



Pravni vidiki uporabe umetne inteligence v delovnih razmerjih – Uredba (EU) 2024/1689 o določitvi harmoniziranih pravil o umetni inteligenci in slovenski zakon o izvajanju uredbe

Damjan Mašera*

UDK: 331.108:004.8
349.2:061.1EU:004.8

Povzetek: Prispevek analizira uporabo umetne inteligence pri zaposlovanju in urejanju delovnih razmerij. Akt o UI kadrovske sisteme uvršča med visokotvegane, zato morajo delodajalci kot njihovi uporabniki spoštovati vrsto strogih tehničnih in organizacijskih obveznosti. Slovenija je z ZIUODHPUI prilagodila nacionalni pravni red zahtevam evropske uredbe in določila pristojne organe za nadzor ter (stroge) prekrškovne sankcije.

Ključne besede: umetna inteligenca, delovna razmerja, Akt o UI, visokotvegani sistemi, zaposlovanje in upravljanje delavcev, diskriminacija, transparentnost, človeški nadzor, ZIUODHPUI.

Legal Aspects of the Use of Artificial Intelligence in Employment Relationships – Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence and the Slovenian Act Implementing the Regulation

Abstract: The article analyses the use of artificial intelligence in recruitment and in the regulation of employment relationships. The AI Act classifies HR systems as high-risk, meaning that employers, as their deployers, must comply with a range of strict technical and organisational obligations. Slovenia has aligned its national legal framework with the requirements

* Damjan Mašera, univ. dipl. pravnik, direktor strokovnih služb Združenja delodajalcev Slovenije. damjan.masera@zds.si
Damjan Mašera, LL.B., Director of Expert Services at the Association of Employers of Slovenia.

of the European regulation through the ZIUODHPUI and has designated the competent supervisory authorities and (strict) administrative offence sanctions.

Key words: *artificial intelligence, employment relationships, AI Act, high-risk systems, recruitment and workforce management, discrimination, transparency, human oversight, ZIUODHPUI.*

1. UVOD

Uporaba umetne inteligence (v nadaljevanju: UI) postaja vse bolj razširjena tudi v delovnih okoljih in lahko prinaša številne prednosti, obenem pa odpira tudi pomembna pravna vprašanja. V delovnih razmerjih lahko namreč UI nastopa pri vseh fazah urejanja le-teh – od postopka zaposlovanja, upravljanja in nadzora dela do prenehanja pogodbe o zaposlitvi.

UI se tako lahko pojavlja v vseh fazah zaposlitvenega cikla delavcev – od iskanja kandidatov, izbora in zaposlitve, do spremljanja delovne uspešnosti in prenehanja delovnega razmerja. V zaposlitvenih postopkih lahko delodajalci uporabljajo UI za optimizacijo zaposlitvenih oglasov in ciljno usmerjeno iskanje kandidatov. V okviru prejetih prijav na razpisano delovno mesto lahko UI na podlagi vnaprej določenih meril avtomatizirano razvršča kandidate in celo vodi razgovore, razgovori se lahko vodijo kot video intervjuji, kjer kandidati odgovarjajo preko kamere, UI pa analizira njihove odgovore in na podlagi tega ocenjuje njihovo ustreznost. V končni fazi izbire lahko sistemi UI delodajalcem predlagajo najustreznejšega kandidata. Poleg zaposlovanja se UI lahko uporablja tudi pri usposabljanju in ocenjevanju delavcev, delodajalci pa lahko uvajajo UI klepetalnike (generativna UI za splošne namene), ki odgovarjajo na (kadrovska) vprašanja zaposlenih. UI se lahko uporablja za spremljanje učinkovitosti dela (npr. s senzorji in nosljivimi napravami), načrtovanje in razporejanje dela in celo za oblikovanje in izdajane aktov v zvezi z delovnim razmerjem. Že danes obstajajo primeri, ko algoritmično upravljanje pri delodajalcih, kot je npr. Amazon, samodejno generira opozorila ob zaznani nižji produktivnosti ali kakovosti dela¹. Prav tako se uporabljajo GPS-

¹ Gibson K., Amazon under fire for software that recommends firing workers, CBS News (MoneyWatch), 26. 4. 2019, <https://www.cbsnews.com/news/amazon-under-fire-for-software-that-recommends-firing-workers/>

sledenje dostavljavcev, periodično zajemanje posnetkov zaslona na računalnikih ter beleženje pritiskov na tipkovnico – vse z namenom nadzorovati in dvigniti učinkovitost².

Pri uporabi UI v delovnem razmerju bi sicer lahko sklepali o objektivnejšem odločanju brez človeških predsodkov, vendar lahko uporaba v praksi prinaša nove oblike pristranskosti in diskriminacije. Algoritmi so tako objektivni kot podatki, na katerih se učijo in kot je objektivna zasnova njihovih modelov. Pristranskost se lahko nehote vtihotapi v sistem UI na več načinov: (1) z izbiro in oblikovanjem algoritma (če je ta optimiziran na način, ki določene skupine obravnava slabše), (2) prek učenja na zgodovinskih podatkih, ki odražajo pretekle človeške pristranskosti, ali (3) zaradi napačne uporabe oziroma interpretacije rezultatov³. Tako lahko že sicer v zasnovi nevtralen sistem prevzame pristranske vzorce. Na primer, če je v preteklosti v neki panogi na vodilnih mestih prevladovala ena demografska skupina, lahko algoritem za izbor kadrov tak profil »nezavedno« izbira tudi v bodoče.

V praksi so se tveganja diskriminacije z UI že udejanjila. V ZDA je Komisija za enake zaposlitvene možnosti ZDA (EEOC) v zadevi iTutorGroup izpostavila, da je programska oprema za prijave samodejno zavračala kandidatke, stare 55 let ali več, ter kandidate, stare 60 let ali več. Kandidate je npr. sistem zaradi določene starosti izločil iz postopka, medtem ko je z lažno navedeno nižjo starostjo kandidat prejel vabilo na razgovor⁴. Po navedbah EEOC je bilo na tej podlagi zavrženih več kot 200 sicer kvalificiranih kandidatov. V Evropi je odmeval primer Deliveroo: dostavljavci hrane so utrpeli sankcije zaradi algoritma, ki je kaznoval odsotnosti od prijavljenih delovnih terminov ne glede na vzroke. Sodišče v Bologni je ugotovilo diskriminatorne učinke sistema razporejanja terminov ter naložilo prilagoditev sistema, kar poudarja pomen preglednosti delovanja algoritmov – platforma oziroma delodajalec mora biti zmožen razložiti, kako sistem odloča, da lahko delavec učinkovito uveljavlja svoje pravice⁵.

² Ibidem.

³ Ferrer X. et al., Bias and discrimination in UI: A cross-disciplinary perspective, IEEE Technology and Society Magazine, 2021, Vol. 40, No. 2.

⁴ EEOC, iTutorGroup to Pay \$365,000 to Settle EEOC Discriminatory Hiring Suit, 16. 5. 2022, <https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit>

⁵ Tribunale di Bologna, N. R.G. 2949/2019 (Filcams CGIL Bologna idr. proti Deliveroo Italia S.r.l.), odločba z dne 31. 12. 2020; glej tudi Eurofound, »Italian Court rules that the Deliveroo Algorithm Discriminates Workers«, 6. 1. 2022, <https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121>

Hitremu razvoju tehnologije se skuša prilagajati tudi pravni okvir z namenom zaščite temeljnih pravic delavcev ter preprečevanja tveganj, kot so na primer pristranskost algoritmov, prekomeren nadzor ali posegi v zasebnost. V Evropski uniji se je kot odgovor na morebitna tveganja oblikovala Uredba (EU) 2024/1689 o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci)⁶. Akt o umetni inteligenci (v nadaljevanju: Akt o UI) je celovit zakonodajni okvir, ki ureja tako razvoj kot uporabo UI ter skuša zagotoviti varno in zaupanja vredno uporabo naprednih tehnologij.

Prispevek se v nadaljevanju opredeli do evropskega pravnega okvira uporabe UI v delovnem razmerju in s tem okvirom povezano slovensko zakonodajo, s poudarkom na obveznostih delodajalcev pri uporabi UI v delovnih razmerjih.

2. EVROPSKA UREDBA O UMETNI INTELIGENCI – SKUPNI PRAVNI OKVIR

Akt o UI uvaja harmonizirana pravila za razvoj, preizkušanje in uporabo UI v EU. Gre za uredbo neposredne veljavnosti, ki od 1. avgusta 2024 velja v vseh državah članicah. Temeljni cilji akta so dvojni: spodbuditi inovacije na področju UI in hkrati zagotoviti visoko raven varstva zdravja, varnosti ter temeljnih pravic posameznikov. Akt sledi načelu sorazmernosti – uvaja obveznosti glede na stopnjo tveganja, ki ga prinaša posamezen sistem UI.

Akt o UI je kot uredba neposredno zavezujoč in nadrejen morebitnim nacionalnim predpisom. Osrednji cilj je vzpostaviti harmoniziran pravni okvir za razvoj, trženje, uporabo in delovanje sistemov umetne inteligence po vsej EU. Želi izboljšati delovanje notranjega trga, da bi podjetja lažje ponujala UI rešitve ob enakih pravilih za vse (glej recital (1) Akta o UI). Drugi ključni cilj je zagotavljanje varnosti in temeljnih pravic. Akt o UI prepoznava, da lahko UI prinese tveganja za zdravje, varnost in osnovne pravice ljudi, če ni ustrezno nadzorovana. Zato uvaja vrsto

⁶ Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (Besedilo velja za EGP), UL L, 2024/1689, 12.7.2024.

obveznosti za tiste, ki UI razvijajo ali uporabljajo, da se tveganja obvladujejo glede na resnost ogrožanja pravic in temeljnih svoboščin.

Z vidika področja uporabe se Akt o UI nanaša na sisteme umetne inteligence v širokem smislu. V 3. členu je UI sistem opredeljen kot »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«. Gre za splošno definicijo, kjer je pomembno, da ne zajame zgolj kompleksnih nevronske mreže, temveč tudi bolj enostavne algoritmične sisteme, če ti izkazujejo določeno stopnjo avtonomnega učenja ali odločanja. Izvzeti pa so sistemi izključno za raziskave in razvoj, odprtokodni sistemi (dokler ne postanejo del komercialnega produkta ali prepovedane rabe) ter stroji brez kakršnekoli »inteligence« (klasična programska oprema). Akt tudi ne posega v uporabo UI za vojaške namene, saj to ostaja zunaj prava EU⁷.

Temeljno načelo Akta o UI je regulacija glede na izpostavljenost tveganja. To pomeni, da se na UI ne gleda enoznačno, temveč glede na vsebino in namen uporabe. Akt ne poskuša vnaprej predpisati tehničnih pravil za vse možne UI, temveč jih razvršča v (štiri) kategorije tveganja in za vsako določi primerne omejitve ali zahteve. Posebej izpostavljeno načelo je etičnost in človekov nadzor: v jedru Akta je prepričanje, da mora UI ostati pod nadzorom človeka in skladna z evropskimi vrednotami. Zato v več določbah najdemo zahteve po preglednosti, možnostih in obveznosti človeškega posredovanja in spoštovanju temeljnih pravic. Na ravni EU se je ustanovil tudi Evropski urad za UI, ki skrbi za usmerjanje in svetovanje glede etične uporabe in pripravlja kodekse ravnanja.

Akt o UI je, kot je izpostavljeno v prejšnjem odstavku, sisteme razdelil na štiri kategorije glede na tveganja, ki jih njihova uporaba povzroča. Prepovedani sistemi (1) vključujejo UI, ki predstavljajo nesprejemljivo tveganje za človekove pravice – na primer sistemi za socialno točkovanje ljudi na podlagi vedenja ali osebnostnih lastnosti ter sistemi za manipulacijo vedenja uporabnikov ali prepoznavanje čustev na delovnem mestu. Takšni sistemi so z 2. februarjem 2025 prepovedani in jih uporabniki (med njimi tudi delodajalci) ne smejo uporabljati. Sledi kategorija visoko tveganih sistemov UI (2), za katere akt določa stroge pogoje uporabe, saj lahko pomembno vplivajo na zdravje, varnost ali pravice ljudi.

⁷ Akt o UI, Člen 3 (opredelitev pojmov).

V to kategorijo spada UI v kontekstu zaposlovanja in upravljanja delavcev, kot bo podrobneje opisano v nadaljevanju. Obveznosti glede visoko tveganih sistemov se bodo začele uporabljati 2. avgusta 2026. Za sisteme, kjer obstaja tveganje za preglednost (3), akt predvideva blažje zahteve, npr. transparentnost za UI, ki ustvarjajo slike, besedila ali posnemajo človeka. Sistemi minimalnega tveganja ali brez tveganja (4) (npr. običajna programska oprema z vgrajenimi UI funkcijami, kot so filtri za neželeno pošto ipd.) pa posebnih novih obveznosti nimajo, razen splošne dolžnosti spoštovanja obstoječe zakonodaje.

2.1. Sistemi nesprejemljivega tveganja

Sistemi nesprejemljivega tveganja so tisti, ki jih Akt o UI prepoveduje⁸, ker bi njihova uporaba nasprotovala evropskim vrednotam in pravicam. Sem sodijo na primer sistemi socialnega točkovanja (dodeljevanje družbene ocene posameznikom na podlagi njihovega vedenja ali lastnosti, po vzoru nekaterih tujih praks), UI za podzavestno manipulacijo ljudi (npr. tehnologije, ki neopazno vplivajo na človekovo vedenje na škodljiv način), obsežni sistemi biometričnega nadzora v realnem času na javnih mestih (razen izjemoma za hud boj proti kriminalu), ter algoritmi za množični nadzor, ki kršijo pravico do zasebnosti.

V kontekstu delovnih razmerij je posebej pomembna prepoved iz točke (f) prvega odstavka 5. člena Akta o UI: »dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov UI za sklepanje o čustvih fizične osebe na delovnem mestu in v izobraževalnih ustanovah, razen kadar je uporaba sistema UI namenjena uvedbi ali dajanju na trg iz zdravstvenih ali varnostnih razlogov«. Prepoved velja za delodajalce kot uporabnike (uvajalce) UI ter tudi za ponudnike takih sistemov⁹.

Evropska komisija je že objavila smernice o prepovedanih praksah umetne inteligence¹⁰, kot so opredeljene v aktu o umetni inteligenci. Gre za pregled praks umetne inteligence, ki se štejejo za nesprejemljive zaradi morebitnih tveganj za evropske vrednote in temeljne pravice. Namenjene so zagotavljanju dosledne, učinkovite in enotne uporabe Akta o UI. Gre za nezavezujočo razlago,

⁸ Akt o UI, Člen 5 (prepovedane prakse UI).

⁹ Akt o UI, Člen 5(1)(f).

¹⁰ Smernice Komisije o prepovedanih praksah umetne inteligence, določenih v Uredbi (EU) 2024/1689 (akt o umetni inteligenci), 29.7.2025, <https://ec.europa.eu/newsroom/dae/redirection/document/118647>

zavezujoče razlage pa so pridržane Sodišču Evropske unije. Smernice skušajo zagotoviti pravna pojasnila in praktične primere, ki pomagajo razumeti zahteve akta o umetni inteligenci in jih izpolnjevati.

2.2. Uporaba UI pri zaposlovanju in upravljanju zaposlenih

Zakonodajalec na ravni EU je posebej prepoznal, da UI v t.i. kadrovskih postopkih in pri upravljanju zaposlenih lahko močno vpliva na posameznikove pravice (npr. pravico do zaposlitve, do zasebnosti, do nediskriminacije). Akt o UI zato uvršča sisteme UI na področju zaposlovanja, upravljanja delavcev in dostopa do zaposlitve med sisteme visokega tveganja¹¹.

Sem sodijo primeroma:

- UI orodja za nabor in izbiro kandidatov (npr. avtomatizirano pregledovanje in selekcija prijav, razvrščanje kandidatov, psihometrični testi z UI, analitika video intervjujev ipd.),
- algoritmi za odločanje o zaposlitvi, napredovanju ali prenehanju delovnega razmerja (npr. UI sistem, ki predlaga izbiro ali zavrnitev kandidata, ali ki zaznava neučinkovite delavce in sproži postopek prenehanja delovnega razmerja),
- sistemi za upravljanje delovne uspešnosti in razporejanje nalog (npr. algoritmično dodeljevanje izmen, sledenje produktivnosti, priprava ocen dela),
- orodja za spremljanje in nadzor nad delavci (npr. nosljive naprave, GPS sledenje, programska oprema za zajem zaslona, analiza tipkanja ali drugih biometričnih podatkov pri delu).

Uvrstitev tovrstnih sistemov med visokotvegane pomeni, da morajo izpolnjevati stroge tehnične in organizacijske zahteve, preden jih je dopustno uporabljati, enako velja tudi med njihovo samo uporabo. Velik del teh zahtev bremeni ponudnike oziroma razvijalce sistemov (obveznosti glede kakovosti podatkov, tehnične dokumentacije, ocen skladnosti itd.). Vendar pa akt nalaga tudi pomembne obveznosti uporabnikom (Akt o UI uporabnike definira kot uvajalce UI) teh sistemov – v našem primeru delodajalcem, ki takšne UI sisteme uporabljajo v razmerju do kandidatov ali zaposlenih. Uporaba UI pri kadrovanju in upravljanju

¹¹ Akt o UI, Priloga III (visokotvegani sistemi): področje zaposlovanja, upravljanja delavcev in dostopa do samozaposlitve.

delavcev je torej zakonita, vendar ob upoštevanju pravil iz Akta o UI, ki ciljajo na preprečevanje pristranskosti, diskriminacije, ogrožanja zasebnosti in drugih škodljivih posledic.

2.2.1. Obveznosti delodajalcev kot uporabnikov visokotveganih sistemov

Če podjetje kot delodajalec uvaja oziroma uporablja visokotvegani UI sistem na delovnem mestu, nastopa v vlogi uporabnika (uvajalca) visokotvegane sistema po Aktu o UI. Pomembno je poudariti, da akt razlikuje med ponudniki (ki razvijejo in dajo UI sistem na trg) in uporabniki - uvajalci (ki sistem uporabljajo v praksi).

Delodajalec, ki denimo na trgu pridobi komercialni UI - sistem za npr. predselekcijo kandidatov, velja za uporabnika tega visokotvegane sistema in ima sledeče ključne obveznosti (glej člen 26 Akta o UI):

- **Uporaba skladno z namenom in navodili:** Delodajalec sme sistem uporabljati le v skladu z vnaprej določenim namenom in navodili proizvajalca. Zagotoviti mora, da se UI uporablja na način, kot je bil predviden ob oceni skladnosti, sicer lahko gre za kršitev. Prav tako mora vzdrževati in preverjati UI sistem po navodilih – npr. redno posodabljanje modele, če tako priporoča proizvajalec.
- **Človeški nadzor nad delovanjem:** Akt o UI izrecno zahteva, da uporabnik določi osebe, ki bodo izvajale človeški nadzor nad sistemom. To pomeni, da mora delodajalec imenovati dovolj usposobljenega in pooblaščenega zaposlenega (ali več njih), ki razume delovanje sistema in lahko vpliva na njegove odločitve. Človeški nadzor vključuje spremljanje izhodnih podatkov UI ter možnost posredovati, če bi sistem sprejel neustrezno odločitev ali če pride do napake.
- **Relevantnost in kakovost vhodnih podatkov:** Če delodajalec pri uporabi sistema sam vpliva na vhodne podatke (npr. izbira kriterije, uvaža podatke o kandidatih), mora zagotoviti, da so ti podatki ustrezni, točni in reprezentativni glede na namen uporabe. S tem se preprečuje, da bi UI sklepala na podlagi napačnih ali pristranskih podatkov. V praksi to pomeni na primer, da se v sistem ne vnašajo podatki, ki niso povezani z zahtevami delovnega mesta (npr. verska pripadnost ali družinski status kandidata, kar bi lahko bilo v nasprotju z

zakonom že zbirati le-te), in da se podatkovne zbirke sproti čistijo nerelevantnih podatkov.

- **Spremljanje delovanja in odzivanje na tveganja:** Delodajalec mora spremljati delovanje UI sistema v skladu z navodili za uporabo. Če med uporabo opazi, da odločitve UI odstopajo in bi lahko predstavljale tveganje za varnost ali pravice ljudi, mora nemudoma obvestiti proizvajalca oziroma dobavitelja ter pristojni nadzorni organ. V primeru resnih dogodkov (npr. da bi UI zaradi napake nezakonito diskriminiral kandidata ali ogrozil varnost delavca) je dolžan to prijaviti ter začasno ustaviti uporabo sistema.
- **Vodenje evidenc in beleženje:** Uporabnik visokotveganega sistema mora hraniti avtomatske zapise (dnevniške datoteke) o delovanju sistema vsaj 6 mesecev ali dlje, če to določa drug predpis. Dnevniški zapisi (npr. kateri kandidat je bil s strani UI predlagan v nadaljnji postopek, katere odločitve je UI podala ipd.) so pomembni za sledljivost in morebitna naknadna preverjanja ustreznosti odločitev. Ti podatki so lahko ključni tudi v primeru spora (npr. če kandidat trdi, da je bil diskriminiran, se lahko preveri, na podlagi katerih kriterijev je UI izločila njegovo prijavo ali je ni umestila višje). Hranjenje dnevniških zapisov mora biti skladno tudi z zakonodajo o varstvu osebnih podatkov – nepotrebno dolgoročno shranjevanje ali shranjevanje občutljivih podatkov brez podlage ni dopustno.
- **Transparentnost in obveščanje delavcev:** Ena izmed pomembnejših obveznosti je obveščanje oseb. Akt o UI določa, da mora delodajalec pred uvedbo ali uporabo visokotveganega UI sistema na delovnem mestu o tem obvestiti predstavnike delavcev (npr. svet delavcev ali sindikat) ter same zaposlene, ki bodo takemu sistemu podvrženi (sedmi odstavek člena 26 Akta o UI). Obvestilo mora biti podano vnaprej in na način, kot to zahteva nacionalna zakonodaja (spoštovati je treba postopke obveščanja in posvetovanja z delavci po nacionalnih predpisih). Poleg splošnega obvestila zavezuje Akt o UI delodajalca, da vsakega posameznika (bodisi kandidata bodisi zaposlenega), o katerem se sprejema odločitev s pomočjo UI, seznaniti, da je bil v postopku uporabljen UI sistem (enajsti odstavek člena 26 Akta o UI). Transparentnost omogoča posamezniku razumevanje procesa in uveljavljanje svojih pravic (npr. pravice do pojasnila odločitve ali izpodbijanja odločitve, če meni, da je nepravilna).

Delodajalci, ki uporabljajo visoko tvegane sisteme UI, morajo tako vzpostaviti predpisane mehanizme nadzora, transparentnosti in upravljanja tveganj kot izhaja iz člena 26 Akta o UI.

3. IMPLEMENTACIJA AKTA O UI V SLOVENSKI ZAKONODAJI

Kot evropska uredba je Akt o UI neposredno zavezujoč in se ga ne prenaša v nacionalni pravni red. Vendar pa so države članice na podlagi Akta o UI zavezane urediti nekatere vidike, zlasti nadzorne organe in prekrškovne sankcije, da se zagotovi izvrševanje pravil, ki jih določa uredba. V Sloveniji je bil za ta namen sprejet Zakon o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (v nadaljevanju: ZIUDHPUI). Zakon je bil v Uradnem listu RS št. 85/25 objavljen 6. novembra 2025 in je začel veljati 21. novembra 2025.

3.1. Pristojni nadzorni organi v Sloveniji

Zakon vzpostavlja model razdeljene pristojnosti nadzora nad UI, prilagojen obstoječim nadzornim organom po področjih. Izhaja iz nabora prepovedane uporabe UI in seznama področij visokotveganih UI sistemov v Aktu o UI ter obstoječe delitve regulatorjev v Sloveniji. Ključne pristojnosti za nadzor so opredeljene na naslednji način:

- Informacijski pooblaščenec (IP) je pristojni organ za nadzor nad prepovedanimi praksami UI in nad določenimi visokotveganimi sistemi (zlasti s področja biometrije, izobraževanja, kaznivih dejanj, migracij ter pravosodja in volitev). ZIUDHPUI hkrati določa koordinacijski mehanizem: pri nadzoru visokotveganih sistemov UI iz 3. točke Priloge III Akta o UI se IP posvetuje z vsebinsko pristojnimi inšpekcijskimi organi¹².
- Agencija za komunikacijska omrežja in storitve RS (AKOS) prevzema vlogo organa za visokotvegane UI sisteme na več področjih, med drugim tudi za zaposlovanje in upravljanje delavcev. ZIUDHPUI določa, da tudi AKOS pri izvajanju nadzora nad visokotveganimi sistemi UI na navedenih področjih sodeluje oziroma se posvetuje s stvarno pristojnimi inšpekcijskimi organi ter z Informacijskim pooblaščenecem¹³.
- Agencija za zavarovalni nadzor (AZN) je pristojna za nadzor nad UI sistemi v zavarovalništvu, konkretno tistimi, ki ocenjujejo tveganja in določajo premije v življenjskih in zdravstvenih zavarovanjih¹⁴.

¹² ZIUDHPUI, prvi odstavek 10. člena in peti odstavek 13. člena.

¹³ ZIUDHPUI, peti odstavek 10. člena in drugi odstavek 13. člena.

¹⁴ ZIUDHPUI, četrty odstavek 10. člena in četrti odstavek 13. Člena.

- Banka Slovenije (BS) je pristojna za nadzor nad UI sistemi za kreditno ocenjevanje fizičnih oseb pri bankah. Bančni sektor je močno reguliran in BS ima strokovnjake za modele tveganj; UI posojilni algoritmi bodo tako pod njenim drobnogledom. Če pa enako stvar (kreditno ocenjevanje) uporablja kdo zunaj bančnega sektorja (npr. posojilnice), bo to nadziral Tržni inšpektorat RS, ki v predlogu nastopa kot nadomestni organ za finančne UI izven klasičnih institucij¹⁵.
- Tržni inšpektorat RS (TIRS) je organ za nadzor nad UI sistemi, vgrajenimi v proizvode (kadar niso zajeti drugje) ter za ostale primere, ki niso izrecno dodeljeni drugim. TIRS bo torej nekakšen »splošni« inšpekcijski organ, ki lahko posreduje, če kakšno področje ni zajeto v osnovnih pristojnostih drugih organov¹⁶.

Slovenija glede na predhodno navedeno ne ustanavlja povsem nove agencije oziroma nadzornega organa za UI, ampak obstoječe regulatorje opremlja z dodatnimi pooblastili.

3.2. Prekrški in globe

Čeprav Akt o UI določa maksimalne globe, so morale države članice v svojem prekrškovnem pravu opredeliti, katere kršitve so prekrški in kdo jih sankcionira. ZIUDHPUI opredeljuje prekrške za kršitve določb Akta o UI in določa razrede glob, ki so usklajene z aktom. ZIUDHPUI se pri opredelitvi prekrškov sicer sklicuje neposredno na besedilo Akta o UI.

3.2.1. Globe za prepovedane prakse na področju delovnih razmerij

Delodajalci so zaradi neupoštevanje prepovedi praks, ki se nanašajo na delovno razmerje iz 5. člena Uredbe 2024/1689/EU (sklepanje o čustvih na delovnem mestu), sankcionirani z globo od 25.000 do 250.000 evrov, z globo od 100.000 do 450.000 evrov pa delodajalci, ki se po zakonu, ki ureja gospodarske družbe, štejejo za veliko gospodarsko družbo. Gre za prekršek, če **delodajalec daje na trg, v uporabo za ta posebni namen ali uporablja sistem UI za sklepanje o**

¹⁵ ZIUDHPUI, drugi odstavek 10. člena in tretji odstavek 13. člena.

¹⁶ ZIUDHPUI, tretji odstavek 10. člena in šesti odstavek 13. člena.

čustvih fizične osebe na delovnem mestu in v izobraževalnih ustanovah, razen kadar je uporaba sistema UI namenjena uvedbi ali dajanju na trg iz zdravstvenih ali varnostnih razlogov (točka (f) prvega odstavka 5. člena Uredbe 2024/1689/EU).

Z globo od 15.000 do 100.000 eurov se za prekršek kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, z globo 2.000 eurov pa se za prekršek kaznuje posameznik.

Z globo od 2.500 do 10.000 eurov se za prekršek kaznuje tudi odgovorna oseba pravne osebe, odgovorna oseba v državnem organu ali samoupravni lokalni skupnosti ali odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost.

Kadar je prekršek posebno hud zaradi višine povzročene škode oziroma višine pridobljene protipravne premoženjske koristi ali zaradi storilčevega naklepa oziroma njegovega namena koristoljubnosti, se ponudnik ali uvajalec, ki je pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, kaznuje z globo v višini do 35.000.000 eurov ali do sedem odstotkov skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji. Z globo od 5.000 do 30.000 eurov se kaznuje tudi odgovorna oseba pravne osebe, odgovorna oseba v državnem organu ali samoupravni lokalni skupnosti, odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost podjetnika. Z globo od 3.000 do 15.000 eurov pa se za prekršek kaznuje posameznik.

Z globo v višini do 35.000.000 eurov ali do sedmih odstotkov skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je nižji, se kaznuje pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za mikro, majhno in srednjo družbo, ter samostojni podjetnik posameznik oziroma posameznik, ki samostojno opravlja dejavnost. Takšna globa se izreče le v primeru, da je ta nižja od globe, določene v prvem, drugem ali petem odstavku 26. člena zakona.

3.2.2. Globe na področju uporabe visokotvegane sistema

Več prekrškovnih določb se nanaša na delodajalca, ki je uvajalec (uporabnik) visokotveganih sistemov UI.

Z globo od 25.000 do 250.000 eurov se za prekrške uvajalca kaznuje pravna oseba, z globo od 100.000 do 450.000 eurov pa pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za veliko gospodarsko družbo, če (izpostavljene so za delodajalce bistvene točke 31. člena zakona):

1. **ne sprejme ustreznih tehničnih in organizacijskih ukrepov, s katerimi se zagotovi uporaba sistemov v skladu s priloženimi navodili** za uporabo na podlagi tretjega in šestega odstavka 26. člena Uredbe 2024/1689/EU (prvi odstavek 26. člena Uredbe 2024/1689/EU);
2. **ne dodeli človeškega nadzora** fizičnim osebam, ki imajo potrebne kompetence, usposobljenost in pooblastila ter potrebno podporo (drugi odstavek 26. člena Uredbe 2024/1689/EU);
7. **ne vodi dnevnikov**, ki jih visokotvegani sistem UI samodejno ustvari, če je ta dnevnik pod njenim nadzorom, v obdobju, ki ustreza predvidenemu namenu visokotveganega sistema UI, in sicer vsaj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače (šesti odstavek 26. člena Uredbe 2024/1689/EU);
9. kadar je delodajalec, **pred dajanjem visokotveganega sistema UI v uporabo ali pred uporabo visokotveganega sistema UI na delovnem mestu, ne obvesti predstavnikov delavcev ali delavce, na katere se to nanaša, da se bo zanje uporabljal visokotvegani sistem UI** (sedmi odstavek 26. člena Uredbe 2024/1689/EU);
19. v primeru visokotveganih sistemov iz Priloge III Uredbe 2024/1689/EU, ki sprejemajo **odločitve ali pomagajo pri odločanju v zvezi s fizičnimi osebami, slednjih ne obvesti, da se zanje uporablja navedeni sistem** (enajsti odstavek 26. člena Uredbe 2024/1689/EU);
20. pred uvedbo visokotveganega sistema UI iz Priloge III Uredbe 2024/1689/EU, razen na področju iz 2. točke Priloge III Uredbe 2024/1689/EU, **kadar je oseba javnega prava ali zasebni subjekt in zagotavlja javne storitve, in kadar uvaja visokotvegane sisteme UI pod (b) in (c) 5. točke Priloge III Uredbe 2024/1689/EU, ne izvede ocene učinka**, ki ga lahko povzroči uporaba takega sistema na temeljne pravice (prvi odstavek 27. člena Uredbe 2024/1689/EU);
21. **ne zagotovi jasnih in smiselnih pojasnil o vlogi sistema UI v postopku odločanja in glavnih elementih sprejete odločitve, ki jo sprejme na podlagi izhodnih podatkov visokotveganega sistema UI** iz Priloge III Uredbe 2024/1689/EU, razen sistema iz 2. točke Priloge III Uredbe

2024/1689/EU, **vsaki prizadeti osebi, za katero velja odločitev**, in ki ima pravne učinke ali na to osebo podobno znatno vpliva na način, ki ima po njenem mnenju negativne učinke na njeno zdravje, varnost in temeljne pravice (prvi odstavek 86. člena Uredbe 2024/1689/EU).

Z globo od 15.000 do 100.000 eurov se za prekršek kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, z globo 2.000 eurov pa se za prekršek kaznuje posameznik.

Z globo od 2.500 do 10.000 eurov se za prekršek kaznuje tudi odgovorna oseba pravne osebe, odgovorna oseba v državnem organu ali samoupravni lokalni skupnosti ali odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost.

Kadar je prekršek posebno hud zaradi višine povzročene škode oziroma višine pridobljene protipravne premoženjske koristi ali zaradi storilčevega naklepa oziroma njegovega namena koristoljubnosti, se ponudnik ali uvajalec, ki je pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, kaznuje z globo v višini do 15.000.000 eurov ali do treh odstotkov skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji. Z globo od 5.000 do 30.000 eurov se kaznuje tudi odgovorna oseba pravne osebe, odgovorna oseba v državnem organu ali samoupravni lokalni skupnosti, odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost podjetnika. Z globo od 3.000 do 15.000 eurov pa se za prekršek kaznuje posameznik.

Z globo v višini do 15.000.000 eurov ali do treh odstotkov skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je nižji, se kaznuje pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za mikro, majhno in srednjo družbo, ter samostojni podjetnik posameznik oziroma posameznik, ki samostojno opravlja dejavnost. Takšna globa se izreče le v primeru, da je ta nižja od globe, določene v prvem, drugem ali petem odstavku 31. člena zakona.

4. SKLEPNO

Z uvajanjem uporabe UI v delovno okolje se priložnosti za optimizacijo in inovacije prepletajo z izzivi zagotavljanja skladnosti s pravnim okvirom in zaščito pravic. Akt o UI vzpostavlja enoten, neposredno zavezujoč okvir, ki skuša slediti načelu sorazmernosti – spodbuja razvoj UI, hkrati pa uvaja stroge varovalke glede na raven tveganja uporabe. Sistemi UI, uporabljeni pri zaposlovanju in upravljanju delavcev, so prepoznani kot visoko tvegani, zato morajo delodajalci kot njihovi uporabniki spoštovati vrsto tehničnih in organizacijskih obveznosti. Te vključujejo uporabo skladno z namenom in navodili proizvajalca, uvedbo človeškega nadzora nad delovanjem sistemov, zagotavljanje kakovostnih in relevantnih vhodnih podatkov, stalno spremljanje delovanja UI ter dnevniške zapise o odločitvah. Posebno pozornost morajo delodajalci nameniti transparentnosti – pred uvedbo visoko tveganega UI sistema morajo obvestiti predstavnike delavcev in delavce ter jih seznaniti, da se v postopkih odločanja uporablja UI. S takšnimi ukrepi se preprečujejo morebitna pristranskost, diskriminacija ali nedopustni posegi v zasebnost pri uporabi naprednih tehnologij v kadrovske postopkih.

Slovenija je z ZIUODHPUI prilagodila nacionalni pravni red zahtevam evropske uredbe in določila pristojne organe za nadzor in (strobe) prekrškovne sankcije za kršitve določb Akta o UI. Uporaba prepovedanih praks in neizpolnitev obveznosti, povezanih z uporabo visokotveganih sistemov UI je podvržena visokim globam, tudi do 450.000 eurov za velika podjetja, v posebej hudih primerih pa lahko globe dosežejo do 35.000.000 eurov oziroma 7 % letnega prometa podjetja.

V praksi se bodo s strani delodajalcev vsaj v začetni fazi uporabe pojavile določena odprta vprašanja in nejasnosti zaradi nepreglednosti pravne ureditve in s tem povezanih procesnih posledic neposredne uporabe Akta o UI kot materialnega predpisa. ZIUODHPUI v pretežni meri ureja le nadzor in prekrške, materialne določbe in posledično vsebinske zahteve (npr. kaj pomeni učinkovit človeški nadzor, kdaj gre za upravljanje delavcev, kako daleč sega razlaga odločitev in kako se obveznosti iz Akta o UI prepletajo z Zakonom o delovnih razmerjih) pa ostajajo primarna vsebina ureditve evropske uredbe, harmoniziranih standardov in smernic. To lahko povzroči tudi neenotno prakso in pravno negotovost, saj bodo nadzorni organi (pa tudi zavezanci) uporabljali uredbo neposredno, brez da bi nacionalni predpis vseboval podrobnejša materialna merila.

Dodatno praktično dilemo bo zagotovo povzročala tudi uporaba generativne UI (splošno namenska UI), ki se v praksi pogosto uporablja kot pomožno orodje in

podpora tudi kadrovskim procesom (npr. oblikovanje besedil oglasov, povzetki razgovorov, priprava vprašanj, izbira kandidatov, osnutki ocen uspešnosti ali odpovednih aktov). Tudi če takšno orodje samo po sebi ni zasnovano kot visokotvegani sistem in ga tudi Akt o UI ne obravnava na takšen način, lahko zaradi namena uporabe postane funkcionalni del visokotvegane verige, če njegova uporaba odločilno vpliva na razporejanje kandidatov, ocenjevanje, razporejanje delavcev, disciplinske ukrepe ali prenehanje delovnega razmerja. V takih primerih se bo pojavilo vprašanje, ali mora delodajalec generativno orodje obravnavati kot (del) visokotvegane sistema in posledično upoštevati zahteve iz člena 26 Akta o UI. V dvomu bo delavcem v korist treba obravnavati uporabo generativne UI v kadrovskih postopkih kot odločanje s podporo UI, ki bo moralo zadostiti zahtevam iz Akta o UI, ki so predpisane za visokotvegane sisteme.

Z vidika delodajalcev bo tako zelo pomembno, da se bodo zavedali, na kakšen način se UI v podjetju uporablja in kako takšno rabo UI umestiti glede na opredelitve iz Akta o UI. Posledično bodo obveznosti, ki jih nalaga Akt o UI, lahko tudi ustrezno izvršili, nasprotno pa lahko opustitev katere od predpisanih obveznosti vodi tudi do inšpekcijskega nadzora in izreka kazenskih sankcij. Eden izmed pomembnejših časovnih mejnikov bo 2. avgust 2026, saj se bodo takrat začele v celoti uporabljati določbe glede obveznosti, povezanih z visokotveganimi sistemi.

VIRI IN LITERATURA

- Bagari, S., Tveganja pri uvajanju UI v delovna razmerja in možne pravne rešitve, Delavci in delodajalci, 2023, letnik 23, št. 2-3, str. 237-238.
- De Stefano, V., Negotiating the Algorithm: Automation, AI and labour protection, ILO Working Paper No. 246, 2018.
- EEOC, iTutorGroup to Pay \$365,000 to Settle EEOC Discriminatory Hiring Suit, 16. 5. 2022, <https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit>
- Eurofound, Italian Court rules that the Deliveroo Algorithm Discriminates Workers, 6. 1. 2022, <https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121>
- Evropska komisija, Smernice Komisije o prepovedanih praksah umetne inteligence, določenih v Uredbi (EU) 2024/1689 (akt o umetni inteligenci), 29.7.2025, <https://ec.europa.eu/newsroom/dae/redirection/document/118647>
- Ferrer X. et al., Bias and discrimination in UI: A cross-disciplinary perspective, IEEE Technology and Society Magazine, 2021, Vol. 40, No. 2.
- Gibson K., Amazon under fire for software that recommends firing workers, CBS News (MoneyWatch), 26. 4. 2019, <https://www.cbsnews.com/news/amazon-under-fire-for-software-that-recommends-firing-workers>

- Informacijski pooblaščenec, VARSTVO OSEBNIH PODATKOV V DELOVNIH RAZMERJIH, 25. 11. 2019, https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_koncna.pdf
- Nemac, L., UI in delovno pravo, magistrsko delo, 2023.
- Tribunale di Bologna, N. R.G. 2949/2019 (Filcams CGIL Bologna idr. proti Deliveroo Italia S.r.l.), odločba z dne 31. 12. 2020.
- Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (Besedilo velja za EGP), UL L, 2024/1689, 12.7.2024.
- Vlada Republike Slovenije, Besedilo Predloga zakona o izvajanju uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci, 22.8.2025, https://www.dz-rs.si/wps/portal/Home/zakonodaja/izbran/!ut/p/z/1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zivSy9Hb283Q0N3E3dLQwCQ7z9g7w8nAwsnMz1w9EUGAWZGgS6GDn5BhsYGwQHG-pHEaPfaAdwNCBOPx4FUfiNL8gNDQ11VFQEAAxcoa4!/dz/d5/L2dBISEvZ0FBIS9nQSEh/?uid=C1257A70003EE6A1C1258CEE00477E2C&db=kon_zak&mandat=IX&tip=doc#
- Zakon o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (ZIUDHPUI), Uradni list RS, št. 85/25.

Legal Aspects of the Use of Artificial Intelligence in Employment Relationships – Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence and the Slovenian Act Implementing the Regulation

Damjan Mašera*

Summary

AI is being increasingly deployed across the whole employment cycle - targeted job advertising, automated CV screening, video interviews, task allocation and performance scoring, and workplace monitoring. While such tools promise efficiency and objectivity, the AI algorithmic outputs can replicate or amplify historical bias and generate discrimination.

The EU AI Act (Regulation (EU) 2024/1689) introduces a risk-based framework directly applicable since 1 August 2024: unacceptable-risk practices are banned from 2 February 2025, including AI systems inferring a person's emotions at the workplace (Art. 5(1)(f), with a narrow health/safety exception). HR and employee-management systems that decide or materially support decisions on recruitment, promotion, evaluation, task allocation, worker monitoring and termination, are classified as high-risk (Annex III), with the core high-risk regime applying from 2 August 2026.

Employers, as deployers (users), must implement key organisational controls (Art. 26): use the system as intended and per instructions; assign competent staff for effective human oversight; ensure relevance/quality of input data under their control; monitor performance and report serious incidents; retain automatically generated logs for at least 6 months; and meet transparency duties, including prior information to workers' representatives/workers and notice to affected individuals that AI was used.

Slovenia complements the AI Act via the ZIUODHPUI (Official Gazette No. 85/25; in force 21 November 2025) by allocating supervisory competence (Agency for Communication Networks and Services of the Republic of Slovenia (AKOS) for employment/workforce-management high-risk systems, with coordination with sectoral inspectors) and setting administrative penalties for offences:

* Damjan Mašera, LL.B., Director of Expert Services at the Association of Employers of Slovenia

finances range from EUR 25,000–250,000 (or EUR 100,000–450,000 for large companies), and in particularly serious cases can reach up to EUR 35 million or 7% of worldwide annual turnover; for serious deployer breaches linked to high-risk obligations, ceilings reach up to EUR 15 million or 3% turnover. The article concludes that employers must map real AI use cases (including general-purpose generative AI models embedded in HR processes) and treat any tool that decisively shapes employment outcomes as part of the high-risk chain, while aligning AI Act duties with labour, data-protection and discrimination law.