

Odklad AI Actu firmy uklidnil. Kvůli Shadow AI přitom porušují povinnosti už dnes

Od neděle 2. srpna se začala uplatňovat další důležitá část evropského AI Actu, která se týká transparentnosti. Firmy si sice po červnovém odkladu části pravidel oddechly, ale většina z nich stále podceňuje rizika takzvané Shadow AI. Fenoménu, kdy zaměstnanci potají využívají veřejné nástroje umělé inteligence a vkládají do nich firemní know-how či osobní údaje. Advokát Michal Nulíček z ROWAN LEGAL upozorňuje, že se tím firmy dostávají do paradoxní pozice oběti i pachatele: data vynese zaměstnanec, případnou pokutu však zaplatí zaměstnavatel.

Pod označením Shadow AI se skrývá poměrně běžná a stále rozšířenější praxe, kdy zaměstnanci používají veřejně dostupné AI nástroje, jako jsou ChatGPT, Gemini nebo Claude, bez vědomí a souhlasu zaměstnavatele. Motivace bývá často nevinná – snaha zvýšit efektivitu nebo si ulevit od rutiny. Důsledky takového počínání však mohou být závažné, protože do nástrojů se mohou nekontrolovaně dostat firemní know-how, informace o maržích, zdrojové kódy či osobní údaje zákazníků nebo zaměstnanců.

Zaměstnanci si toto riziko často neuvědomují. Shadow AI se přitom týká prakticky každé firmy, v níž se pracuje s počítači nebo mobilními telefony. Průzkum UpGuard z listopadu 2025 zjistil, že až 80 % zaměstnanců při práci využívá neschválené AI nástroje. KPMG zase ve vlastní studii ze stejného roku dospěla k závěru, že 57 % zaměstnanců používání těchto nástrojů aktivně tají. Nejvíce jsou tímto fenoménem ohroženy společnosti působící v oblasti IT, vývoje, marketingu, práva, daní a poradenství.

Legislativní balík EU Digital Omnibus, který v červnu definitivně schválily Evropský parlament i Rada EU, sice odložil účinnost části pravidel pro vysoce rizikové AI systémy, rozhodně to však není důvod k oddechu. „*Firmy si po červnovém odkladu části pravidel AI Actu oddechly. Nesmějí ale přehlížet, že každá firma, kde lidé potají používají AI nástroje bez jakýchkoli pravidel, porušuje právní předpisy už dnes,*“ komentuje přehlížený paradox **Michal Nulíček, advokát a partner ROWAN LEGAL specializující se na ochranu osobních údajů**. Od letošního 2. srpna se navíc začala uplatňovat většina zbývajících pravidel AI Actu.

Problematické je, že přestože know-how nebo osobní údaje vynáší zaměstnanec, právně za jeho jednání odpovídá firma – jako správce osobních údajů podle GDPR, smluvní strana dohody o mlčenlivosti i povinný subjekt podle AI Actu. „*Na Shadow AI je zrádné, že firma je zároveň obětí i pachatelem. Know-how vynese zaměstnanec, který chtěl jen ušetřit čas, ale pokutu za únik osobních údajů nebo porušení NDA zaplatí zaměstnavatel,*“ dokresluje **Michal Nulíček**. Firmám navíc hrozí souběh sankcí vyplývajících z AI Actu i GDPR. Regulovaným subjektům jako jsou finanční instituce navíc i podle dalších předpisů.

Takové případy se již objevují v domácí i zahraniční praxi. Ústavní soud loni v prosinci udělil advokátovi pořádkovou pokutu 25 tisíc korun za stížnost, v níž argumentoval z podstatné části neexistující judikaturou vygenerovanou umělou inteligencí. Většina incidentů se navíc řeší v rámci interních procesů, takže veřejně zmapované případy představují pouze pomyslnou špičku ledovce.

Asi největší poprask vyvolala v roce 2023 kauza jihokorejské technologické společnosti Samsung, jejíž inženýři vložili do bezplatné verze ChatGPT citlivé zdrojové kódy, které se tak dostaly mimo kontrolu firmy. Samsung v návaznosti na incident zakázal svým zaměstnancům používat veřejně dostupné AI nástroje pod hrozbou výpovědi. *„Není to teoretické riziko. Instinktivní reakce řady firem je zavést plošný zákaz AI nástrojů, to ale není příliš šťastné. Zákaz je totiž prakticky obtížně vymahatelný a uživatele jen nažene hlouběji do šedé zóny. Jediná funkční cesta je dát lidem schválený a bezpečný nástroj a naučit je s ním pracovat,“* doplňuje další z odborníků na ochranu osobních údajů kanceláře ROWAN LEGAL **Filip Beneš**.

Řada firem proto musí s ohledem na tuto realitu zavést bezpečné komerční verze AI nástrojů se smluvními zárukami pro nakládání s daty, přijmout interní AI politiku jasně vymezující, jaká data do nástrojů nepatří, a proškolit zaměstnance. Podle **Michala Nulíčka** je vhodným prvním krokem anonymní audit, který managementu ukáže, jaké nástroje zaměstnanci nejčastěji používají. *„Další užitečnou formou může být samotné školení, kde se v otevřenější atmosféře zaměstnanci spíše rozmluví o konkrétních nástrojích, které v praxi reálně využívají,“* dodává **Filip Beneš**.

Regulatorní tlak však bude nadále sílit. Legislativním procesem v Česku zároveň prochází adaptační zákon o umělé inteligenci, podle něhož bude dozor nad dodržováním pravidel vykonávat primárně Český telekomunikační úřad a v oblasti ochrany osobních údajů Úřad pro ochranu osobních údajů. Firmy, které Shadow AI dosud neřešily, by proto měly reagovat dříve, než je na nesoulad s pravidly upozorní regulátor nebo zákazník. A to vše bez ohledu na AI Act, protože pravidla, která je třeba dodržovat, platí již podle stávajících regulací a pokuty za neoprávněné nakládání s citlivými informacemi a osobními údaji hrozí už dnes.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Firmy čekají na rok 2027, první povinnosti podle CRA ale přichází už teď v září. Dopadají i na produkty, které už jsou na trhu](#)
- [Karin Pomaizlová posiluje IP tým Brichta & Partners jako Senior Counsel](#)
- [Aliance Horizons rozšiřuje svoji působnost do Slovinska a Bosny a Hercegoviny](#)
- [Heureka v přelomovém sporu s Googlem vysoudila před prvostupňovým soudem přes 400 milionů korun. Zastupovala ji advokátní kancelář ROWAN LEGAL](#)
- [V prvním pololetí zaznamenala skupina HAVEL & PARTNERS tržby 815 milionů korun](#)
- [Změny v AML legislativě: co přinese nová evropská a česká úprava](#)
- [JUDr. Lucia Šoralová posílila tým bpv BRAUN PARTNERS](#)
- [Katrin Vydržel novou advokátkou Aegis Law](#)
- [Žádná teorie, jen praxe: Zaposlouvejte se do nové podcastové série Na ROWinu od ROWAN LEGAL](#)
- [Vyloučení položek z koupě části závodu aneb kde leží hranice možného vylučování majetku a dluhů z převodu](#)
- [Zkušený advokát Radek Matušek posiluje ROWAN LEGAL](#)