AI a minimální povinná výbava pro firmy

– TEXT – Dalibor Kovář – FOTO – Havel & Partners

Řada firem zavádí umělou inteligenci rychleji, než si stihnou zodpovědět otázku, kdo za ni interně odpovídá. Sledují pečlivě regulaci, ale vnitřní pravidla, procesy a jasně přiřazená odpovědnost související s užíváním AI ve firmě chybí… Jaké je za mě jako právníka základní minimum, na co v rámci AI governance ve firmě dbát?



Nasazením umělé inteligence se odpovědnost ve firmě nepřenáší na technologii ani na jejího dodavatele. Péče řádného hospodáře totiž vyžaduje jednat informovaně a s potřebnou pečlivostí a přehlížení rizik může znamenat i osobní odpovědnost vedení – členů statutárních orgánů. Sankce podle AI Actu mohou dosáhnout až 35 milionů eur nebo sedm procent celosvětového obratu.

Jak tedy nastavit funkční pravidla? Prvním krokem je inventura. Nelze řídit riziko, o kterém nevíte, a skutečný rozsah používání umělé inteligence bývá výrazně širší, než si ve vedení připouštíte. Shadow AI, tedy používání veřejně dostupných nástrojů bez vědomí zaměstnavatele, přitom zpravidla nevzniká ze snahy obcházet pravidla.

Zaměstnanci si zvykli využívat AI pro shrnutí textů, překlady či analýzu dokumentů často ještě z doby, kdy jim firma nenabízela žádnou schválenou alternativu. Pravděpodobně nevíte, kdo jaký nástroj používá, jaké informace do něj vkládá, kde jsou data uložena a zda mohou být využita k trénování modelů. Nejcitlivější jsou osobní údaje zákazníků a zaměstnanců, důvěrná klientská data, obchodní tajemství nebo zdrojový kód.

Zmapujte tedy detailně, jaké nástroje se u vás používají, kým, s jakými daty a od jakého dodavatele. Nabídněte zaměstnancům bezpečnou a použitelnou alternativu, podnikové verze nástrojů s odpovídajícími smluvními a bezpečnostními garancemi. A upozorněte na možné nesprávné pracovní návyky, které ohrožují vaši společnost.

Čtyři kroky k vnitřní governance

Vnitřní governance nemusí být od počátku dokonalá, musí však existovat a být otevřená dalším úpravám. Za minimální výbavu považuji čtyři prvky. Prvním je interní směrnice pro používání AI. Osvědčuje se princip semaforu. Jasně vymezte, které použití je volné, které vyžaduje schválení a které je vyloučeno. Každý zaměstnanec musí vědět, do které kategorie jeho práce spadá.

Dalším důležitým prvkem jsou pravidla pro nakládání s daty. Ve firmě potřebujete vymezit informační perimetr, tedy kategorie dat od veřejných přes interní a důvěrná až po jinak chráněná, a určit, která data smějí opustit firemní prostředí a která naopak ne. U osobních údajů a informací krytých mlčenlivostí rozhodně neplatí zásada, že co není zakázáno, je dovoleno.

Nabídněte zaměstnancům bezpečnou a použitelnou alternativu, podnikové verze nástrojů s odpovídajícími smluvními a bezpečnostními garancemi.

Skutečný rozsah používání umělé inteligence bývá výrazně širší, než si ve vedení připouštíte.

Za třetí si nastavte i schvalovací proces pro nové AI projekty či systémy. Postačí jednoduché pravidlo: kdo nasazení schvaluje a co přesně se před ním posuzuje.

A jako čtvrtý bod by neměla chybět ani pravidla pro dodavatele. Značná část stávajících smluv na AI nástroje nezohledňuje požadavky regulace. Začněte licenčními a SaaS smlouvami na samotné AI nástroje, pokračujte zpracovatelskými smlouvami podle GDPR a smlouvami s IT dodavateli a externími poskytovateli služeb, kteří AI zabudovávají do vašich systémů nebo s ní pracují s vašimi daty. A ověřte, zda vám smlouvy s klienty vůbec dovolují jejich data v AI nástrojích zpracovávat. Prohlášení dodavatele o souladu vás totiž nezbavuje vlastní odpovědnosti – za to, jak AI používáte a jaká data do ní vkládáte, odpovídá vaše firma.

Stejně jako se stalo ve firmách standardem řízení kybernetické bezpečnosti nebo ochrany osobních údajů, mělo by se stát standardem i řízení umělé inteligence.

Autor je partnerem Havel & Partners

inzerce



Zorientujte se
v záplavě informací
s tištěným Ekonomem
každý čtvrtek

Předplaťte si
papírový Ekonom přímo
do vaší schránky.

