ChatGPT a firemné dáta: Čo je bezpečné a čo už nikdy nezadávať do AI

6.7.2026 - | COMTEC

V roku 2026 používa generatívnu AI väčšina kancelárskych pracovníkov. ChatGPT, Microsoft Copilot či Gemini už nie sú experimentom, ale bežným pracovným nástrojom. To však prináša nový problém: zamestnanci do AI kopírujú e-maily, zmluvy, cenové ponuky aj osobné údaje zákazníkov bez toho, aby si uvedomovali bezpečnostné dôsledky. Otázka dnes už neznie, či AI používať. Otázka znie, ako ju používať bezpečne.

Čo sa v článku dozviete

- · Ktoré informácie nikdy nevkladať do ChatGPT
- · Ako vytvoriť interné pravidlá používania AI
- · Aké možnosti ponúkajú Enterprise AI riešenia
- · Aké požiadavky prinášajú AI Act a GDPR
- · Ako nastaviť AI tak, aby pomáhala a neohrozovala firmu

AI je nový zamestnanec. Dali by ste mu prístup ku všetkému?

Veľa zamestnancov vníma ChatGPT ako inteligentný vyhľadávač. V skutočnosti ide o externú cloudovú službu, do ktorej používateľ vedome odosiela údaje.

Predstavte si, že nastúpi nový brigádnik. Je šikovný, rýchly a pomáha s každou úlohou. Ale nik ho nekontroloval, nik s ním nepodpísal NDA a všetko, čo mu poviete, môže zdieľať ďalej. **Pristupovali by ste k nemu rovnako ako k preverenému kolegovi?**

Práve preto by mala firma pristupovať ku generatívnej AI podobne ako ku každému ďalšiemu dodávateľovi IT služieb – s jasnými pravidlami, nie len dobrou vôľou.

Otázka dnes už neznie, *či* AI používať. Otázka znie, *ako* ju používať bezpečne.

Čo zamestnanci nikdy nemajú zadávať do AI

Typ údajov	Prečo je to riziko
Zmluvy	Obchodné tajomstvo
Cenové ponuky	Konkurenčná výhoda
Zdrojové kódy	Duševné vlastníctvo
Databázy zákazníkov	GDPR
Rodné čísla	Osobné údaje
Prihlasovacie údaje a heslá	Kompromitácia systémov

Typ údajov	Prečo je to riziko
Interné smernice	Know-how firmy
Finančné výsledky	Dôverné informácie
API kľúče	Prístup k systémom

Najčastejšia chyba vo firmách

Nie je to samotné používanie ChatGPT. Je to **kopírovanie celých e-mailových vlákien**.

Typický scenár: Zamestnanec chce nechať AI vylepšiť odpoveď zákazníkovi. Napíše prompt:

„Napíš lepšiu odpoveď zákazníkovi.“

A do správy vloží celé vlákno vrátane:

mena zákazníkatelefónuadresyčísla objednávkyinterných poznámokreklamačného procesu
 Riešenie je jednoduché Všetky tieto informácie pritom nie sú na text odpovede vôbec potrebné. Stačí údaje anonymizovať – nahradiť meno zákazníka za „zákazník“, číslo objednávky za „č. obj. XY“. AI funguje rovnako dobre, ale firemné dáta zostávajú vo firme.

Verejná AI vs Enterprise AI: zásadný rozdiel

Nie všetky verzie ChatGPT fungujú rovnako. Z pohľadu bezpečnosti je rozdiel obrovský:

Osobné účty (Free, Plus)

- Dáta môžu byť použité na trénovanie
- Žiadna firemná správa používateľov
- Žiadny audit log
- Nevhodné na firemné použitie

Enterprise verzie (Team, Enterprise, Copilot, Gemini for Workspace)

- Dáta sa nepoužívajú na trénovanie
- Šifrovanie dát
- Správa používateľov a rolí
- Audit logy – kto, kedy, čo
- SSO napojenie na firemné identity
- Zmluvné záruky ochrany dát (DPA)

Ak zamestnanci používajú osobné ChatGPT účty na firemné úlohy, firma nemá žiadnu kontrolu, žiadne záruky a žiadne záznamy. Enterprise verzia to mení – a jej cena je zlomok potenciálnych škôd.

AI Act mení pravidlá – aj pre malé firmy

Väčšina slovenských článkov túto časť vynecháva. V roku 2026 už firmy riešia povinnosti z európskeho nariadenia **AI Act**, ktoré nadobúda účinnosť postupne.

Čo to v praxi znamená:

1. 1**AI gramotnosť zamestnancov**Firmy musia zabezpečiť, aby zamestnanci rozumeli AI nástrojom, ktoré používajú – nielen ako ich ovládať, ale aj aké riziká prinášajú.
2. 2**Interné pravidlá používania AI**Zdokumentované, nie len ústne dohody. Firma musí vedieť preukázať, že pravidlá existujú a zamestnanci ich poznajú.
3. 3**Dokumentácia rizík**Evidencia AI systémov používaných vo firme a ich potenciálnych dopadov na zamestnancov, zákazníkov a procesy.
4. 4**Transparentnosť**Zákazníci musia vedieť, ak s nimi komunikuje AI – napríklad chatbot, automatická odpoveď alebo AI-generovaný obsah.

 Nie každá firma je „high-risk“ Ale prakticky každá organizácia, ktorá AI používa, by mala mať základné pravidlá – aj len preto, aby sa vedela preukázať pri audite, kontrole alebo riešení incidentu.

Interná AI smernica: základ, bez ktorého sa nezaobídete

Toto je najhodnotnejšia vec, ktorú môže firma pre bezpečné používanie AI urobiť. AI smernica nemusí mať 50 strán – musí odpovedať na niekoľko základných otázok:

 Aké AI nástroje sú povolené?
 Kto ich môže používať?
 Aké dáta je možné zadávať?
 Aké dáta sú zakázané?
 Ako anonymizovať údaje pred vložením do AI?
 Kto schvaľuje nové AI nástroje?
 Ako sa rieši bezpečnostný incident?
 Ako sa evidujú AI aplikácie vo firme?

Firma, ktorá má túto smernicu, je v inej pozícii pri audite, pri GDPR kontrole aj pri riešení incidentu. Firma bez nej sa len spolieha na to, že sa nič nestane.

Pravidlo 3 farieb: jednoduchý návod pre každého zamestnanca

Ak chcete ľuďom vysvetliť, čo môžu a nemôžu zadávať do AI bez toho, aby si museli pamätať 10 pravidiel – toto funguje.

Zelené – možno zadávať priamo

- Všeobecné otázky a vyhľadávanie
- Marketingové texty a copywriting
- Anonymizované dokumenty

- □ Brainstorming a návrhy

□Žlté – najprv anonymizovať, potom zadať

- → E-maily (odstrániť mená, kontakty, interné čísla)
- → Cenové ponuky (odstrániť meno klienta a hodnoty)
- → Zápisy z porád (odstrániť mená a citlivé informácie)
- → Analýzy projektov (anonymizovať klienta)

□Červené – nikdy nezadávať

- □ Osobné a zdravotné údaje zákazníkov
- □ Zdrojové kódy a databázy
- □ Zmluvy s klientmi
- □ Heslá a API kľúče
- □ Obchodné tajomstvá a finančné výsledky

Ako používať AI bezpečne: konkrétne odporúčania

- →**Používajte firemné AI účty** namiesto súkromných – nikdy osobný ChatGPT na firemné úlohy
- →**Anonymizujte dokumenty** pred vložením do AI
- →**Využívajte Enterprise verzie** nástrojov s ochranou dát
- → Nastavte **viacfaktorové overenie** pre prístup k AI nástrojom
- →**Školte zamestnancov** – nie jednorazovo, ale pravidelne
- →**Pravidelne aktualizujte AI smernicu** – AI sa vyvíja rýchlo, pravidlá musia držať krok
- →**Kontrolujte výstupy AI človekom** – AI robí chyby, ktoré nerozozná sama

AI nenahrádza zodpovednosť

Aj keď AI vytvorí text, analýzu alebo návrh riešenia, zodpovednosť za správnosť, zákonnosť a ochranu údajov zostáva na firme. Pred zákazníkom, pred regulátorom aj pred súdom.

Preto by mal byť každý výstup AI primerane overený človekom – nie zaslaný bez kontroly priamo zákazníkovi, na web alebo do zmluvy.

Najčastejšie otázky

Je ChatGPT vo firme bezpečný? +

Záleží od toho, akú verziu a ako ho zamestnanci používajú. Osobné účty (Free, Plus) nie sú vhodné na firemné použitie s citlivými dátami. ChatGPT Team alebo Enterprise verzia ponúka zmluvné záruky, zákaz trénovania na vašich dátach a správu používateľov.

Čo je to AI Act a týka sa nás? +

AI Act je európske nariadenie, ktoré reguluje používanie umelej inteligencie. Väčšiny malých a stredných firiem sa netýka ako „high-risk“ prevádzkovateľov, ale základné povinnosti – ako AI gramotnosť, dokumentácia a transparentnosť – platia pre každú firmu, ktorá AI využíva.

Ako anonymizovať dáta pred vložením do AI? +

Nahraďte konkrétne mená zákazníkov za „zákazník“, čísla objednávok za generické označenia, finančné hodnoty za zástupné sumy. Adresu, telefón a e-mail z textu jednoducho vymažte. AI funguje rovnako dobre – ale vaše dáta zostávajú len u vás.

Musíme zakázať ChatGPT zamestnancov? +

Nie – a zákaz väčšinou nefunguje. Zamestnanci budú AI používať aj naďalej, len bez vedomia firmy. Efektívnejší prístup je nastaviť jasné pravidlá, poskytnúť schválené nástroje a vzdelávať ľudí o tom, čo môžu a čo nesmú zadávať.

Kto zodpovedá za chyby AI vo firemnom výstupe? +

Vždy firma – nie AI nástroj. Za správnosť, zákonnosť a ochranu údajov vo výstupoch zodpovedá organizácia, ktorá ich používa a zverejňuje. Preto je ľudská kontrola každého AI výstupu nevyhnutná.

Záver

Najväčším rizikom nie je samotný ChatGPT. Najväčším rizikom je, keď zamestnanci používajú AI bez pravidiel – každý inak, každý s inými dátami, každý bez vedomia, kde tieto dáta končia.

Správne nastavené interné smernice, školenia a vhodne zvolené AI nástroje umožnia firmám využívať výhody umelej inteligencie bez zbytočného ohrozenia obchodného tajomstva či osobných údajov.

Neviete, či vaša firma používa AI bezpečne?

Bezplatný audit kybernetickej bezpečnosti vám ukáže, kde sú vaše dáta a aké riziká hrozia – vrátane Shadow AI a nepovolených nástrojov.

Chcem bezplatný audit →

Alebo sa pozrite na naše služby:

Kybernetická bezpečnosť → Komplexná správa IT →

https://comtec.sk/novinky/chatgpt-firemne-data-bezpecnost