Shadow AI aneb nový strašák zaměstnavatelů (a HR oddělení)

Shadow AI se stává jedním z největších právních a bezpečnostních rizik současných firem. Zaměstnanci využívají generativní AI často bez vědomí zaměstnavatele a do veřejných nástrojů přitom mohou vkládat osobní údaje, důvěrné dokumenty i obchodně citlivé informace. Jaké povinnosti z toho vyplývají podle GDPR, AI Actu a pracovního práva a jak na novou situaci reagovat v praxi? Podrobně se tématu věnuje Barbara Roubíčková z advokátní kanceláři Borovec legal v následujícím článku.

Všimli jste si v poslední době, že vaši zaměstnanci najednou píší e-maily jako vystřižené z novin? Jejich výstupy působí, jako by je připravoval člen Akademie věd, nebo naopak obsahují až překvapivé množství smajlíků a bullet pointů? Je dost možné, že se i ve vaší společnosti projevuje fenomén tzv. Shadow AI (používání AI zaměstnanci bez jasných pravidel, kontroly nebo schválení zaměstnavatele[1)]).

Zaměstnanci dnes používají nástroje generativní AI rychleji, než na to stíhají reagovat interní pravidla společností. Podle globální studie KPMG z roku 2025 téměř každý druhý zaměstnanec nahrává do veřejných AI nástrojů citlivé firemní informace, včetně finančních dat, zákaznických údajů nebo materiálů chráněných autorským právem[2)].

Ukazuje se, že samotné zákazy používání AI nejsou efektivním řešením a že klíčovou otázkou se stává praktické nastavení interních pravidel. Tento článek se proto zaměřuje na specifické právní aspekty fenoménu Shadow AI a jejich (možné) řešení.

AI a GDPR

Personalista vloží životopis uchazeče do ChatGPT a požádá o vytvoření pořadí kandidátů. Za několik vteřin získá přehledný výstup, avšak aniž by si to musel nutně uvědomit, předal tímto osobní údaje třetí osobě – poskytovateli AI. Stejně tak se lze setkat s předáváním osobních údajů poskytovateli AI při přípravě hodnocení zaměstnanců, analýze e-mailové komunikace nebo zpracování interních dokumentů.

Právě na takových situacích lze ilustrovat jeden z největších problémů Shadow AI – ochranu osobních údajů.

Je zřejmé, že je při využívání AI nutné dodržovat základní pravidla GDPR, na která jsme za dobu působnosti nařízení GDPR již zvyklí. V souvislosti se Shadow AI je však třeba věnovat pozornost aspektu, který bývá často přehlížen – pravidlům pro **zapojení třetích osob do zpracování osobních údajů** – na které GDPR výslovně pamatuje.

Pokud totiž osobní údaje zpracovává jiný subjekt než správce, tedy zaměstnavatel, musí být jejich vztah zpravidla upraven zpracovatelskou smlouvou.

Zpracovatelská smlouva by měla vymezovat například účel a dobu zpracování, kategorie zpracovávaných údajů, další práva a povinnosti smluvních stran nebo požadavky na zabezpečení osobních údajů. Její součástí by měl být též závazek mlčenlivosti osob, které se

na zpracování podílejí.

Právě zde naráží Shadow AI na jeden z největších praktických problémů. U velkého množství běžně používaných AI nástrojů (např. neplacená verze ChatGPT či Microsoft Copilot) totiž není možné zpracovatelskou smlouvu uzavřít (případně zaměstnavatel ani netuší, že zaměstnanci takový nástroj používají). Riziko lze částečně snížit anonymizací nebo pseudonymizací údajů před jejich vložením do AI. To nicméně není ideální řešení tohoto problému.

Na trhu však existují i AI nástroje určené pro firemní prostředí, které požadavky GDPR zohledňují. Příkladem může být Microsoft 365 Copilot nebo podnikové verze Google Workspace, u nichž bývá zpracovatelská smlouva součástí smluvní dokumentace a které současně nabízejí možnost vyšší úrovně zabezpečení dat.

Důležitým krokem zaměstnavatele je proto z pohledu GDPR výběr vhodných AI nástrojů určených pro firemní prostředí, které nabízejí odpovídající smluvní záruky a ochranu dat. Pokud zaměstnavatel poskytne zaměstnancům bezpečnou alternativu, výrazně se snižuje motivace využívat neschválené veřejně dostupné AI.

AI a důvěrné informace

Rizika spojená se Shadow AI zdaleka nekončí u ochrany osobních údajů. Zaměstnanci totiž do AI nástrojů často nevkládají pouze životopisy nebo údaje o zaměstnancích, ale také smlouvy, cenové nabídky, vnitřní předpisy, obchodní strategie, právní stanoviska atd.

Typickým příkladem může být zaměstnanec, který požádá generativní AI o revizi smlouvy, vytvoření obchodní nabídky nebo přípravu prezentace pro významného klienta. Aby získal co nejpřesnější výstup, zpravidla do systému vloží celý dokument včetně důvěrných informací.

U veřejně dostupných AI nástrojů však uživatel zpravidla nemá plnou kontrolu nad tím, jak se bude s vloženými informacemi či dokumenty dále nakládat. V závislosti na konkrétním poskytovateli mohou být zadaná data například analyzována za účelem zlepšování služby nebo použita pro účely „trénování" AI (další zlepšování modelu AI).

Problematické je především to, že zaměstnanci si tato rizika často neuvědomují. Na rozdíl od klasického předání dokumentu třetí osobě působí komunikace s AI jako běžná práce s počítačem. Uživatel tak může snadno získat dojem, že informace neopouštějí jeho pracovní prostředí, přestože ve skutečnosti dochází k jejich zpřístupnění externímu poskytovateli služby.

Právě proto by zaměstnavatelé měli řešit i otázku nastavení pravidel pro práci s důvěrnými informacemi při využívání AI. Součástí interních pravidel by mělo být zejména vymezení údajů, které je možné do AI nástrojů zadávat, a naopak informací, které musí zůstat výhradně uvnitř společnosti. Míra tohoto rizika se přitom opět významně liší podle konkrétního AI nástroje.

AI v HR

Z pohledu HR je v neposlední řadě třeba zmínit, že se budeme stále častěji setkávat s AI nástroji určenými přímo pro HR agendu. Již dnes existují systémy schopné automaticky vyhodnocovat životopisy, třídit kandidáty, analyzovat výsledky pohovorů nebo pomáhat s další administrativou spojenou s náborem a řízením lidských zdrojů.

Právě v této souvislosti nabývá na významu evropské nařízení o umělé inteligenci (AI Act), které postupně nabývá účinnosti. To totiž považuje některé AI systémy používané v oblasti zaměstnání za tzv. vysoce rizikové systémy. Jedná se zejména o systémy využívané při náboru zaměstnanců, výběru uchazečů, rozhodování o povýšení, přidělování pracovních úkolů nebo hodnocení výkonnosti[3)].

Důvodem je skutečnost, že rozhodnutí učiněná nebo ovlivněná AI mohou mít zásadní dopad na život jednotlivců. Nevhodně nastavený systém může například znevýhodňovat určité skupiny uchazečů nebo vést k netransparentnímu rozhodování o zaměstnancích.

Používání těchto AI systémů je spojeno s řadou povinností. Zaměstnavatelé musí zejména zajistit odpovídající lidský dohled nad fungováním AI systému a neměli by se spoléhat výhradně na automatizované výstupy. Rozhodnutí s významným dopadem na zaměstnance nebo uchazeče by měla být vždy podrobena lidskému posouzení.

Současně je třeba zajistit dostatečnou transparentnost vůči osobám, kterých se použití AI týká. Uchazeči o zaměstnání nebo zaměstnanci by měli být informováni o tom, že při určitých procesech dochází k využívání AI.

AI Act dále klade důraz na kvalitu vstupních dat, průběžné monitorování fungování systému a vedení dokumentace o jeho používání. Zaměstnavatelé by proto měli být schopni doložit, jakým způsobem byl konkrétní AI nástroj využíván a jaká opatření byla přijata k omezení rizik diskriminace nebo chybných rozhodnutí.

Ačkoli většina povinností AI Actu dopadá primárně na poskytovatele vysoce rizikových AI systémů, ani zaměstnavatelé využívající tyto nástroje nezůstávají bez odpovědnosti. Právě oni totiž budou v praxi čelit důsledkům případných např. diskriminačních rozhodnutí nebo nedostatečné transparentnosti vůči zaměstnancům a uchazečům o zaměstnání.

Pro úplnost je vhodné doplnit, že na výstupy AI systémů se nadále vztahují obecné pracovněprávní předpisy, zejména zákaz diskriminace a povinnost rovného zacházení podle:

- zákoníku práce;
- zákona o zaměstnanosti; a
- antidiskriminačního zákona.

Skutečnost, že určité doporučení nebo hodnocení vytvořila AI, sama o sobě zaměstnavatele nezbavuje odpovědnosti za výsledné rozhodnutí.

Často zmiňovaným příkladem v této souvislosti je projekt jedné americké společnosti, která vyvíjela AI nástroj pro vyhodnocování životopisů. Ukázalo se však, že systém znevýhodňoval ženy. Důvod byl poměrně jednoduchý – algoritmus byl trénován na historických datech, která odrážela dlouhodobou převahu mužů. Systém se tak naučil upřednostňovat charakteristiky typické pro dříve úspěšné kandidáty a naopak znevýhodňovat některé životopisy obsahující například slovo „ženské".

Výše uvedený příklad dobře ukazuje, že AI nemusí být ze své podstaty objektivní. AI systémy se učí z historických dat, která mohou obsahovat lidské předsudky nebo nerovnosti. Právě z tohoto důvodu AI Act klade v případě vysoce rizikových systémů důraz na lidský dohled, transparentnost a průběžné vyhodnocování rizik.

Zaměstnavatel by proto neměl nekriticky přebírat doporučení generovaná AI, ale vždy posuzovat, zda nejsou výsledky zatíženy systematickou chybou nebo diskriminačním dopadem na určité skupiny zaměstnanců či uchazečů o zaměstnání.

Jak by měli zaměstnavatelé reagovat?

Jak vyplývá z výše uvedeného, většina rizik spojených se Shadow AI nevzniká proto, že by zaměstnanci chtěli porušovat právní předpisy nebo ohrozit zájmy zaměstnavatele. Ve většině případů jde spíše o důsledek nedostatečné informovanosti zaměstnanců a absence jasných pravidel pro využívání AI na pracovišti.

1. Identifikujte veškeré AI systémy

Prvním krokem by proto mělo být zjištění:

- jaké AI nástroje zaměstnanci skutečně používají;
- k jakým účelům je využívají; a–
- jaké informace do nich zadávají.

Bez této základní analýzy nelze účinně posoudit související právní ani bezpečnostní rizika.

Následně je vhodné jednotlivé AI systémy posoudit z hlediska jejich rizikovosti a ověřit, zda jejich používání nevyžaduje splnění dalších povinností podle GDPR, AI Actu nebo jiných právních předpisů. V některých případech může být nezbytné provést také posouzení vlivu na ochranu osobních údajů (DPIA) nebo přijmout další technická a organizační opatření.

2. Připravte interní směrnici

- Klíčovým nástrojem pro omezení rizik je dále přijetí interní směrnice upravující používání AI. Ta by měla obsahovat zejména:
- seznam schválených AI nástrojů (případně nástrojů zakázaných);
- pravidla pro práci s osobními údaji, obchodním tajemstvím a dalšími důvěrnými informacemi;
- požadavky na anonymizaci nebo pseudonymizaci dat; a
- pravidla pro lidský dohled nad výstupy umělé inteligence.

Součástí směrnice by mělo být také vymezení odpovědnosti zaměstnanců za porušení stanovených pravidel a nastavení interních procesů pro zavádění nových AI systémů do společnosti. Zaměstnanci by měli vědět nejen jaké nástroje mohou používat, ale také na koho se obrátit v případě pochybností nebo při posuzování nových AI řešení.

3. Proškolte zaměstnance

Ani sebelepší interní pravidla však nebudou fungovat bez odpovídajícího proškolení zaměstnanců.

V praxi by školení nemělo být zaměřeno pouze na technické ovládání jednotlivých nástrojů. Zaměstnanci by měli rozumět také tomu:

- jaké údaje mohou do AI systémů zadávat;
- kdy je nutné údaje anonymizovat nebo pseudonymizovat;
- jaká rizika jsou spojena s využíváním veřejně dostupných AI nástrojů; a
- jaké důsledky může mít porušení interních pravidel nebo právních předpisů.

Stejně důležité je pochopení limitů AI, včetně rizika nepřesných, zavádějících nebo diskriminačních výstupů.

POZOR: Význam školení není pouze otázkou dobré praxe. AI Act ukládá (a to již s účinností od 2. 2. 2025!) zaměstnavatelům povinnost přijmout opatření k zajištění dostatečné úrovně AI gramotnosti osob, které AI systémy používají. Pokud jste tak tedy dosud neučinili, je načase.

4. **Průběžně kontrolujte**

Vzhledem k rychlému vývoji technologií i právní úpravy v tomto odvětví by zaměstnavatelé neměli zapomínat ani na průběžnou kontrolu souladu používaných AI systémů s právními předpisy. To platí zejména s ohledem na postupné nabývání účinnosti AI Actu a očekávaný vývoj právních požadavků v následujících letech.

Shadow AI totiž nepředstavuje problém samotné AI. Je především důsledkem situace, kdy zaměstnanci začnou nové technologie používat rychleji, než na ně dokáže reagovat vnitřní nastavení organizace. Úkolem zaměstnavatelů proto není AI zakazovat, ale vytvořit prostředí, ve kterém ji lze využívat tak, aby zaměstnavatel nebyl vystaven rizikům.

Zdroj: Premiové články 7/2026