IUSTORIA
Advokátní kancelář

telefon: (+420) **777 366 857**
email: info@iustoria.cz
web: www.iustoria.cz

Použití GPAI pro specifický, např. vysoce rizikový účel

AI Act striktně rozlišuje mezi obecným modelem (GPAI) a konkrétním AI systémem, který je nasazen pro specifický účel.

Odpovědnost se tak rozděluje v řetězci. Zde je podrobný rozklad:

1. Nástroj sám o sobě: ChatGPT jako GPAI s omezeným rizikem

Samotný model ChatGPT, když ho používáte pro obecné účely (psaní e-mailů, brainstorming, překlady), je považován za **GPAI (model s obecným účelem)**. V základní rovině na něj dopadají povinnosti transparentnosti, které jsme již zmínili (technická dokumentace, souhrn dat, autorské právo).

Pokud by byl navíc vyhodnocen jako GPAI se systémovým rizikem (což GPT-4 a novější modely jsou), má jeho poskytovatel (OpenAI) další povinnosti (testování, hlášení incidentů atd.).

Důležité ale je, že OpenAI neuvádí na trh "Nástroj pro hodnocení životopisů". Poskytuje pouze obecnou technologii.

2. Aplikace pro rizikový účel: Hodnocení životopisů jako vysoce rizikový systém

V momentě, kdy jakákoli firma (např. HR oddělení nebo softwarová společnost) vezme technologii ChatGPT (např. přes API) a vytvoří z ní nástroj, jehož **zamýšleným účelem je nábor zaměstnanců nebo rozhodování o jejich povýšení**, tento konkrétní systém se stává **vysoce rizikovým AI systémem** podle Přílohy III AI Actu.

A v tuto chvíli se těžiště odpovědnosti přesouvá.

Kdo je za co zodpovědný?

Použijme skvělou analogii: **motor a auto.**

1. **Poskytovatel GPAI (OpenAI) je jako výrobce motoru.**
    - Jeho povinností je dodat motor (model GPT-4) s **technickou dokumentací a manuálem**. Musí v něm jasně popsat výkon motoru, jeho spotřebu, limity a **instrukce pro bezpečné použití** (např. "Tento model může halucinovat" nebo "Není trénován na datech po roce 2023 a může mít skryté předsudky").
    - OpenAI není přímo zodpovědné za to, že si někdo vezme jejich motor a postaví z něj nebezpečné auto bez brzd. Jejich rolí je poskytnout všechny potřebné informace, aby se bezpečné auto postavit dalo.

2. **Provozovatel vysoce rizikového systému (HR firma) je jako výrobce auta.**
    - Tato firma bere motor (GPT-4) a zabudovává ho do auta (nástroj na hodnocení životopisů). Tím se stává **poskytovatem vysoce rizikového AI systému**.
    - **Na tuto firmu dopadají všechny přísné povinnosti pro vysoce rizikové systémy:**
        - **Systém řízení rizik:** Musí identifikovat a zmírnit rizika (např. riziko diskriminace na základě pohlaví, věku nebo etnika).
        - **Správa dat:** Musí zajistit, že data použitá pro případné doladění (fine-tuning) jsou kvalitní a bez předsudků.
        - **Lidský dohled:** Musí navrhnout systém tak, aby finální rozhodnutí dělal vždy člověk, a aby mohl efektivně zasáhnout a opravit chyby AI.
        - **Přesnost, robustnost a kybernetická bezpečnost:** Musí zajistit, že systém funguje spolehlivě a je bezpečný.
        - **Posouzení shody a certifikace CE:** Před uvedením na trh musí projít procesem posouzení, zda splňuje všechny požadavky, a označit svůj produkt značkou CE.

Co to znamená v praxi?

Pokud vaše firma chce používat ChatGPT pro hodnocení životopisů, nemůže se zbavit odpovědnosti s tím, že "to dělá ChatGPT". Musí:

1. **Vytvořit interní proces:** Definovat, jak bude nástroj používán. Bude to jen pro první třídění? Pro kontrolu gramatiky? Nebo pro samotné bodování kandidátů?
2. **Zajistit lidský dohled:** Každý životopis, který AI označí jako nevhodný, musí být zkontrolován člověkem. Finální rozhodnutí nesmí být nikdy plně automatizované.
3. **Testovat na diskriminaci:** Firma by měla aktivně testovat, zda systém nezvýhodňuje nebo nediskriminuje určité skupiny lidí.
4. **Informovat kandidáty:** Uchazeči o zaměstnání mají právo vědět, že pro hodnocení jejich žádosti byl použit AI systém.

Závěr: AI Act elegantně řeší tento problém tím, že **odpovědnost klade na toho, kdo AI systém uvádí na trh nebo do provozu pro konkrétní, vysoce rizikový účel**. Obecný nástroj může mít nízké riziko, ale jeho konkrétní nasazení v citlivé oblasti (jako je zaměstnávání) spouští úplně novou sadu přísných pravidel a povinností pro toho, kdo jej takto nasazuje.