Gospodarska zbornica Slovenije
Chamber of Commerce and Industry of Slovenia

KCUI
Kompetenčni center za umetno inteligenco
Slovenian National AI Competence Centre

Praktična klasifikacija UI rešitev glede na tveganje po Aktu o UI

asist. Jernej Renko, mag. prav., LL.M.

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
ARIS

Kaj bo predmet obravnave?

Zakaj je klasifikacija ključna?

- Klasifikacija določa obveznosti in kazni za njihovo neupoštevanje

Piramida tveganj po Aktu o UI

- 4 stopnje: prepovedano, visoko, omejeno, minimalno

Kriteriji za visoko tveganje

- Čl. 6(1): vgradnja v regulirane produkte & Čl. 6(2): 8 sektorjev iz Priloge III

Izvzetje iz režima visokega tveganja

- Derogacija po čl. 6(3) in 4 pogoji – kdaj so izpolnjeni?

Omejeno tveganje: le obveznosti v povezavi s transparentnostjo

- Chatboti, generativna UI, deep fakes (čl. 50)

Primeri in dileme iz IKT prakse

- HR screening, chatboti, CCTV, kreditno ocenjevanje…

Gospodarska zbornica Slovenije
Chamber of Commerce and Industry of Slovenia

Zakaj je klasifikacija ključna?

Obveznosti glede na kategorijo

Prepovedane prakse UI – nesprejemljivo tveganje

Absolutna prepoved od 2.2.2025

Visoko tveganje

Sistem za obvladovanje tveganj, vodenje evidenc, človeški nadzor, preglednost, točnost, robustnost, kibernetska varnost,, CE znak, registracija v EU bazi, FRIA, nadzor...

Omejeno tveganje

Samo razkritje npr.: “komunicirate z UI”

Minimalno tveganje oz. ni tveganj

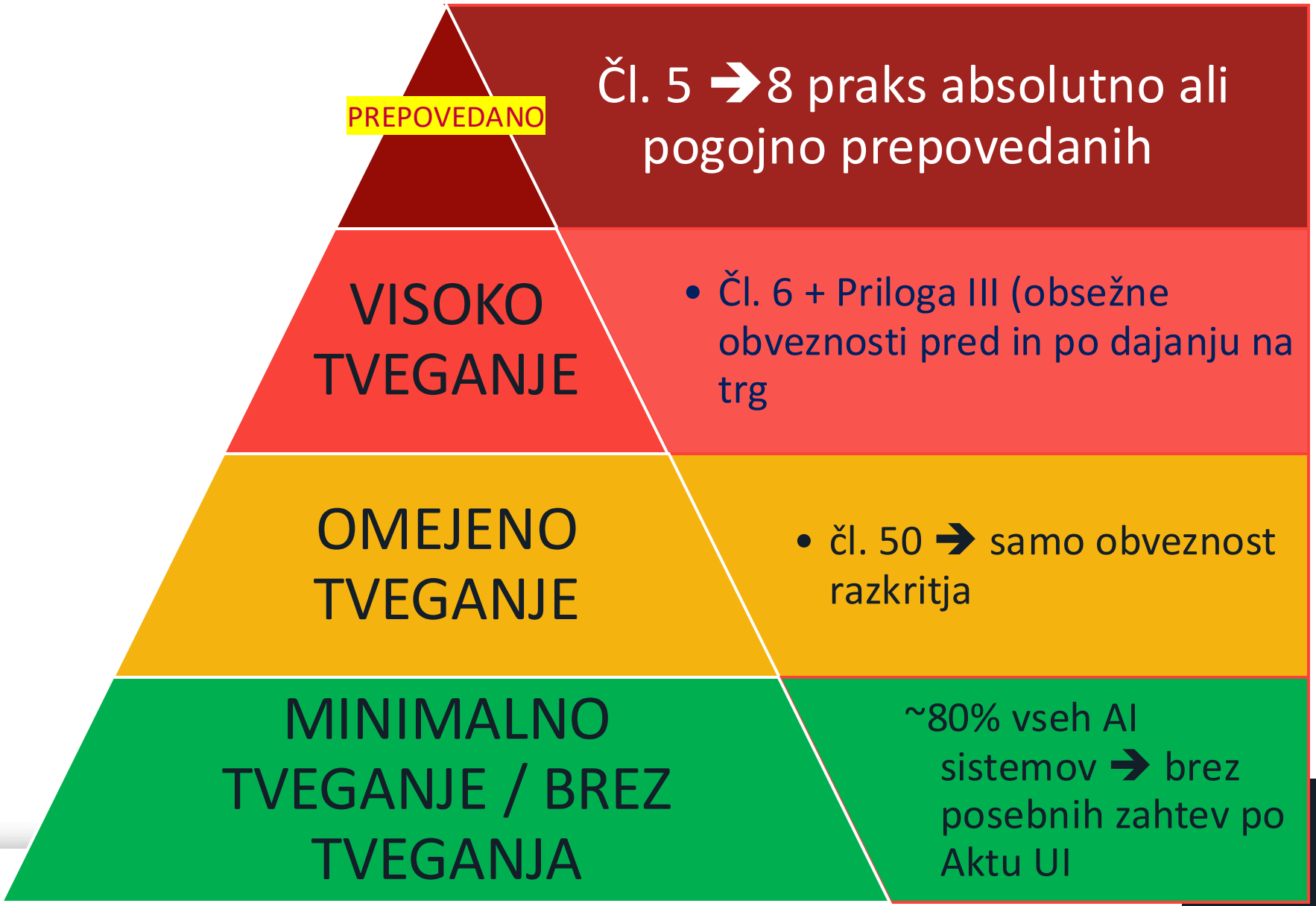
Nobenih posebnih zahtev po Aktu o UI

Visoke kazni

35 mio € / 7% prometa	15 mio € / 3% prometa	7,5 mio € / 1% prometa
Kršitev prepovedi (čl. 5)	Neizpolnjevanje zahtev za visoko tvegane UI sisteme	Napačne informacije nadzornemu organu

Gospodarska zbornica Slovenije
Chamber of Commerce and Industry of Slovenia

Praktična klasifikacija UI rešitev glede na tveganje po Aktu o UI



Od 2.2. 2025

2. 12. 2027 za sisteme UI iz Priloge III

2. 8. 2028: UI vgrajena v proizvode

Od 2. 8. 2026

Kdaj je UI sistem visoko tvegan?

POT 1 – Čl. 6(1): Vgrajeni v regulirane proizvode

Pogoja (oba hkrati):

1. AI sistem je varnostna komponenta proizvoda ali je sam proizvod, zajet v Prilogi I (stroji, medicinski pripomočki, vozila, dvigala, radijska oprema…)
2. Za ta proizvod je s sektorsko zakonodajo zahtevana ocena skladnosti s harmonizacijske zakonodajo s strani tretje osebe (organa)

Primeri: UI v medicinskih napravah, v sistemih za nadzor vozil, v industrijskih strojih

POT 2 – Čl. 6(2): Delovanje v 8 občutljivih sektorjih

Priloga III – 8 sektorjev

1. Biometrika
2. Kritična infrastruktura
3. Izobraževanje in poklicno usposabljanje
4. Zaposlovanje
5. Bistvene storitve (krediti, zdravstvo..)
6. Kazenski pregon in postopek
7. Migracije in azil, nadzor meje
8. Pravosodje in demokratični procesi

Pokriva tveganja za temeljne pravice in ne le zdravje/varnost

Gospodarska zbornica Slovenije
Chamber of Commerce and Industry of Slovenia

8 sektorjev visokega tveganja – Priloga III

Biometrika

UI primeri: Daljinska biometrična identifikacija, prepoznava čustev

IKT: Sistemi za prepoznavo obrazov, analiza glasu, sistemi vstopa na podlagi biometrike

Bistvene in javne storitve

UI primeri: Kreditna ocena, zdravstvene ugodnosti, zavarovalne premije

IKT: AI za kreditno ocenjevanje, sistemi za oceno zavarovalnih tveganj

Kritična infrastruktura

UI primeri: Varnostne komponente za upravljanje prometa, vode, energije

IKT: AI za nadzor energetskih omrežij, sistemi upravljanja prometnih tokov

Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj

UI primeri: Ocena tveganja, profiliranje osumljencev, poligraf

IKT: AI za analizo vzorcev kriminala, sistemi za identifikacijo osumljenih

Izobraževanje in poklicno usposabljanje

UI primeri: Dostop do šolanja, ocenjevanje, zaznavanje prevar na testih

IKT: AI sistemi za preverjanje pristnosti pisnih del, avtomatizirano ocenjevanje

Migracije in azil

UI primeri: Ocena varnostnih tveganj, obdelava vlog

IKT: AI za obdelavo vlog za vizume, sistemi za upravljanje meje

Zaposlovanje/upravljanje delavcev in dostop do samozaposlitve

UI primeri: Rekrutiranje, razporeditev nalog, vrednotenje delavcev

IKT: AI za razvrščanje življenjepisov, sistemi za ocenjevanje videoposnetkov razgovorov

Pravosodje in demokratični procesi

UI primeri: Podpora sodiščem, vplivanje na volitve

IKT: AI za pregled pravnih dokumentov v kazenskih postopkih, sistemi za politično oglaševanje

6

Kdaj sistem kljub sektorju NI visoko tvegan?

Člen 6(3) – derogacija: sistem ni visoko tvegan, če:
(a) ne predstavlja znatnega tveganja za zdravje, varnost ali temeljne pravice, IN
(b) ne vpliva bistveno na izid odločitve, TER velja EN od naslednjih 4 pogojev:

a

Omejena postopkovna naloga

Sistem opravlja zgolj ozko opravilo – npr. razvrščanje dokumentov, iskanje duplikatov, indeksiranje

Primer: UI za razvrščanje pogodb po vrsti v odvetniški pisarni

b

Izboljšava predhodno zaključene človeške dejavnosti

UI izboljšuje rezultat človeške dejavnosti, ki je ŽE zaključena, brez vpliva na vsebino

Primer: UI, ki preveri slovnico že napisanega dopisa HR managerja

c

Zaznava vzorcev brez nadomeščanja človeka

UI zazna vzorce/odstopanja za informiranje, ne za nadomeščanje predhodne človeške ocene

Primer: Analitično orodje, ki pokaže anomalije v plačilnih tokovih, odloča pa le revizor

d

Pripravljalna naloga za oceno, ki je pomembna za namene primerov uporabe iz Priloge III

UI opravlja pripravljalno nalogo za podporo človeškim odločitvam – iskanje, sortiranje, prevajanje dokumentov

Primer: UI prevajalnik pravnih dokumentov za sodne postopke (sam ne odloča)

⚠ **POZOR: Sistemi, ki opravljajo profiliranje fizičnih oseb, so VEDNO visoko tvegani – derogacija ne velja! (čl. 6(3), 2. odst.)**

„oblikovanje profilov“ pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;

7

Omejeno tveganje: samo transparentnost

Člen 50 ➔ Velja od 2. avgusta 2026

Čl. 50(1): Interakcija z UI

Kdo: Ponudnik mora vgraditi razkritje

Kaj: Sistem mora obvestiti, da gre za UI

Primer: Chatbot mora povedati: "Sem UI asistent"

Izjema: Razkritje ni potrebno, če je “očitno”, da je fizična oseba v interakciji z UI – npr. industrijski robot

Čl. 50(2): Označevanje sintetične vsebine

Kdo: Ponudniki UI za generiranje slik/videov/besedil

Kaj: Strojno berljive metaoznake v formatu za zaznavanje

Primer: vodni znaki (watermarks), metapodatki v generiranih slikah

Izjema: manjše urejanje, ki bistveno ne spremeni vhodnih podatkov oz. semantike

Čl. 50(4): Deepfakes in sintetična vsebina

Kdo: Uvajalec sistema je zavezan k razkritju

Kaj: Vsebina mora biti označena kot umetno ustvarjena ali prirejena

Primer: UI-generiran video z obstoječo osebo mora nositi opozorilo

Izjema: umetniška dela in satira (z opozorilom na “ustrezen način”, ki ne ovira prikazovanja ali uživanja dela)

Čl. 50(3): Biometrična kategorizacija / čustva

Kdo: Uvajalec sistema

Kaj: Obvestitev izpostavljenih oseb

Primer: klicni center z analizo glasu ugotavlja razpoloženje strank, zato mora stranke o tem obvestiti

Dodatno: upoštevanje zahtev iz GDPR (posebni podatki)

⚠ **POZOR:** Na delovnem mestu in v izobraževanju je prepoznavanje čustev **prepovedano** (čl. 5(1)(f)), razen iz zdravstvenih ali varnostnih razlogov.

Praktični primeri iz IKT prakse

Chatbot za podporo strankam

OMEJENO

Sektor: Splošna storitev

Razlog: Razkritje interakcije z UI (čl. 50(1))

Generativna UI za trženje ali vsebino: dodati označevanje (čl. 50(2))

Kreditni scoring za banko

VISOKO

Sektor: Bistvene storitve (Aneks III)

Razlog: Aneks III, točka 5 – kreditna sposobnost (razen za namene odkrivanje goljufij)

Odkrivanje goljufij je izrecno izvzeto iz te kategorije

UI za razvrščanje prijav za zaposlitev

VISOKO

Sektor: Zaposlovanje (Aneks III)

Razlog: Aneks III, točka 4 – vpliva na dostop do zaposlitve

Izjema: le uvrstitev v map po ključnih besedah brez profiliranja (čl. 6(3)(a))?

UI za samodejno prevajanje pogodb

MORDA NI TVEGANJA

Sektor: Pravosodje (Aneks III)

Razlog: Čl. 6(3)(d): pripravljalna naloga, ne nadomešča pravne ocene

Ključno: ali prevod vpliva na razlago ali le omogoča branje?

UI analiza vedenjskih vzorcev zaposlenih

VISOKO

Sektor: Zaposlovanje (Aneks III)

Razlog: Profiliranje – derogacija čl. 6(3) ne velja!

Profiliranje vedno pomeni visoko tveganje ne glede na obseg naloge

Generativna UI za pisanje poročil

MINIMALNO

Sektor: Splošna raba

Razlog: Noben od 8 sektorjev, ni varnostna komponenta

Označevanje vsebine po čl. 50(2), če je vsebina javna

Dileme in mejni primeri

Pogosta napačna razumevanja

“Naš sistem ima človeka v zanki → ni visoko tvegan”

Napačno! Čl. 6(3) ne velja, če sistem ”bistveno vpliva" na izid. Formalni nadzor ≠ dejanski nadzor.

“Naš sistem je samo za interno rabo → Akt o UI ne velja”

Akt o UI velja za sisteme, dane na trg ali v uporabo v EU, ne glede na to, ali so interne rabe. Izjema: zasebna neposlovna raba.

“Sistem je samo pripomoček, ne odloča → ni visoko tvegan”

Pozor! Pripravljalne naloge (čl. 6(3)(d)) morajo biti RES ozke. Če sistem de facto usmerja človekovo odločitev, je visoko tvegan.

“GPAI model (ChatGPT, Gemini…) ni naš sistem → nimamo obveznosti”

Če na GPAI zgradite lastno rešitev, ste ponudnik tega sistema (čl. 3(3)). Če jo uporabite v kontekstu iz Priloge III, je visoko tvegana.

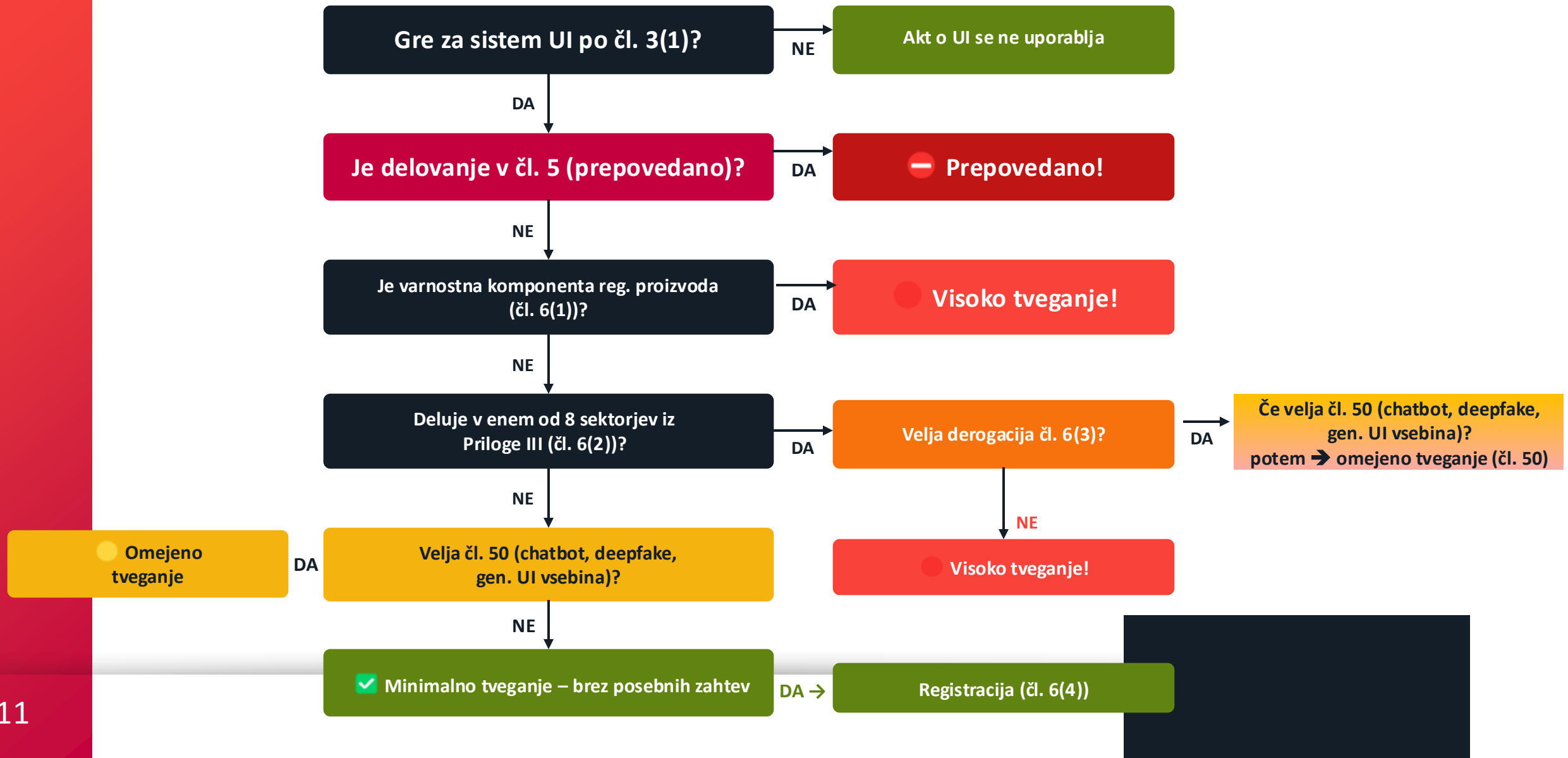
“Akt o UI nas ne zadeva, ker smo le razvijalci”

Napačno! Razvijalci so ponudniki (čl. 3(3)). Prav tako: distributerji in uvozniki lahko postanejo ponudniki (čl. 25).

“Vodja si pri ocenah le pomaga s ChatGPT → to nas ne zadeva”

Pozor! Tipični primer “shadow AI”. Če splošno orodje uporabite za namen iz Priloge III (razvrščanje kandidatov, ocene delavcev), podjetje postane ponudnik visoko tveganega sistema (čl. 25(1)(c)). Rešitev: interna politika rabe UI.

Kako klasificirati UI sistem glede na tveganje?



Ključna sporočila

1. Kategorija tveganja določa VSE – vsak ponudnik in razvijalec mora vedeti, kam spada njegov sistem

2. Čl. 6(3) je izhod, ne vhod – ne iščite razloga za izjemo; najprej ugotovite, ali vaš sistem UI sploh spada med sektorje iz Priloge III

3. Profiliranje predstavlja past – kateri koli sistem, ki izvaja profiliranje fizičnih oseb, je visoko tvegan, ne glede na obseg naloge

4. Chatboti, generativna UI → omejeno, ne visoko – obveznosti glede transparentnosti (čl. 50) veljajo

5. Samoocena prinaša odgovornost – napačna klasifikacija ima lahko za posledice visoke kazni

Hvala za pozornost!

asist. Jernej Renko
mag. prav., LL.M.

jernej.renko@pf.uni-lj.si