UPORABA UMETNE INTELIGENCE: Kakšne so zahteve Akta o umetni inteligenci in varstva osebnih podatkov?

18. Konferenca notranjih revizorjev javnega sektorja Urada RS za nadzor proračuna

dr. Pika Šarf, Vodja področja UI na Informacijskem pooblaščencu

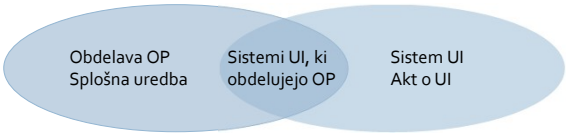
INFORMACIJSKI POOBLAŠČENEC

SOBIVANJE AKTA O UI IN SPLOŠNE UREDBE

Splošna uredba in Akt o umetni inteligenci se uporabljata komplementarno. Akt o umetni inteligenci načeloma ne posega v ureditev Splošne uredbe (dve izjemi: člen 10(5) in člen 59).

Področje urejanja Splošne uredbe Akta o UI in GRPR se prekriva v delu, ki se nanaša na sisteme UI, ki obdelujejo osebne podatke.

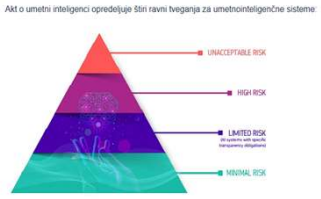
Skladnost z Aktom o UI ne pomeni nujno, da je uporaba sistema UI skladna s Splošno uredbo – in obratno.



PREDMET UREJANJA

- Zahteve, ki izhajajo iz Akta o umetni inteligenci, se nanašajo na **sisteme umetne inteligence.**
- Komplementaren drugim pravnim režimom, npr. varstvu osebnih podatkov, potrošniškem pravu, uredbi o varnosti proizvodov.
- Pristop Akta temelji na **tveganjih**, ki jih predstavlja določen sistem UI za temeljne pravice, zdravje in varnost:
  - prepovedane prakse;
  - visoko tvegani sistemi UI;
  - sistemi UI z omejenimi tveganji;
  - sistemi z nizkimi tveganji;

  + modeli UI za splošne namene.



Večje kot je tveganje, strožja so pravila.

DEFINICIJA SISTEMA UI

Sistem UI pomeni sistem temelječ na napravah, ki je zasnovan za delovanje z različnimi stopnjami avtonomije in lahko po uvedbi izkaže prilagodljivost ter za eksplicitne ali implicitne cilje iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke, kot so napovedi, vsebine, priporočila ali odločitve, ki lahko vplivajo na fizična ali virtualna okolja.

Definicija vsebuje **sedem elementov**:

1. sistem temelječ na napravah,
2. ki je zasnovan za delovanje z različnimi stopnjami avtonomije,
3. lahko po uvedbi izkaže prilagodljivost,
4. za eksplicitne ali implicitne cilje,
5. iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke,
6. kot so napovedi, vsebine, priporočila ali odločitve,
7. lahko vplivajo na fizična ali virtualna okolja.

SMERNICE O DEFINICIJI SISTEMA UI

Smernice Komisije o opredelitvi umetnointeligenčnega sistema, določeni v Uredbi (EU) 2024/1689: https://ec.europa.eu/newsroom/dae/redirection/document/118642

COM: Definicija sistema umetne inteligence **temelji na življenjskem ciklu sistema UI**:

- dve fazi: (1) faza pred uvedbo ali „izgradnja" sistema in (2) fazo po uvedbi ali „ uporabo" sistema;
- ni nujno, da so elementi iz definicije stalno prisotni v obeh fazah tega življenjskega cikla, temveč se določeni elementi lahko pojavijo samo v eni fazi;
- definicija odraža kompleksnost in raznolikost sistemov umetne inteligence ter zagotavlja, da je opredelitev skladna s cilji Akta o umetni inteligenci, saj vključuje širok obseg sistemov UI.

PREPOVEDANE PRAKSE

- Prakse, ki predstavljajo nesprejemljivo tveganje, zato jih ni dovoljeno dajati na trg, dajati v uporabo in uporabljati, na primer:
  - sistemi UI, ki uporabljajo škodljive subliminalne, manipulativne ali zavajajoče tehnike*;
  - sistemi UI za socialno točkovanje*;
  - za ocenjevanje ali napovedovanje tveganja izvršitve kaznivega dejanja*;
  - sistemi UI za prepoznavanje čustev na delovnih mestih in v izobraževalnih ustanovah*.

  ***poenostavljena definicija** - da gre za prepovedano prakso, morajo biti kumulativno izpolnjeni vsi pogoji iz Akta o umetni inteligenci!!

  - Uporaba sistemov UI za biometrično identifikacijo na daljavo v realnem času za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v javno dostopnih prostorih – načeloma prepovedana, lahko pa jo dovoli DČ v nacionalni zakonodaji.
  - Začetek uporabe: **2. februar 2025**

VISOKO TVEGANI SISTEMI UI

PRILOGA I: sistem UI je namenjen uporabi kot varnostna komponenta proizvoda ali pa je sam sistem UI proizvod, ki ga zajema harmonizacijska zakonodaja Unije iz Priloge I, za katerega je treba opraviti ugotavljanje skladnosti s strani tretje osebe zaradi dajanja tega proizvoda na trg ali v uporabo

Primeri: igrače, medicinski pripomočki, osebna varovalna oprema, stroji, plovila

PRILOGA III: med visoko tvegane sodijo nekateri sistemi UI na naslednjih področjih:

1. **biometrija,**
2. kritična infrastruktura,
3. **izobraževanje in poklicno usposabljanje,**
4. zaposlovanje, upravljanje delavcev in dostop do samozaposlitve,
5. uživanje bistvenih zasebnih in javnih storitev in ugodnosti ter dostop do njih,
6. **preprečevanje, odkrivanje in preiskovanje kaznivih dejanj,**
7. **migracije, azil in upravljanje nadzora meje,**
8. **pravosodje in demokratični procesi.**

Začetek uporabe: 2. avgust 2026 (Digitalni omnibus za UI ?)

MEJA MED PREPOVEDANIMI PRAKSAMI IN OSTALIMI SISTEMI UI

- Meja med prepovedanimi praksami in visoko tveganimi sistemi UI (lahko pa tudi ostalimi sistemi UI) je v praksi včasih težko določljiva.
- Primeri:
  - Sistem UI za prepoznavo čustev?
  - Sistem UI za ocenjevanje kreditnih tveganj?
  - Sistem UI za oceno tveganja, da posameznik postane žrtev kaznivega delanja?
  - sistem UI za splošne namene, ki posameznika spodbudi, da neha jemati predpisana zdravila ali se začne prekomerno odrekati hrani ali si vzame življenje?

SMERNICE

- Smernice COM o prepovedanih praksah (4. 2. 2025): https://ec.europa.eu/newsroom/dae/redirection/document/118647
- Osnutek Smernic COM o klasifikaciji visoko tveganih sistemih UI – objavljen 19. 5. 2026, javno posvetovanje do 23. 6. 2026:

https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems

PRVI KORAKI K ZAGOTAVLJANJU SKLADNOSTI?

1. Preverite, ali vaša organizacija uporablja sisteme, ki ustrezajo definiciji sistema umetne inteligence iz Akta o UI.
2. Ugotovite, v katero kategorijo se uvršča sistem UI, ki ga uporabljate, glede na namen njegove uporabe in v kakšni vlogi nastopa vaša organizacija (ponudnik, uvajalec, itd.).
3. Preverite, ali se relevanten del obveznosti iz Akta o UI že uporablja oziroma kdaj se bo začel uporabljati (preverite tudi t. i. *grandfathering clause*).

RAZDELITEV PRISTOJNOSTI MED ORGANI ZA NADZOR TRGA V SLOVENIJI

V Sloveniji bo nadzor nad določbami Akta o umetni inteligenci opravljalo pet organov za nadzor trga:

1. *Agencija za komunikacijska omrežja in storitve (AKOS)*: enotna kontaktna točka, nadzor nad Prilogo I in manjšim delom priloge III (kritična infrastruktura, zaposlovanje in dostop do bistvenih javnih in zasebnih storitev),
2. *Informacijski pooblaščenec*: prepovedane prakse in večji del Priloge III (biometrija, izobraževanje, preprečevanje, odkrivanje in preiskovanje KD, meje, migracije in azil ter pravosodje in demokratični procesi);
3. Agencija za zavarovalni nadzor;
4. Banka Slovenije;
5. Tržni inšpektorat Republike Slovenije.

KAKŠNE PA SO ZAHTEVE VARSTVA OSEBNIH PODATKOV?

Če sistem UI, ki ga uporabljate, obdeluje osebne podatke, se uporabljajo vsa pravila varstva osebnih podatkov.

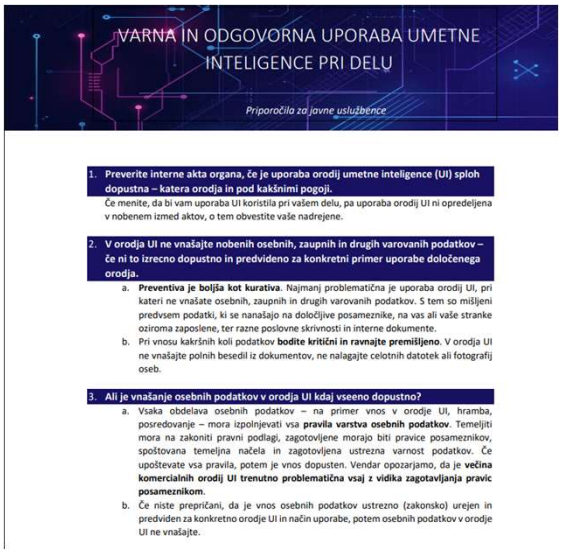
Osebni podatki niso samo imena in priimki, nalovi, davčne in EMŠO številke, temveč so to vse informacije, ki so v zvezi z določenim ali določljivim posameznikom.

Ključni koraki pri zagotavljanju skladnosti sistemov UI z varstvom osebnih podatkov:

- Opredelite, kakšna je vloga podjetja ali organizacije v sistemu varstva osebnih podatkov (upravljavec, obdelovalec, skupni upravljavec).
- Določite namen ali namene obdelave osebnih podatkov.
- Opredelite pravno podlago za obdelavo podatkov in – če sistem UI obdeluje posebne vrste podatkov – , tudi pravno podlago za obdelavo teh podatkov.
- Omejite obseg osebnih podatkov, ki se obdelujejo, zgolj na tiste podatke, ki so nujno potrebni glede na zasledovani namen obdelave.
- Določite obdobje hrambe osebnih podatkov.
- Razmislite, ali boste lahko uresničevali pravice, ki jih Splošna uredba daje posameznikom in na kakšen način boste to učinkovito zagotavljali.
- Določite organizacijske in tehnične ukrepe za zagotavljanje varnosti osebnih podatkov.

Več o tem na: https://www.ip-rs.si/varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/umetna-inteligenca-in-varstvo-osebnih-podatkov.

UMETNA INTELIGENCA – PRIPOROČILA ZA JAVNE USLUŽBENCE



VARNA IN ODGOVORNA UPORABA UMETNE INTELIGENCE PRI DELU

Priporočila za javne uslužbence

1. **Preverite interne akta organa, če je uporaba orodij umetne inteligence (UI) sploh dopustna – katera orodja in pod kakšnimi pogoji.**
   Če menite, da bi vam uporaba UI koristila pri vašem delu, pa uporaba orodij UI ni opredeljena v nobenem izmed aktov, o tem obvestite vaše nadrejene.

2. **V orodja UI ne vnašajte nobenih osebnih, zaupnih in drugih varovanih podatkov – če ni to izrecno dopustno in predvideno za konkretni primer uporabe določenega orodja.**
   a. **Preventiva je boljša kot kurativa**. Najmanj problematična je uporaba orodij UI, pri kateri ne vnašate osebnih, zaupnih in drugih varovanih podatkov. S tem so mišljeni predvsem podatki, ki se nanašajo na določljive posameznike, na vas ali vaše stranke oziroma zaposlene, ter razne poslovne skrivnosti in interne dokumente.
   b. Pri vnosu kakršnih koli podatkov **bodite kritični in ravnajte premišljeno**. V orodja UI ne vnašajte polnih besedil iz dokumentov, ne nalagajte celotnih datotek ali fotografij oseb.

3. **Ali je vnašanje osebnih podatkov v orodja UI kdaj vseeno dopustno?**
   a. Vsaka obdelava osebnih podatkov – na primer vnos v orodje UI, hramba, posredovanje – mora izpolnjevati vsa **pravila varstva osebnih podatkov**. Temeljiti mora na zakoniti pravni podlagi, zagotovljene morajo biti pravice posameznikov, spoštovana temeljna načela in zagotovljena ustrezna varnost podatkov. Če upoštevate vsa pravila, potem je vnos dopusten. Vendar opozarjamo, da je **večina komercialnih orodij UI trenutno problematična vsaj z vidika zagotavljanja pravic posameznikom**.
   b. Če niste prepričani, da je vnos osebnih podatkov ustrezno (zakonsko) urejen in predviden za konkretno orodje UI in način uporabe, potem osebnih podatkov v orodje UI ne vnašajte.

Priporočila so dostopna na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Priporocila/Varna%20in%20odgovorna%20uporaba%20UI%20pri%20delu_%20Priporo%C4%8Dila%20za%20javne%20uslu%C5%BEbence_10feb2026.pdf

UMETNA INTELIGENCA – PRIPOROČILA ZA JAVNE USLUŽBENCE

1. Preverite interne akta organa, če je uporaba orodij umetne inteligence (UI) sploh dopustna – katera orodja in pod kakšnimi pogoji.
2. V orodja UI ne vnašajte nobenih osebnih, zaupnih in drugih varovanih podatkov, če ni to izrecno dopustno in predvideno za konkretni primer uporabe določenega orodja.
3. Ali je vnašanje osebnih podatkov v orodja UI kdaj vseeno dopustno?
4. Manj je več – če že uporabljate orodja UI pri svojem delu, poskrbite, da v njih vnašate najmanjši možen obseg podatkov, s katerim še lahko dovolj učinkovito opravite svoje delo.
5. Ni vsako brisanje osebnih podatkov anonimizacija.
6. Vedno preverite pravilnost prejetih odgovorov.

Hvala za pozornost.

Več informacij: https://www.ip-rs.si/umetna-inteligenca/

Dosegljivi smo na: **01 230 97 30** ali **gp.ip@ip-rs.si**

INFORMACIJSKI POOBLAŠČENEC