UNIVERZA V LJUBLJANI | PF Pravna fakulteta

KCUI

Kompetenčni center za umetno inteligenco

Slovenian National AI Competence Centre

Uporaba generativne umetne inteligence in modelov umetne inteligence za splošne namene

Lovro Bobnar
Inštitut za primerjalno pravo pri Pravni fakulteti v Ljubljani;
Univerza v Ljubljani, Pravna fakulteta

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE IN JAVNO UPRAVO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN MLADINO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSTVO DELO IN ŠPORT

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

ARRS

Uporaba generativne umetne inteligence in modelov UI za splošne namene

Od uporabe že izdelanega orodja do razvoja lastnega modela

Ključno vprašanje: kaj podjetje dejansko počne z modelom?

Uporabljam orodje

- Zaposleni pri delu uporabljajo že pripravljeno generativno rešitev, ki jo zagotavlja zunanji ponudnik. Podjetje modela ne razvija in ga ne vključuje v lasten produkt.

Gradim aplikacijo

- V lasten produkt, storitev ali aplikacijo vključim model drugega ponudnika ter ga uporabim kot osnovo za svojo rešitev.

Ponujam model

- Razvijem model UI za splošne namene (GPAI) ali obstoječi model pomembno spremenim ter ga pod svojim imenom zagotavljam na trgu.

Model ni isto kot sistem

To razlikovanje je izhodišče za razumevanje nadaljnjih obveznosti po Aktu o UI.

MODEL UI ZA SPLOŠNE NAMENE

- **»Motor« rešitve:** model, ki je usposobljen na veliki količini podatkov, izkazuje znatno splošnost ter lahko kompetentno opravlja širok nabor različnih nalog. Tak model se lahko vključi v različne sisteme ali aplikacije.
- **Primer:** jezikovni model, ki lahko povzema besedila, odgovarja na vprašanja, prevaja, ustvarja vsebine in piše programsko kodo.

SISTEM UI

- **»Avtomobil« oziroma konkretna rešitev:** sistem, v katerem je model povezan z uporabniškim vmesnikom, navodili, podatki, dodatnimi funkcionalnostmi in po potrebi drugimi programskimi komponentami za doseganje določenega namena.
- **Primer:** pomočnik za podporo strankam, ki uporablja jezikovni model in je povezan z dokumentacijo ter podatkovnimi viri podjetja.

Pomembno:

- generativnost opisuje, kaj model ali sistem počne – ustvarja besedilo, slike, zvok ali druge vsebine.
- **Model UI za splošne namene (GPAI) pa je pravna kategorija modela po Aktu o UI.**

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

Isto podjetje – tri različne (pravne) vloge

Primer: IKT-podjetje želi z uporabo generativne umetne inteligence izboljšati podporo strankam. Njegova pravna vloga je odvisna od tega, **kako tehnologijo uporablja in kaj daje na trg**.

A Uporabi pripravljeno orodje
Zaposleni uporabljajo obstoječo generativno rešitev.
Vloga: praviloma uvajalec sistema.
Posledica: samo zaradi uporabe podjetje ne postane ponudnik GPAI

B Vgradi tuj model
Podjetje prek API-ja vključi model drugega ponudnika v svojega pomočnika.
Vloga: ponudnik lastnega sistema; ponudnik modela ostane ločen.
Posledica: obveznosti iz 53. člena se na integratorja ne prenesejo avtomatično.

C Ponudi lasten model
Podjetje razvije ali naroči razvoj GPAI in ga trži pod svojim imenom.
Vloga: ponudnik GPAI, lahko tudi ponudnik sistema.
Posledica: neposredne obveznosti V. poglavja.

Isti model lahko pomeni različne pravne vloge – odvisno od tega, kaj podjetje z njim počne.

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

Kaj pomeni izraz »prilagajamo model«?

Navodila, RAG in fine-tuning niso ista stvar.

PROMPTING

- Modelu z navodili določimo, **kako naj odgovarja**.
- **Primer:** »Odgovarjaj kratko in samo na podlagi pravilnika.«
- Parametri modela se praviloma **ne spreminjajo**.

RAG

- Sistem poišče relevantne dokumente in jih modelu doda kot **kontekst za pripravo konkretnega odgovora**.
- Če parametri generativnega modela ostanejo nespremenjeni, RAG sam po sebi praviloma **ne pomeni dodatnega učenja modela**.

FINE-TUNING

- Model se dodatno uči na izbranih podatkih, pri čemer se spremenijo njegovi **parametri ali druge učljive komponente**.
- Potrebna je presoja **obsega in učinkov spremembe**.

Smernice Evropske komisije: pri pomembnejših spremembah je treba presoditi, ali prilagajalec postane **ponudnik spremenjenega modela UI za splošne namene**.

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

Štiri osrednje obveznosti ponudnikov modelov UI za splošne namene

Akt o UI določa štiri ločene obveznosti za različne namene in naslovnike

1. Tehnična dokumentacija
Opis razvoja, učenja, preskušanja in vrednotenja modela.
Namen: predvsem omogočiti nadzor in preverjanje skladnosti.

2. Informacije za ponudnika sistema UI, ki model vključuje v svoj sistem
Informacije, ki jih potrebuje ponudnik sistema, da lahko model ustrezno vključi v svoj sistem UI.

3. Politika skladnosti z avtorskim pravom
Politika za zagotavljanje skladnosti z avtorskim pravom EU, vključno s spoštovanjem pridržkov pravic.

4. Javni povzetek učnih vsebin
Dovolj podroben javni povzetek vsebin, uporabljenih za učenje modela, pripravljen po predlogi Urada za UI.

Pomembno: tehnična dokumentacija ≠ informacije za ponudnika sistema UI, ki model vključuje v svoj sistem ≠ javni povzetek.

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

Kaj mora vedeti podjetje, ki vgrajuje tuj model?

Informacije, ki jih mora zagotoviti ponudnik modela

- predvidene naloge, zmogljivosti in omejitve modela
- pogoji uporabe in licenčne omejitve
- tehnične zahteve za integracijo
- vrste, značilnosti in omejitve vhodov ter izhodov
- relevantne informacije o podatkih za učenje, testiranje in validacijo

Dodatno je smiselno pogodbeno urediti

- obveščanje o novih različicah in pomembnih spremembah modela
- ali in za katere namene se naši podatki uporabljajo za nadaljnje učenje
- podporo pri napakah, incidentih in motnjah delovanja
- razmejitev odgovornosti ter možnosti zamenjave ponudnika

Dve posebnosti: odprta koda in sistemsko tveganje

ODPRTOKODNI MODELI UI ZA SPLOŠNE NAMENE

- **Akt o UI v drugem odstavku 53. člena** določa delno izjemo za določene odprtokodne modele.
- Če so izpolnjeni pogoji glede licence ter javne dostopnosti parametrov, informacij o arhitekturi in uporabi modela, se obveznosti iz **člena 53(1)(a) in (b)** ne uporabljajo.
  - Ta izjema ne velja za modele UI za splošne namene s sistemskim tveganjem.
- **Ostaneta:** politika skladnosti z avtorskim pravom in javni povzetek učnih vsebin.

MODELI UI ZA SPLOŠNE NAMENE S SISTEMSKIM TVEGANJEM

- Za modele UI za splošne namene s sistemskim tveganjem velja **dodatni režim iz členov 51–55**.
- Dodatno med drugim:
  - vrednotenje modela in adversarial testing
  - ocenjevanje in zmanjševanje sistemskih tveganj
  - spremljanje in poročanje o resnih incidentih
  - ustrezna raven kibernetske zaščite

Pomembno: model UI za splošne namene s sistemskim tveganjem ni isto kot **visokotvegani sistem UI po 6. členu Akta o UI**.

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

Pet ključnih vprašanj pred uporabo modela UI za splošne namene

Kateri model in katero različico uporabljamo?
Ali poznamo izvor modela, njegovo različico in pogoje uporabe?

Kdo je ponudnik modela in kakšna je naša pravna vloga?

Ali model le uporabljamo, ga vključujemo v svoj sistem ali ga ponujamo naprej?

Kaj pri modelu dejansko spreminjamo ali prilagajamo?

Gre za prompting, RAG, fine-tuning ali drugo spremembo modela?

Katere informacije, licence in pravice imamo na voljo?

Ali imamo dovolj informacij za integracijo ter ustrezne pravice glede uporabe modela in podatkov?

Kako bomo spremljali spremembe, delovanje in incidente?

Kdo spremlja nove različice, spremembe pogojev, napake in morebitne resne incidente?

UNIVERZA V LJUBLJANI | PF Pravna fakulteta

KCUI

Hvala za pozornost!

Lovro Bobnar
lovro.bobnar@pf.uni-lj.si

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE IN JAVNO UPRAVO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN MLADINO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSTVO DELO IN ŠPORT

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

ARRS

Gospodarska zbornica Slovenije

Chamber of Commerce and Industry of Slovenia

KCUI

Vprašanja in odgovori

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE IN JAVNO UPRAVO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN MLADINO

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSTVO DELO IN ŠPORT

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

apis