněte malými kroky

Místo abyste AI nasadili všude najednou, zaměřte se nejdříve na pár oddělení, např. na marketing, obchod, zákaznický servis nebo finance. Potom vyberte jednu či dvě oblasti, kde bude mít AI viditelný přínos, ale představuje nízké riziko. Může jít o automatizaci části zákaznické péče, shrnování dlouhých dokumentů pro lepší přehlednost nebo analýzu dat a tvorbu reportů.

Využívejte low-code/no-code AI platformy

Většina AI platforem dnes nevyžaduje vývoj na míru ani složitou integraci. Nástroje jako Copilot lze obvykle začít plošně využívat s minimálním zapojením IT týmu, zvláště pokud je lze jednoduše integrovat do systémů, které už používáte.

Vsadte na cloudové nástroje

Cloudová AI dokáže ulehčit práci IT oddělení. Hledejte dodavatele, kteří nabízejí podporu, špičkové zabezpečení a propojení s vaším prostředím.





Q Jak zajistíme bezpečnost firmy?

A Při práci s AI modely (jako je Microsoft 365 Copilot, ChatGPT nebo Gemini) v podstatě uplatňujete stejné bezpečnostní zásady, jaké už máte nastaveny pro ostatní pracovní nástroje. Typicky jde o tyto kroky:

- Stanovte srozumitelné pokyny, jak se má AI v rámci firmy používat.
- Důsledně hlídejte a omezujte přístup k citlivým informacím.
- Využívejte nástroje pro monitoring, detekci hrozeb a automatická varování.
- Školte zaměstnance, aby věděli, jak rozpoznat potenciální hrozby, jak se jim vyhnout a komu je nahlásit.
- Vybírejte si pouze prověřené a spolehlivé poskytovatele.



Q Potřebujeme k zavedení Copilota pomoc specialistů?

A **Ne nutně.** Vše závisí na tom, jak velká je vaše firma, jak složitá může být samotná implementace a jak moc si v této oblasti věříte. Odborná podpora vám pomůže s úspěšným zavedením do provozu tak, aby vám toto řešení dlouhodobě přinášelo výsledky.

Pořízení Copilota u Vodafone Business pro vás znamená spolupráci s důvěryhodným partnerem, který vás provede kompletním zavedením od A do Z. To vše bezpečně a spolehlivě díky naší globálně sdílenému know-how a podpoře certifikovaných expertů.

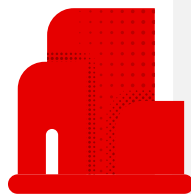


Q Můžeme používat Microsoft 365 Copilot, i když pracujeme v silně regulovaném prostředí?

A **Ano.** Microsoft 365 Copilot je navržen tak, aby vyhovoval potřebám organizací i v regulovaných sektorech, jako jsou finance, zdravotnictví nebo státní správa. Staví na stejných bezpečnostních základech jako ostatní komerční služby Microsoftu a automaticky přebírá pravidla a nastavení, která už vaše firma používá.

Copilot splňuje také požadavky GDPR, závazky v rámci **EU Data Boundary** i **certifikace ISO/IEC 27001 a 27018**.

Copilot se navíc integruje s Microsoft Purview, takže máte na jednom místě k dispozici nástroje pro prevenci úniku dat, ochranu informací i auditní záznamy v přehledné a jednotné platformě.



Q Je Copilot v souladu s GDPR?

A **Ano.** Podle GDPR musí všechny systémy využívající AI splňovat přísné bezpečnostní standardy, které chrání citlivá data a brání neoprávněnému přístupu. Vývojáři AI nesou odpovědnost za to, že se tyto požadavky skutečně dodržují. V případě Copilota vystupuje Microsoft v roli zpracovatele osobních údajů. Jeho smluvní závazky ke splnění požadavků GDPR jsou definovány v dokumentu Data Protection Addendum (DPA). Microsoft tak zpracovává osobní údaje pouze vaším jménem a s odpovídajícími ochrannými opatřeními.



Q Je Copilot bezpečnější než ChatGPT?

A **Ano.** U veřejně dostupných AI nástrojů, jako je třeba ChatGPT, se model učí přímo na uživatelských datech. To znamená, že jakékoli citlivé údaje nejsou v soukromí a jsou vystaveny riziku. Microsoft 365 Copilot má bezpečnostní opatření zabudované už v samotném základu. Vaše prompty, odpovědi i data zůstávají uzavřené ve firemním prostředí. Vše probíhá v naprostém souladu s předpisy.



Využijte potenciál Microsoft 365 Copilota naplno

Mýty o bezpečnosti a soukromí brání firmám, aby naplno využily potenciál a skutečné výhody, které nástroje jako Microsoft 365 Copilot nabízejí, ať už jde o efektivitu provozu, spokojenost lidí, správu rozpočtů, nebo celkový růst. Proověřené nástroje disponují několika úrovněmi ochrany, díky čemuž jsou vhodné pro firmy všech velikostí i oborů, a to včetně přísně regulovaných odvětví, jako jsou finance, zdravotnictví nebo státní správa.

Vaše soukromé konverzace a chaty zůstanou bezpečně uvnitř organizace. Zároveň získáte jistotu, že každá interakce s AI splňuje vaše vnitrofiremní standardy pro správu dat, bezpečnost i shodu s předpisy.

Pořídte si licenci Microsoft 365 Copilot od Vodafone Business a začněte využívat možností umělé inteligence naplno.

Pokud se chcete naučit využívat Copilota a další aplikace Microsoft 365 tak, aby vám skutečně pomáhaly v každodenní práci, je tu pro vás naše **edukační platforma SkillUp.**

