Poročilo 5.1: Priporočila za ponudnike in uporabnike UI sistemov

Pripravili: Maja Škrjanc (IJS), Maruša Škrjanc (IJS)

Datum: 25. 10. 2026

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Kazalo

Povzetek za vodstvo....4
1 Uvod....6
1.1 Namen in naslovniki....6
1.2 Kako brati poročilo....6
1.3 Oznake priporočil....7
1.4 Razmejitev do drugih rezultatov projekta....7
1.5 Stanje virov in metoda....8
2 Širši okvir: skupna načela, različna pravila....10
2.1 Od načel do pravil....10
2.2 Zavezujoči okvir Sveta Evrope....10
2.3 Globalno upravljanje v okviru Združenih narodov....11
2.4 Orodja za organizacije....11
2.5 Kje mednarodni okviri segajo dlje od Akta o UI....12
2.6 Slovenska vpetost....12
3 Izhodišča....13
3.1 Kaj se uporablja in od kdaj....13
3.2 Vloge....14
3.3 Namen, ne tehnologija....14
3.4 Na čem temeljijo priporočila....15
4 Skupno jedro: kar potrebuje vsaka organizacija....17
4.1 Pregled nad sistemi....17
4.2 Ljudje in pravila....17
4.3 Podatki in kakovost....18
4.4 Napake, pritožbe in umik....19
4.5 Ena ureditev za več okvirov....19
4.6 Prvih 90 dni....20
5 Priporočila za ponudnike....21
5.1 Vloga in predvideni namen....21
5.2 Podatki in pristranskost....21
5.3 Preizkušanje, nadzor in varnost....22
5.4 Sistem vodenja kakovosti in dokumentacija....23
5.5 Ugotavljanje skladnosti in spremljanje na trgu....23
5.6 Preglednost....24
5.7 Modeli drugih ponudnikov, MSP in odgovornost....24
6 Priporočila za uvajalce....26
6.1 Pred odločitvijo....26
6.2 Izbira in naročanje....26
6.3 Pred uvedbo....27
6.4 Uporaba....27
6.5 Preglednost do ljudi....28
6.6 Obratovanje....28
6.7 Posebnosti javnega sektorja....29
7 Tehnološki profili....31
7.1 T1 Klasično strojno učenje za odločanje o ljudeh....31

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

7.2 T2 Klepetalniki in pisni asistenti na jezikovnih modelih....32
7.3 T3 Iskanje po znanju organizacije (RAG)....33
7.4 T4 Agenti UI....34
7.5 T5 Ustvarjanje slik, zvoka in videa....35
7.6 T6 Govor: prepoznava, zapisovanje in povzemanje....35
7.7 T7 Biometrija in prepoznavanje čustev....36
7.8 T8 UI v proizvodih in industriji....37
7.9 Profili po področjih uporabe....38
8 Priporočila za odločevalce in nadzornike....39
8.1 Jasna pravila in vodniki....39
8.2 Infrastruktura za skladnost....39
8.3 Javni sektor kot zgled....40
8.4 Sektorski okviri....40
8.5 Kompetence....40
8.6 Suverenost in odvisnost od ponudnikov....41
8.7 Mednarodno sodelovanje....41
8.8 Spremljanje....41
9 Časovni načrt in kazalniki....42
10 Zaključek....44
Viri....45
Pravni in izvedbeni viri Evropske unije in Slovenije....45
Mednarodni viri....46
Rezultati projekta NOSI-AI....47
Drugi viri....47
Priloga A: Pregled mednarodnih okvirov in drugih predpisov....48
Priloga B: Kontrolni seznam za uvajanje UI....49
Priloga C: Delovni list za presojo lastnega primera....52
Priloga D: Preslikava priporočil na vire....53
Priloga E: Slovar izrazov....58
Priloga F: Preslikava mednarodnih okvirov na Akt o UI in priporočila....60

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Povzetek za vodstvo

Poročilo R5.1 je zaključni rezultat projekta NOSI-AI. Ponudnikom in uvajalcem sistemov UI ter odločevalcem daje priporočila, ki povezujejo ugotovitve rezultatov R1.1 do R4.3 z najnovejšimi instrumenti Evropske unije in s širšim mednarodnim okvirom. Priporočila so zapisana kot ukrepi. Za vsakega je navedeno, ali gre za zakonsko zahtevo, smernico ali dobro prakso, kaj je dokaz izvedbe in do kdaj naj bo ukrep izveden.

Osrednja ugotovitev projekta je, da tveganja sistema UI pogosto ne določa tehnologija, temveč namen uporabe in način uvedbe. Isti jezikovni model je lahko pomočnik za pisanje brez posebnih obveznosti ali visokotvegani sistem za izbor kandidatov. Zato so priporočila razvrščena po vlogah: skupno jedro velja za vse, sledijo priporočila za ponudnike, uvajalce in odločevalce. Posebnosti posameznih tehnologij so zbrane v kratkih tehnoloških profilih.

Deset ključnih priporočil:

- **Popis.** Popišite vse sisteme UI, tudi orodja, ki jih zaposleni uporabljajo sami, in za vsakega zapišite namen, vlogo in odgovorno osebo (S-1).
- **Razvrstitev po namenu.** Razvrstitev dokumentirajte glede na namen uporabe in jo ponovite ob vsaki spremembi namena, modela ali funkcije (S-2, S-3).
- **Pismenost po vlogah.** Ukrepe za pismenost na področju UI načrtujte po vlogah in jih povežite z uvedbo konkretnih sistemov (S-5).
- **Najprej podatki, nato rešitev.** Pred izbiro rešitve razvrstite podatke. Razred podatkov določa, kje sme model teči in kateri ponudniki pridejo v poštev (S-7).
- **Merila pred uvedbo.** Pred uvedbo določite merila uspeha in pripravite lasten nabor preizkusnih primerov. Brez tega ne morete dokazati, da sistem deluje, niti primerjati ponudnikov (S-8, U-4).
- **Dejanski človeški nadzor.** Merite, kolikokrat ljudje predlog sistema popravijo ali zavrnejo. Nadzor, pri katerem nihče nikoli ne odstopi od predloga, je le formalen (U-7).
- **Ponudniki: namen in kakovost.** Ponudniki naj predvideni namen in izključene rabe jasno zapišejo v navodila in promocijsko gradivo, saj s tem določijo meje svoje odgovornosti in odgovornosti uvajalca. Ponudniki visokotveganih sistemov naj sistem vodenja kakovosti gradijo na SIST EN 18286:2026, ki je trenutno edini harmonizirani standard za Akt o UI (P-2, P-9).
- **Pogodbe z dobavitelji.** Uvajalci naj v pogodbe vključijo obveznost obveščanja o spremembah, prepoved uporabe svojih podatkov za učenje modelov brez soglasja in pogoje za varen izstop (U-3).
- **Javni sektor kot zgled.** Organi javnega sektorja naj objavijo vse sisteme UI v uporabi po 21. členu ZIUDHPUI, v javnih klepetalnikih pa zagotovijo obvestilo o UI in pot do človeka (U-13, U-16).
- **Podpora države.** Država naj do leta 2027 zagotovi vodnika za razvrščanje in za EN 18286, delujoč peskovnik pri AKOS ter preizkusne nabore v slovenščini (O-1, O-3, O-4).

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Časovno so ukrepi razporejeni v tri obdobja. Takoj, do 2. decembra 2026, je treba urediti tisto, kar se že uporablja: prepovedi, pismenost, preglednost po 50. členu in javno objavo v javnem sektorju. Do 2. decembra 2027 morajo biti izpolnjene zahteve za visokotvegane sisteme iz Priloge III, do 2. avgusta 2028 pa za sisteme iz Priloge I. Odlog visokotveganih obveznosti z digitalnim omnibusom ni odpustek: priprava sistema vodenja kakovosti, tehnične dokumentacije in preizkusov traja več mesecev.

Poglavje 2 umešča priporočila v širši mednarodni okvir. Načela OECD, Priporočilo UNESCO o etiki UI, Okvirna konvencija Sveta Evrope in orodja OECD za potrebno skrbnost se z Aktom o UI v veliki meri pokrivajo. Organizacija, ki izvaja priporočila iz tega poročila, zato izpolni tudi večino pričakovanj mednarodnih okvirov. Ti ponekod segajo dlje od Akta o UI, zlasti pri pritožbenih poteh, vključevanju deležnikov in okoljskem vplivu. Te vsebine poročilo vključuje kot dobre prakse.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

1 Uvod

1.1 Namen in naslovniki

Poročilo je rezultat naloge 5.1 projekta NOSI-AI »Izdelava zaključnega poročila s priporočili za ponudnike in uporabnike UI sistemov«. Prejšnji rezultati projekta so obravnavali pravni okvir (R1.1) [32], standarde (R1.3, R2.2, R4.1) [33, 34, 36] in dobre prakse uvajanja (R2.3, R4.3) [35, 37]. To poročilo njihove ugotovitve prevede v priporočila, ki jih organizacija lahko neposredno izvede in preveri.

Poročilo je namenjeno trem skupinam naslovnikov:

- **Ponudnikom,** to je organizacijam, ki sistem UI razvijejo ali ga dajo razviti in ga dajo na trg ali v uporabo pod svojim imenom. Mednje sodijo tudi organizacije, ki sistem razvijejo samo za lastno rabo, in tiste, ki na modelu drugega ponudnika zgradijo lastno rešitev.
- **Uvajalcem,** to je organizacijam, ki sistem UI uporabljajo pri svoji dejavnosti, v zasebnem ali javnem sektorju.
- **Odločevalcem,** to je ministrstvom, nadzornim organom in standardizacijskim telesom, ki oblikujejo pogoje, v katerih ponudniki in uvajalci izpolnjujejo zahteve.

Naslov poročila uporablja izraz »uporabniki«, kot ga je določil program dela projekta. Akt o UI za osebo ali organizacijo, ki sistem UI uporablja v svoji pristojnosti, razen pri osebni nepoklicni dejavnosti, uporablja izraz »uvajalec« (člen 3(4)) [1], zato ga uporabljamo tudi v besedilu. Fizične osebe, na katere se izhod sistema nanaša, imenujemo »osebe, na katere sistem vpliva«.

1.2 Kako brati poročilo

Poročilo ni namenjeno branju od začetka do konca. Bralec najprej odgovori na tri vprašanja: kakšna je njegova vloga (razdelek 3.2), ali namen uporabe sodi med prepovedane, visokotvegane ali preglednostne primere (razdelek 3.3) in katero tehnologijo uporablja (poglavje 7). Odgovori ga usmerijo k ustreznim delom poročila (Preglednica 1).

Preglednica 1: Kateri deli poročila so namenjeni posameznim naslovnikom

Naslovnik	Obvezno branje	Priporočeno
Vsaka organizacija, ki uporablja ali razvija UI	poglavji 3 in 4	poglavje 2, ustrezni profil iz poglavja 7
Ponudnik	poglavja 3, 4 in 5, ustrezni profil iz poglavja 7	poglavje 6 (kaj uvajalec potrebuje od ponudnika), poglavje 9
Uvajalec v zasebnem sektorju	poglavja 3, 4 in 6, ustrezni profil iz poglavja 7	razdelek 5.4 (kaj morajo vsebovati navodila), poglavje 9
Organ javnega sektorja kot uvajalec	poglavja 3, 4 in 6, zlasti razdelek 6.7	poglavji 8 in 9

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Naslovnik	Obvezno branje	Priporočeno
Odločevalci in nadzorniki	poglavja 2, 8 in 9	poglavja 4–7 (kaj se pričakuje od organizacij)

1.3 Oznake priporočil

Vsako priporočilo ima oznako, ki pove, komu je namenjeno: S za skupno jedro, P za ponudnike, U za uvajalce, T za tehnološke profile in O za odločevalce. Pod priporočili S, P, U in T je vrstica z vrsto, podlago, dokazom izvedbe, rokom, ravnjo in virom, pod priporočili za odločevalce pa naslovniki, rok in vir. Ločimo tri vrste priporočil:

- **Zahteva:** obveznost iz Akta o UI, GDPR ali ZIUDHPUI. Neizpolnitev je kršitev predpisa.
- **Smernica:** izhaja iz nezavezujočih smernic Komisije ali kodeksa prakse. Nadzorniki jih bodo pri presoji upoštevali, niso pa pravno zavezujoče.
- **Dobra praksa:** izhaja iz primerov, ki jih je obravnaval projekt, in iz mednarodnih okvirov. Ne ustvarja nove obveznosti, olajša pa izpolnjevanje zahtev in dokazovanje skrbnosti.

Rok je naveden kot »že velja«, »takoj« (do 2. 12. 2026), »do 2. 12. 2027« (Priloga III), »do 2. 8. 2028« (Priloga I) ali »stalno«. Raven »osnovno« pomeni, da je ukrep smiseln za vsako organizacijo ne glede na velikost. Raven »napredno« velja za organizacije z visokotveganimi sistemi ali z večjim številom sistemov. Izvedba dobre prakse sama po sebi ne pomeni domneve o skladnosti.

1.4 Razmejitev do drugih rezultatov projekta

Poročilo ne ponavlja vsebin prejšnjih rezultatov, temveč se nanje sklicuje (Preglednica 2).

Preglednica 2: Razmejitev R5.1 do drugih rezultatov projekta NOSI-AI

Rezultat	Kaj obravnava	Kako se R5.1 nanj navezuje
R1.1 (30. 3. 2025)	Pravni okvir Akta o UI za visokotvegane sisteme.	Pravne razlage ne ponavlja. Člene navaja, kadar so podlaga priporočila.
R1.3 (30. 6. 2025) in Observatorij standardov UI	Katalog standardov z opisi in povezavami z Aktom o UI.	Standarde navaja kot orodja za izvedbo priporočil. Podrobnosti so v Observatoriju.
R2.2 in R4.1	Standardizacijski okvir, EN 18286, nacionalni prevzem, simulacija preizkušanja.	Prevzame ugotovitve o sistemu vodenja kakovosti, preizkušanju in ugotavljanju skladnosti.
R2.3 in R4.3	Enajst primerov dobrih praks, štirinajst skupnih vzorcev, kontrolni seznam in delovna orodja (Priloge A–D).	Glavni vir priporočil. Primerov ne opisuje znova, temveč se nanje sklicuje.
Sodelovanje s SIST	Predstavitve rezultatov projekta in strokovne razprave z deležniki iz standardizacije.	Izkušnje iz teh razprav so upoštevane pri priporočilih. Podrobneje o sodelovanju R4.1 (razdelek 1.4).

Rezultat	Kaj obravnava	Kako se R5.1 nanj navezuje
R5.2	Trajnostni načrt in dokumentacija tehničnih predlogov za nacionalne standarde.	Predaje dokumentacije in nadaljevanja dejavnosti ne obravnava. Poglavje 8 navaja le, kaj naj institucije storijo, da bodo ponudniki in uvajalci lahko izpolnili zahteve.

1.5 Stanje virov in metoda

Poročilo odraža stanje na dan 25. oktobra 2026. Priporočila so izpeljana iz treh skupin virov: iz rezultatov projekta, iz zavezujočih predpisov in nezavezujočih instrumentov Evropske unije ter iz mednarodnih okvirov. Kjer smernice Komisije še niso dokončne, priporočilo to navede in predlaga ravnanje do njihove objave. Stanje ključnih instrumentov povzema Preglednica 3.

Preglednica 3: Stanje ključnih instrumentov Evropske unije in Slovenije na dan 25. 10. 2026

Instrument	Stanje	Kje v poročilu
Akt o UI (Uredba (EU) 2024/1689), kot ga je spremenila Uredba (EU) 2026/1744 [1, 2]	Zavezujoč; časovnica v razdelku 3.1.	vse
Smernice o opredelitvi sistema UI (6. 2. 2025) in o prepovedanih praksah (4. 2. 2025)	Končni, nezavezujoči.	3.3, profil T7
Smernice za ponudnike modelov UI za splošne namene, kodeks prakse za te modele in predloga povzetka učnih vsebin (julij 2025)	Končni, nezavezujoči.	P-15, profili T2–T4
Smernice k 50. členu (vsebina potrjena 20. 7. 2026) in kodeks prakse za preglednost vsebin, ustvarjenih z UI (10. 6. 2026), z naborom ikon EU za označevanje [4–6]	Nezavezujoči; kodeks je Komisija ocenila kot ustreznega.	P-13, P-14, U-10
Odgovori na pogosta vprašanja o pismenosti na področju UI, posodobljeni po digitalnem omnibusu [10]	Nezavezujoči.	S-5
Smernice za razvrščanje visokotveganih sistemov po 6. členu [7]	Osnutek z dne 19. 5. 2026.	3.3, S-2
Smernice in predloga za poročanje o resnih incidentih [9]	Osnutek z dne 26. 9. 2025. Pregledna stran Komisije predlogo navaja med objavljenimi gradivi [8], končnega besedila nismo našli.	P-12, U-11

Instrument	Stanje	Kje v poročilu
Predloga za oceno učinka na temeljne pravice; smernice o odgovornostih v vrednostni verigi, bistveni spremembi, spremljanju po dajanju na trg, poenostavljenem sistemu vodenja kakovosti za MSP in mala podjetja s srednje veliko tržno kapitalizacijo ter razmerju do drugih predpisov, vključno s skupnimi smernicami Komisije in EDPB o varstvu podatkov [8]	Napovedani; smernice o razmerju do sektorske zakonodaje so po digitalnem omnibusu predvidene do 1. 8. 2027, druge brez datuma.	v besedilu kot »do objave smernic«
SIST EN 18286:2026 – sistem vodenja kakovosti [3]	Harmonizirani standard; sklic objavljen v UL EU 14. 10. 2026.	P-9
Vzorčne pogodbene klavzule EU za javno naročanje UI (MCC-AI) [12]	Prostovoljne.	U-3, U-15
ZIUDHPUI [17]	Zavezujoč od 21. 11. 2025.	6.7, poglavje 8

Poročilo ni pravno mnenje. Razvrstitev konkretnega sistema in presoja skladnosti sta odvisni od njegovega namena, zasnove in okoliščin uporabe, zato ju mora organizacija opraviti sama ali s pomočjo strokovnjakov.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

2 Širši okvir: skupna načela, različna pravila

Akt o UI ni osamljen instrument. Njegova načela izhajajo iz Etičnih smernic za zaupanja vredno UI, ki jih je leta 2019 pripravila strokovna skupina na visoki ravni pri Evropski komisiji (uvodna izjava 27) [43], in se v veliki meri ujemajo z mednarodnimi priporočili, sprejetimi med letoma 2019 in 2021. Nanj se navezujejo tudi novejši zavezujoči in nezavezujoči instrumenti. Za slovenske organizacije je to pomembno iz treh razlogov. Prvič, podjetja, ki delujejo tudi zunaj Evropske unije, srečujejo različna pravila, ki pa temeljijo na skupnih načelih, zato lahko ena dobro zasnovana ureditev pokrije več okvirov. Drugič, mednarodni okviri ponekod segajo dlje od Akta o UI in kažejo, v katero smer se razvija dobra praksa. Tretjič, Slovenija ima v mednarodnem upravljanju UI prepoznavno vlogo, kar odpira možnosti za sodelovanje.

2.1 Od načel do pravil

Prvi medvladni dogovor o načelih zaupanja vredne UI je Priporočilo Sveta OECD o umetni inteligenci iz maja 2019, ki ga je OECD maja 2024 posodobil, med drugim zaradi razvoja generativne UI [19]. Načela OECD zajemajo vključujočo rast in trajnostni razvoj, spoštovanje pravne države, človekovih pravic in demokratičnih vrednot, vključno s pravičnostjo in zasebnostjo, preglednost in razložljivost, robustnost, varnost in zaščito ter odgovornost. Opredelitev sistema UI v Aktu o UI je usklajena z opredelitvijo OECD.

Priporočilo UNESCO o etiki umetne inteligence so novembra 2021 sprejele vse države članice UNESCO [20]. Je prvi globalni normativni instrument na tem področju. Poleg vrednot in načel določa enajst področij politik, med drugim okolje, enakost spolov, izobraževanje, zdravje ter delo in gospodarstvo. Za izvajanje sta na voljo dve orodji: metodologija za oceno pripravljenosti držav (RAM) in ocena etičnega učinka (EIA), ki je namenjena zlasti javnim uslužbencem pri naročanju sistemov UI [21, 22].

Države skupine G7 so oktobra 2023 v okviru hirošimskega procesa sprejele mednarodna vodilna načela in kodeks ravnanja za organizacije, ki razvijajo napredne sisteme UI. Na njih temelji okvir za javno poročanje, ki ga vodi OECD (razdelek 2.4) [29].

2.2 Zavezujoči okvir Sveta Evrope

Okvirna konvencija Sveta Evrope o umetni inteligenci in človekovih pravicah, demokraciji in pravni državi (CETS št. 225) je prva mednarodna pogodba na tem področju. Za podpis je bila odprta 5. septembra 2024. Do septembra 2026 jo je podpisalo 21 podpisnic, med njimi Švica, Kanada, Japonska in Združene države [24]. Evropska unija jo je ratificirala 15. maja 2026 kot prva pogodbenica [23, 24] in jo izvaja prek Akta o UI [44]. Konvencija začne veljati, ko jo ratificira pet podpisnic, med njimi vsaj tri države članice Sveta Evrope. Ob pripravi poročila še ni veljala.

Za uvajalce je uporabna metodologija HUDERIA za oceno tveganj in vpliva sistemov UI na človekove pravice, demokracijo in pravno državo. Odbor ministrov jo je potrdil 26. februarja 2025, model za njeno izvedbo pa 25. februarja 2026. Metodologija ima štiri sestavine: analizo tveganj glede na kontekst, vključevanje deležnikov, oceno tveganj in vpliva ter načrt blažitve, ki vključuje tudi pravna sredstva. Ni zavezujoča in je namenjena javnim in zasebnim akterjem

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

[25]. Dopolnjuje oceno učinka na temeljne pravice po 27. členu Akta o UI, zlasti pri vključevanju oseb, na katere sistem vpliva (U-5).

2.3 Globalno upravljanje v okviru Združenih narodov

Generalna skupščina Združenih narodov je septembra 2024 sprejela Globalni digitalni dogovor. Na njegovi podlagi je z resolucijo 79/325 z dne 26. avgusta 2025 ustanovila dva mehanizma [26]:

- **Neodvisni mednarodni znanstveni panel za UI** ima 40 članov in pripravlja letna poročila o priložnostih, tveganjih in učinkih UI. Predhodno poročilo je objavil 1. julija 2026.
- **Globalni dialog o upravljanju UI** se je začel 25. septembra 2025 v New Yorku. Prvo zasedanje je bilo 6. in 7. julija 2026 v Ženevi, drugo bo leta 2027 v New Yorku.

Nobeden od mehanizmov ne sprejema zavezujočih pravil. Njun pomen je v skupni znanstveni podlagi in v usklajevanju pristopov, kar bo dolgoročno vplivalo tudi na izvajanje Akta o UI. Vzporedno potekajo mednarodni vrhovi o UI. Po Bletchleyju (2023), Seulu (2024) in Parizu (2025) je bil februarja 2026 vrh v New Delhiju, ki se je končal z deklaracijo o vplivu UI [27]. Poudarek vrhov se je premaknil od varnosti najzmogljivejših modelov k širši uporabi in učinkom UI.

2.4 Orodja za organizacije

Za podjetja in javne organizacije so najbolj uporabna orodja, ki načela prevedejo v postopke:

- **Smernice OECD o potrebni skrbnosti za odgovorno UI** (19. februar 2026) so namenjene podjetjem v celotni vrednostni verigi UI [28]. Sledijo šestim korakom iz Smernic OECD za večnacionalna podjetja: vključitev odgovornega ravnanja v politike in sisteme vodenja, prepoznavanje in ocena škodljivih učinkov, preprečevanje in blažitev, spremljanje izvajanja, obveščanje o ukrepih ter zagotavljanje pravnih sredstev ali sodelovanje pri njih. Vsak korak je povezan z obstoječimi okviri, vključno z Aktom o UI.
- **Okvir za poročanje po hirošimskem procesu, različica 2.0** (28. maj 2026) omogoča prostovoljno javno poročanje organizacij, ki razvijajo napredne sisteme UI [29]. Vprašanja so urejena po vlogah (razvijalci modelov, razvijalci aplikacij, uvajalci), okvir je prilagojen tudi MSP in vključuje agente UI. Poročati je namenilo več kot 50 organizacij.
- **Ocena etičnega učinka UNESCO** je vprašalnik za oceno sistema skozi življenjski cikel, uporaben zlasti pri javnem naročanju [22].
- **Mednarodni standardi za upravljanje UI,** zlasti ISO/IEC 42001 (sistem vodenja), ISO/IEC 23894 (obvladovanje tveganj) in ISO/IEC 42005 (ocena vpliva), se uporabljajo ne glede na pravni okvir. Preslikava med EN 18286 in ISO/IEC 42001 je v Prilogi A k R4.1 [36].

Organizacija, ki izvaja priporočila iz poglavij 4–6 tega poročila, izpolni večino pričakovanj teh orodij: popis in razvrstitev ustrezata prepoznavanju učinkov, ocena učinka in preizkusi ocenjevanju in blažitvi, spremljanje in javna objava pa spremljanju in obveščanju. Razlike so zbrane v naslednjem razdelku.

2.5 Kje mednarodni okviri segajo dlje od Akta o UI

Akt o UI ureja predvsem varnost izdelkov in temeljne pravice pri visokotveganih sistemih. Mednarodni okviri so širši. Področja, na katerih segajo dlje, povzema Preglednica 4. Poročilo jih vključuje kot dobre prakse.

Preglednica 4: Področja, na katerih mednarodni okviri segajo dlje od Akta o UI

Področje	Mednarodni okvir	Akt o UI	Priporočilo R5.1
Pritožbe in pravna sredstva	Smernice OECD o potrebni skrbnosti (korak 6), HUDERIA, UNESCO	Pritožba pri organu za nadzor trga (85. člen), pravica do pojasnila (86. člen), pritožbeni mehanizmi kot del ocene po 27. členu	S-10, U-16
Vključevanje deležnikov	Smernice OECD o potrebni skrbnosti, HUDERIA	Obveščanje delavcev (člen 26(7)); splošnega posvetovanja ne zahteva	U-5, U-6
Okoljski vpliv	UNESCO (okolje in ekosistemi), OECD (trajnostni razvoj)	Podatki o porabi energije le za modele UI za splošne namene; prostovoljni kodeksi ravnanja (95. člen)	S-13
Delo v dobavni verigi	Smernice OECD za večnacionalna podjetja in o potrebni skrbnosti	Ni urejeno	U-3 (napredno)
Javno poročanje	Okvir za poročanje po hirošimskem procesu	Registracija v podatkovni zbirki EU za visokotvegane sisteme; javna objava po 21. členu ZIUDHPUI za javni sektor	U-13, U-15
Jezik in dostopnost	Globalni digitalni dogovor, UNESCO (kulturna in jezikovna raznolikost)	Zahteve glede dostopnosti za visokotvegane sisteme (člen 16(l))	S-8, P-6

2.6 Slovenska vpetost

Slovenija je v mednarodnem upravljanju UI dejavna na več ravneh. Na Institutu »Jožef Stefan« deluje Mednarodni raziskovalni center za umetno inteligenco pod okriljem UNESCO (IRCAI). Februarja 2024 je Slovenija na Brdu pri Kranju pod pokroviteljstvom UNESCO gostila drugi Globalni forum o etiki UI z več kot 600 udeleženci iz skoraj 70 držav. Na robu foruma se je osem tehnoloških podjetij z UNESCO zavezalo k razvoju UI v skladu z njegovim priporočilom [31]. Slovenija je ustanovna članica Globalnega partnerstva za UI (GPAI), ki se je julija 2024 združilo z OECD [30]. Nacionalna strategija UI do leta 2030 med petimi cilji navaja tudi mednarodno vpetost in ugled Slovenije na področju UI [18].

Za ponudnike in uvajalce to pomeni dostop do mednarodnih mrež in orodij. Za odločevalce pa pomeni priložnost, da slovenske izkušnje, na primer javno objavo sistemov UI po 21. členu ZIUDHPUI, vnesejo v mednarodne razprave (poglavje 8).

3 Izhodišča

Poglavje na kratko povzema pravna izhodišča, ki jih priporočila predpostavljajo. Podrobna pravna razlaga je v R1.1 in R4.3, standardi pa so obravnavani v R1.3, R2.2 in R4.1.

3.1 Kaj se uporablja in od kdaj

Akt o UI velja od 1. avgusta 2024, njegove določbe pa se uporabljajo postopoma. Digitalni omnibus, ki velja od 27. julija 2026, je zamaknil roke za visokotvegane sisteme, obstoječih rokov za prepovedi, modele UI za splošne namene in preglednost pa ni zamaknil. Dodal je nove prepovedi, ki se uporabljajo od 2. decembra 2026, in prehodno obdobje za člen 50(2) [1, 2]. Preglednica 5 povzema roke, ki so pomembni za priporočila.

Preglednica 5: Roki, pomembni za priporočila

Od	Kaj se uporablja	Koga zadeva
2. 2. 2025	Prepovedane prakse (5. člen) in pismenost na področju UI (4. člen, od 27. 7. 2026 v spremenjeni obliki).	vse ponudnike in uvajalce
2. 8. 2025	Obveznosti ponudnikov modelov UI za splošne namene (53.–55. člen); upravljanje in kazni (99. in 100. člen).	ponudnike modelov; vse
21. 11. 2025	ZIUDHPUI: pristojni organi, nadzor, javna objava sistemov UI v javnem sektorju (21. člen) [17].	vse; javni sektor
2. 8. 2026	Obveznosti glede preglednosti (50. člen), nadzor organov za nadzor trga, globe Komisije za ponudnike modelov UI za splošne namene (101. člen).	ponudnike in uvajalce
2. 12. 2026	Označevanje izhodov po členu 50(2) tudi za generativne sisteme, dane na trg pred 2. 8. 2026; nova prepoved sistemov za ustvarjanje nekonsenzualnih intimnih posnetkov in gradiva spolne zlorabe otrok.	ponudnike generativnih sistemov
2. 8. 2027	Vsaj en delujoč nacionalni regulativni peskovnik.	AKOS, ponudnike
2. 12. 2027	Zahteve za visokotvegane sisteme iz Priloge III.	ponudnike in uvajalce
2. 8. 2028	Zahteve za visokotvegane sisteme iz Priloge I (UI v reguliranih proizvodih).	ponudnike proizvodov
2. 8. 2030	Rok za visokotvegane sisteme, namenjene javnim organom, ki so bili dani na trg ali v uporabo pred začetkom uporabe zahtev (111. člen).	javni sektor

Odlog ni odpustek. Prepovedi, pismenost, preglednost, obveznosti za modele UI za splošne namene in nacionalni nadzor se že uporabljajo. Zamik rokov za visokotvegane sisteme pomeni več časa za pripravo, ne manj dela. Priprava sistema vodenja kakovosti, tehnične dokumentacije in preizkusov traja več mesecev.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

3.2 Vloge

Obveznosti po Aktu o UI so vezane na vlogo, ki jo ima organizacija pri posameznem sistemu. Vloga ni odvisna od pogodbe, temveč od tega, kaj organizacija dejansko počne (člena 3 in 25) [1]. Ista organizacija ima lahko pri različnih sistemih različne vloge. Najpogostejše primere povzema Preglednica 6.

Preglednica 6: Vloga organizacije glede na to, kaj počne s sistemom

Kaj organizacija počne	Vloga po Aktu o UI	Posledica
Kupljeno ali najeto orodje uporablja tako, kot ga je zasnoval ponudnik.	uvajalec	4. člen; uporaba po navodilih; člen 50(3) in (4); pri visokotveganem namenu 26. člen in po potrebi 27. člen.
Na model drugega ponudnika zgradi lastno rešitev in jo ponudi strankam ali zaposlenim pod svojim imenom.	ponudnik sistema UI	Člen 50(1); pri visokotveganem namenu 9.–17. člen in ugotavljanje skladnosti. Obveznosti za model ostanejo pri ponudniku modela.
Sistem razvije sama, tudi samo za lastno rabo.	ponudnik (dajanje v uporabo, člen 3(11))	Kot zgoraj.
Kupljen visokotvegani sistem označi s svojim imenom ali ga bistveno spremeni.	ponudnik (člen 25(1) (a) in (b))	Vse obveznosti ponudnika visokotveganega sistema.
Sistemu, ki ni bil visokotvegan, spremeni namen tako, da postane visokotvegan.	ponudnik (člen 25(1) (c))	Vse obveznosti ponudnika visokotveganega sistema.
Razvija model UI za splošne namene.	ponudnik modela	53.–55. člen; nadzor Urada za UI.
Sistem razvija ali preizkuša v raziskovalne namene, preden ga da na trg ali v uporabo.	zunaj področja uporabe (člen 2(6) in (8))	Do dajanja na trg ali v uporabo. Preizkušanje v realnih razmerah ni izvzeto.

Vloge po Aktu o UI se ne ujemajo z vlogami po GDPR. Organizacija je lahko hkrati uvajalka po Aktu o UI in upravljavka osebnih podatkov, ponudnik jezikovnega modela pa je lahko obdelovalec ali samostojni upravljavec, odvisno od namena obdelave. Evropski nadzornik za varstvo podatkov v smernicah za institucije EU poudarja, da je vloge treba presojati za vsak primer posebej, lahko tudi ločeno za razvoj in uporabo [13]. Obe presoji je treba dokumentirati ločeno.

3.3 Namen, ne tehnologija

Razvrstitev sistema je odvisna od njegovega predvidenega namena, kot ga ponudnik opiše v navodilih za uporabo, promocijskem gradivu in tehnični dokumentaciji (člen 3(12)) [1]. Sistem s področja Priloge III je visokotvegan, razen če ponudnik dokumentira, da ne pomeni znatnega tveganja, ker opravlja le ozko postopkovno ali pripravljalno nalogo, izboljša rezultat že opravljene človeške dejavnosti ali zaznava odstopanja od vzorcev odločanja (člen 6(3)). Sistem s področja Priloge III, ki profilira fizične osebe, je vedno visokotvegan. Osnutek smernic Komisije izjemo razlaga ozko. Pri večnamenskih sistemih šteje, da predvideni namen zajema tudi visokotvegane rabe, razen če jih ponudnik jasno in dosledno izključi v vseh gradivih; izjava v pogojih uporabe ne zadošča [7].

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Iz tega sledita dve praktični posledici. Prva: splošno orodje, ki ga organizacija uporabi za razvrščanje kandidatov ali za odločanje o kreditu, je pri tej uporabi visokotvegano, čeprav ponudnik tega ni predvidel. Organizacija lahko s tem po členu 25(1)(c) postane ponudnica. Druga: Akt o UI ne pozna posebne kategorije agentov UI. Zanje veljajo enaka pravila kot za druge sisteme UI, odločilen pa je predvideni namen [11]. Preglednica 7 prikazuje razvrstitev tipičnih primerov uporabe. Za dokumentiranje razvrstitve je na voljo delovni list v Prilogi A k R4.3, ilustrativni primer v Prilogi D k R4.3, slovenski primeri pa so v razdelku 8.6 R4.1 [36, 37].

Preglednica 7: Tipični primeri uporabe in njihova razvrstitev

Primer uporabe	Razvrstitev	Glavna obveznost
Klepetalnik za pomoč strankam na jezikovnem modelu	preglednost (člen 50(1))	Obvestilo, da gre za UI, najpozneje ob prvem stiku (člen 50(5)).
Pomočnik za pisanje dopisov in povzetkov za interno rabo	brez posebnih obveznosti po Aktu o UI	4. člen, GDPR; človeški pregled kot dobra praksa.
Iskanje po notranjih dokumentih z RAG	brez posebnih obveznosti, dokler ne vpliva na odločitve o ljudeh	GDPR, nadzor dostopa do dokumentov, 4. člen.
Predizbor in ocenjevanje kandidatov za zaposlitev	visokotvegano (Priloga III, točka 4(a))	Ponudnik: 9.–17. člen in ugotavljanje skladnosti; uvajalec: 26. člen.
Ocenjevanje kreditne sposobnosti fizičnih oseb	visokotvegano (Priloga III, točka 5(b))	Kot zgoraj; uvajalec tudi ocena učinka na temeljne pravice (27. člen).
Zaznavanje finančnih goljufij	ni na seznamu Priloge III (izrecna izjema v točki 5(b))	GDPR, sektorski predpisi; dobra praksa.
Prepoznavanje čustev pri zaposlenih ali v šoli	prepovedano (člen 5(1)(f))	Ne uvajati, razen iz zdravstvenih ali varnostnih razlogov.
Strojni vid za kontrolo kakovosti v proizvodnji	praviloma ni visokotvegano; po omnibusu ni varnostna komponenta, če se uporablja le za vidike, ki niso povezani z varnostjo (člen 6(1a))	Sektorski predpisi o strojih; dobra praksa.

3.4 Na čem temeljijo priporočila

Projekt je obravnaval enajst dokumentiranih primerov iz evropske in slovenske prakse: štiri v R2.3 (France Travail, Finterai, Albert API, helsinški register sistemov UI) in sedem v R4.3 (smernice ORF, španski peskovnik, nizozemski primer DUO z oceno IAMA in registrom algoritmov, javna objava po 21. členu ZIUDHPUI, nemški agenti UI v občinah, angleški zapisovalniki v zdravstvu in estonski program AI Leap) [35, 37]. Iz primerov je izpeljal štirinajst skupnih vzorcev (Preglednica 8). Priporočila v poglavjih 4–6 jih prevajajo v ukrepe.

Preglednica 8: Skupni vzorci dobrih praks iz R2.3 in R4.3

Št.	Vzorec	Vir
1	Vsebina interakcij ni enaka telemetriji.	R2.3
2	Človeški nadzor mora biti dejanski.	R2.3
3	Vhode je treba upravljati.	R2.3

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Št.	Vzorec	Vir
4	Infrastruktura in dobavna veriga sta del profila tveganja.	R2.3
5	Modeli in njihove posodobitve so varnostno občutljivi.	R2.3
6	Omejitve in kakovost je treba meriti in sporočiti.	R2.3
7	Kontrola mora preživeti prehode med sistemi, subjekti in fazami.	R4.3
8	Regulativni sklep temelji na predpostavkah, ki jih je treba spremljati.	R4.3
9	Dokazilo naj bo čim bližje ravnanju, ki ga dokazuje.	R4.3
10	Preglednost deluje na dveh ravneh, ki se ne nadomeščata.	R4.3
11	Pristranskost in vpliv na pravice je treba oceniti vnaprej in v celotnem postopku.	R4.3
12	Utemeljen negativen izid je del dobre prakse.	R4.3
13	Avtonomija sistema naj bo stopnjevana in vezana na človeško odobritev.	R4.3
14	Nacionalni okvir podpira uvajalca, odgovornosti pa ne prevzame.	R4.3

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

4 Skupno jedro: kar potrebuje vsaka organizacija

Ukrepi v tem poglavju veljajo za vsako organizacijo, ki razvija ali uporablja UI, ne glede na velikost in raven tveganja. So pogoj za vse, kar sledi. Brez popisa organizacija ne ve, katere obveznosti ima. Brez razvrstitve ne ve, kateri režim velja. Brez meril ne more dokazati, da sistem deluje. Večina ukrepov ni zahtevna in jih lahko izvede tudi majhno podjetje.

4.1 Pregled nad sistemi

- **S-1 Popišite vse sisteme UI, tudi neformalno rabo.** Za vsak sistem zapišite namen, lastnika procesa, ponudnika in različico, vlogo organizacije (uvajalec, ponudnik sistema, ponudnik modela ali zunaj področja uporabe), podatke, ki vstopajo v sistem, njihov razred zaupnosti, lokacijo obdelave in osebe, na katere sistem vpliva. Vključite tudi funkcije UI, vgrajene v programe, ki jih organizacija že uporablja (pisarniški paketi, sistemi za upravljanje odnosov s strankami, kadrovski sistemi), in orodja, ki jih zaposleni uporabljajo sami brez odobritve. Popis je temelj za vsa nadaljnja priporočila.

  Vrsta: dobra praksa; za javni sektor zahteva objave po 21. členu ZIUDHPUI · Dokaz: register sistemov UI · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.4), R2.3 (Helsinki)

- **S-2 Za vsak sistem pripravite razvrstitveni zapis.** Razvrstitev opravite po predvidenem namenu in dejanski uporabi, ne po tehnologiji: prepovedano, visokotvegano (Priloga I ali III), zavezano preglednosti po 50. členu ali brez posebnih obveznosti. Kategorije se lahko prekrivajo. Če se ponudnik sklicuje na izjemo po členu 6(3), mora presojo dokumentirati pred dajanjem na trg in sistem registrirati. Zapis naj navaja tudi predpostavke, na katerih razvrstitev temelji, na primer da sistem ne vpliva bistveno na odločitev. Uporabite delovni list iz Priloge A k R4.3.

  Vrsta: zahteva pri izjemi po členu 6(3) (člena 6(4) in 49(2)); sicer dobra praksa · Dokaz: razvrstitveni zapis · Rok: takoj za nove sisteme, do sredine leta 2027 za vse sisteme s področij Priloge III · Raven: osnovno · Vir: R4.3 (razdelek 5.2, Prilogi A in D), R4.1 (poglavje 8)

- **S-3 Razvrstitev ponovite ob vsaki spremembi.** Ponovna presoja je potrebna ob novem modelu ali različici, novi funkciji, razširjenem namenu, novi skupini oseb, spremembi ponudnika ali lokacije obdelave ter ob objavi končnih smernic ali harmoniziranih standardov, ki vplivajo na predpostavke razvrstitve. Vodite register predpostavk in ob spremembi preverite le odločitve, ki so od nje odvisne. Opozorilni znak je namen, ki se je razširil brez nove presoje.

  Vrsta: dobra praksa; pri visokotveganih sistemih zahteva ob bistveni spremembi (člena 3(23) in 43(4)) · Dokaz: dnevnik sprememb, register predpostavk · Rok: stalno · Raven: osnovno · Vir: R4.3 (vzorec 8, Priloga D)

4.2 Ljudje in pravila

- **S-4 Določite vloge in odgovornosti.** Za vsak sistem določite, kdo odloči o uvedbi, kdo je lastnik procesa, kdo nadzira delovanje, kdo lahko sistem ustavi in kdo poroča o napakah. V organizaciji imenujte osebo, ki skrbi za skladnost na področju UI in vsaj vsake tri mesece pregleda regulativne novosti. Primerna je oseba s pravnim znanjem

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

in razumevanjem tehnologije ali obratno. Brez jasnih vlog je odgovornost vseh in hkrati nikogar.

Vrsta: dobra praksa; pri visokotveganih sistemih podlaga za člen 26(2) · Dokaz: matrika odgovornosti · Rok: takoj · Raven: osnovno · Vir: R2.3, R4.3 (primer 4.5)

- **S-5 Ukrepe za pismenost načrtujte po vlogah.** Po spremenjenem 4. členu morajo ponudniki in uvajalci sprejeti ukrepe v podporo razvoju pismenosti svojega osebja in drugih oseb, ki v njihovem imenu uporabljajo sisteme UI. Pri tem upoštevajo njihovo znanje in okoliščine uporabe. Določena raven pismenosti ni predpisana, potrdilo ni potrebno, evidence pa so priporočene [10]. Ukrepe načrtujte ločeno za vodstvo, uporabnike izhodov, informatike in varnostnike, pravno službo in pooblaščeno osebo za varstvo podatkov ter razvijalce. Povežite jih z uvedbo konkretnih sistemov. Človeški nadzor brez razumevanja omejitev sistema je le formalen. V Sloveniji nad 4. členom bdi inšpekcija za informacijsko družbo.

  Vrsta: zahteva (4. člen) · Dokaz: načrt ukrepov po vlogah, evidenca usposabljanj · Rok: že velja · Raven: osnovno · Vir: R4.3 (razdelek 5.4, Preglednica 15)

- **S-6 Sprejmite pravilnik o rabi generativne UI.** Pravilnik naj določa seznam odobrenih orodij, katere vrste podatkov se v posamezna orodja ne smejo vnašati, obvezno preverjanje izhodov pri pravnih, finančnih in drugih pomembnih izjavah, pravila označevanja in ravnanje ob napaki. Dobro deluje preprost semafor: zelena za dovoljeno rabo, rumena za rabo s pogoji in rdeča za prepovedano. Pravilnik je hkrati ukrep pismenosti in odgovor na neformalno rabo orodij.

  Vrsta: dobra praksa (podpira 4. člen in GDPR) · Dokaz: pravilnik, seznam odobrenih orodij · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.1 ORF)

4.3 Podatki in kakovost

- **S-7 Najprej razvrstite podatke, nato izberite rešitev.** Razred podatkov določa, kje sme model teči. Za javne in notranje neobčutljive podatke je praviloma primerna zunanja storitev. Za poslovno občutljive in osebne podatke pride v poštev postavitev v izbrani oblačni regiji s pogodbeno izključeno uporabo podatkov za učenje. Za posebne vrste osebnih podatkov in regulirane podatke je primerna lokalna postavitev. Pri vsaki postavitvi preverite lokacijo obdelave, podobdelovalce, prenose v tretje države, roke hrambe in uporabo za učenje. Lokalna postavitev tveganj ne odpravi, temveč jih prerazporedi k notranji varnosti, dostopom in vzdrževanju.

  Vrsta: dobra praksa; GDPR (28., 32. in 44.–49. člen) zahteva · Dokaz: razvrstitev podatkov, presoja ponudnika · Rok: takoj, pred vsako novo uvedbo · Raven: osnovno · Vir: R2.3 (France Travail, Albert API), vzorec 4

- **S-8 Pred uvedbo določite merila uspeha in pripravite preizkusni nabor.** Pripravite od 50 do 200 reprezentativnih primerov iz dejanske rabe, ne iz predstavitve ponudnika, vključno s težkimi, dvoumnimi in redkimi primeri. Merila (točnost, čas, robustnost, razlike med skupinami uporabnikov, delež izmišljenih navedb) določite pred preizkusom, ne po njem. Pri slovenskih rešitvah vključite primere v slovenščini, tudi narečne in neformalne. Preizkus ponovite ob vsakem novem modelu ali različici. Brez preizkusnega nabora ne morete dokazati, da sistem deluje, niti da je nov model boljši.

  Vrsta: dobra praksa; za ponudnike visokotveganih sistemov zahteva (člen 9(6)–(8) in 15. člen) · Dokaz: preizkusni nabor, poročilo o preizkusu · Rok: pred uvedbo in stalno · Raven: osnovno · Vir: R4.1 (poglavje 9, Priloga B.3), vzorca 6 in 12

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

- **S-9 Vsebino interakcij ločite od telemetrije.** Določite, kaj se beleži (pozivi, izhodi, uporabljeni viri, odločitve), za kakšen namen, koliko časa in kdo ima dostop. Vsebino interakcij hranite le, kadar je potrebna za revizijo, analizo napak ali preverjanje pristranskosti, in časovno omejeno. Za spremljanje rabe zadoščajo podatki o uporabi brez vsebine. Pri visokotveganih sistemih mora uvajalec samodejno ustvarjene dnevnike hraniti najmanj šest mesecev (člen 26(6)).

  Vrsta: zahteva pri visokotveganih sistemih (člena 19 in 26(6)); sicer dobra praksa (GDPR, člen 5(1)(c) in (e)) · Dokaz: politika beleženja z roki hrambe · Rok: takoj · Raven: osnovno · Vir: R2.3 (Albert API, Helsinki), vzorec 1

4.4 Napake, pritožbe in umik

- **S-10 Vzpostavite pot za napake, incidente in pritožbe.** Določite, kdo sprejme prijavo napake od uporabnikov in od oseb, na katere sistem vpliva, kako se sistem začasno ustavi ali vrne na prejšnjo različico, kdaj se obvesti ponudnik in kdaj pristojni organ. Pri visokotveganih sistemih se resni incidenti prijavljajo po 73. členu, kršitve varstva osebnih podatkov po 33. členu GDPR, pri proizvodih z digitalnimi elementi pa tudi po Aktu o kibernetski odpornosti [15]. Osebam, na katere sistem vpliva, zagotovite notranjo pot za pritožbo in popravek. Mednarodni okviri to pričakujejo za vse sisteme, ki vplivajo na ljudi (razdelek 2.5).

  Vrsta: zahteva pri visokotveganih sistemih (člena 26(5) in 73) in pri kršitvah varstva podatkov (GDPR, 33. člen); sicer dobra praksa · Dokaz: postopek, evidenca incidentov in pritožb · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.6), Smernice OECD o potrebni skrbnosti [28]

- **S-11 Umik načrtujte ob uvedbi.** Že ob uvedbi določite, kako boste sistem umaknili: izvoz in izbris podatkov, hramba dnevnikov, prenos na drugega ponudnika in arhiviranje javnega vnosa. Ob umiku zabeležite datum, razlog in ravnanje s podatki. Sistem naj ima enolični identifikator, da je njegova zgodovina sledljiva. Odločitev, da sistem ne prinaša koristi in ga je treba ustaviti, je del dobre prakse, ne neuspeh.

  Vrsta: dobra praksa; za javni sektor 21. člen ZIUDHPUI · Dokaz: načrt izstopa, zapis o umiku · Rok: ob uvedbi in ob umiku · Raven: napredno · Vir: R4.3 (razdelek 3.4, vzorec 12)

4.5 Ena ureditev za več okvirov

- **S-12 Ureditev zasnujte tako, da pokrije več okvirov.** Organizacije, ki delujejo tudi zunaj Evropske unije, naj upravljanje UI zasnujejo na mednarodnem standardu sistema vodenja, na primer ISO/IEC 42001, in ga preslikajo na Akt o UI, Smernice OECD o potrebni skrbnosti in predpise ciljnih trgov. Tako en nabor postopkov in dokazil služi več namenom. Ponudniki visokotveganih sistemov naj sistem vodenja kakovosti po EN 18286 povežejo s sistemom vodenja UI po ISO/IEC 42001 (P-9).

  Vrsta: dobra praksa · Dokaz: sistem vodenja s preslikavo na okvire · Rok: stalno · Raven: napredno · Vir: poglavje 2, R4.1 (Priloga A)

- **S-13 Izberite sorazmeren model in spremljajte porabo virov.** Uporabite najmanjši model, ki dosega merila iz S-8. Spremljajte ceno na rešen primer, vključno s človeškim pregledom in popravki, ter porabo računskih virov. Večji model ni nujno boljši za konkretno nalogo, je pa dražji in okoljsko bolj obremenjujoč.

  Vrsta: dobra praksa · Dokaz: primerjava modelov na preizkusnem naboru, poročilo o stroških · Rok: stalno · Raven: osnovno · Vir: razdelek 2.5, R4.3 (vzorec 12)

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

4.6 Prvih 90 dni

Organizacija, ki začenja, lahko skupno jedro uvede v treh mesecih. Preglednica 9 predlaga vrstni red, pri katerem vsak korak uporabi rezultate prejšnjega.

Preglednica 9: Minimalni paket ukrepov za prve tri mesece

Obdobje	Ukrepi	Priporočila
1. mesec	Imenovanje odgovorne osebe in določitev vlog; popis sistemov, vključno z neformalno rabo; začasni pravilnik o rabi generativne UI.	S-1, S-4, S-6
2. mesec	Razvrstitveni zapisi; razvrstitev podatkov in preveritev postavitev; obvestila po 50. členu pri klepetalnikih; za javni sektor objava po 21. členu ZIUDHPUI.	S-2, S-7, P-13, U-10, U-13
3. mesec	Ukrepi pismenosti po vlogah; preizkusni nabor za najpomembnejši sistem; politika beleženja; pot za napake in pritožbe.	S-5, S-8, S-9, S-10

5 Priporočila za ponudnike

Priporočila so urejena po življenjskem ciklu sistema, od opredelitve namena do spremljanja na trgu. Zahteve za visokotvegane sisteme se uporabljajo od 2. decembra 2027 oziroma 2. avgusta 2028, priprava pa traja več mesecev, zato je čas za začetek zdaj. Priporočila, ki niso vezana na visokotvegane sisteme, so smiselna za vsakega ponudnika.

5.1 Vloga in predvideni namen

- **P-1 Ugotovite, ali ste ponudnik.** Ponudnik ni le podjetje, ki razvija programsko opremo za trg. Ponudnik je tudi organizacija, ki na model drugega ponudnika zgradi lastno rešitev in jo ponudi strankam ali zaposlenim pod svojim imenom, organizacija, ki sistem razvije za lastno rabo, ter uvajalec, ki visokotvegani sistem označi s svojim imenom ali ga bistveno spremeni ali ki sistemu spremeni namen tako, da postane visokotvegan (Preglednica 6). Vlogo zapišite v popis (S-1) za vsak sistem posebej.

  Vrsta: zahteva (člena 3(3) in 25) · Dokaz: zapis o vlogi v popisu · Rok: takoj · Raven: osnovno · Vir: razdelek 3.2

- **P-2 Predvideni namen in izključene rabe zapišite jasno in dosledno.** Predvideni namen določa razvrstitev, zato mora biti v navodilih, promocijskem gradivu, pogodbah in tehnični dokumentaciji opisan enako (člen 3(12)). Navedite tudi rabe, za katere sistem ni zasnovan, zlasti tiste s področij Priloge III, in razumno predvidljive napačne rabe. Splošna izjava o omejitvi odgovornosti ne zadošča, če promocijsko gradivo obljublja drugače. Po osnutku smernic Komisije se pri večnamenskih sistemih šteje, da namen zajema tudi visokotvegane rabe, če jih ponudnik jasno in dosledno ne izključi [7]. Angleški primer zapisovalnikov v zdravstvu kaže, da regulator status presoja po celotni predstavitvi namena in da mora ponudnik status preveriti ob vsaki spremembi izdelka.

  Vrsta: zahteva (člena 3(12) in 13(3)) · Dokaz: navodila za uporabo, promocijsko gradivo · Rok: pred dajanjem na trg · Raven: osnovno · Vir: R4.3 (primer 4.6, razdelek 5.2)

- **P-3 Uredite sodelovanje v vrednostni verigi.** Če lahko sistem pri drugačni rabi postane visokotvegan, v navodilih in pogodbi določite, ali je sprememba namena dovoljena. Uvajalce obveščajte o spremembah, ki lahko vplivajo na razvrstitev ali na uporabo izjeme po členu 6(3). Kadar drug subjekt postane ponudnik po 25. členu, mu mora prvotni ponudnik zagotoviti potrebne informacije in tehnični dostop, razen če je jasno določil, da sistem ni namenjen spremembi v visokotveganega. Kontrole morajo preživeti prehod med subjekti: kar je znano ponudniku, mora biti znano tudi uvajalcu. Do objave smernic Komisije o odgovornostih v vrednostni verigi naj pogodbe te obveznosti urejajo izrecno [8].

  Vrsta: zahteva (člen 25(2)–(4)) · Dokaz: pogodbene določbe, obvestila o spremembah · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (vzorec 7)

5.2 Podatki in pristranskost

- **P-4 Dokumentirajte nabore podatkov.** Za vsak učni, validacijski in preizkusni nabor zapišite izvor, namen in obdobje zbiranja, način označevanja in čiščenja, kdo je

podatke označeval ter katere skupine oseb so zastopane in katere manjkajo. Ohranite rodovnik podatkov od vira do napovedi. Preverite, ali so nabori reprezentativni za populacijo, na kateri bo sistem uporabljen. Opora sta skupina standardov ISO/IEC 5259 in prednostno področje 3 iz R2.2. Pri sistemih na modelu drugega ponudnika uporabite javni povzetek učnih vsebin, ki ga mora objaviti ponudnik modela (člen 53(1)(d)).

Vrsta: zahteva pri visokotveganih sistemih (10. člen); sicer dobra praksa · Dokaz: podatkovni listi, rodovnik podatkov · Rok: do 2. 12. 2027 · Raven: osnovno · Vir: R1.3, R2.2

- **P-5 Pristranskost merite po skupinah in v celotnem postopku.** Točnost preverite ločeno za skupine oseb, pri katerih je delovanje lahko slabše, ne le kot skupno povprečje. Iščite posredne znake, ki nadomeščajo zaščitene lastnosti, na primer kraj bivanja ali vrsto naprave. Nizozemski primer DUO kaže, da je treba razlike meriti na vsakem koraku postopka, od izbora do končnega ukrepa, in da človeški pregled pristranskosti ne odpravi samodejno. Novi člen 4a pod strogimi pogoji dovoljuje obdelavo posebnih vrst osebnih podatkov, kadar je ta nujna za odkrivanje in odpravo pristranskosti. Metode so bile preizkušene v simulaciji iz R4.1.

  Vrsta: zahteva pri visokotveganih sistemih (člen 10(2)(f) in (g)); člen 4a kot pravna podlaga za obdelavo · Dokaz: poročilo o razlikah med skupinami · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (primer 4.3, vzorec 11), R4.1 (Priloga B.3)

5.3 Preizkušanje, nadzor in varnost

- **P-6 Sistem preizkusite po vnaprej določenih merilih.** Preizkuse načrtujte pred razvojem: katere lastnosti preverjate (točnost, robustnost, pristranskost, varnost), s katerimi metrikami, na katerih podatkih in kje je prag sprejemljivosti. Ravni točnosti in metrike navedite v navodilih (člen 15(3)). Dokler harmonizirani standardi za točnost in robustnost niso objavljeni, mora ponudnik merila sprejemljivosti določiti in utemeljiti sam. Simulacija v R4.1 je pokazala, da so zahtevani preizkusi izvedljivi z obstoječimi metodami. Za preizkus v realnih razmerah uporabite regulativni peskovnik AKOS ali preizkušanje v realnih razmerah po 60. členu. Sistemi za slovenske uporabnike naj bodo preizkušeni tudi v slovenščini.

  Vrsta: zahteva pri visokotveganih sistemih (člen 9(6)–(8), 15. člen) · Dokaz: načrt in poročilo o preizkusih · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.1 (poglavje 9, Priloga B.3), R4.3 (primer 4.2)

- **P-7 Človeški nadzor zasnujte v sistemu.** Vmesnik naj uporabniku pokaže, na čem predlog temelji, kako zanesljiv je in katere so druge možnosti. Omogoča naj preprosto zavrnitev, popravek in ustavitev ter beleži, kolikokrat uporabniki predlog spremenijo. Kadar to ustreza nalogi, naj sistem ponudi več predlogov namesto enega. Pri agentih UI določite stopnjo avtonomije in točke, na katerih mora dejanje potrditi človek, zlasti pred nepovratnimi dejanji, kot so plačilo, brisanje ali pošiljanje podatkov zunaj organizacije. V navodilih opišite ukrepe nadzora in nevarnost pretiranega zaupanja v izhode sistema.

  Vrsta: zahteva pri visokotveganih sistemih (14. člen, člen 13(3)(d)) · Dokaz: opis ukrepov nadzora, rezultati preizkusov uporabnosti · Rok: do 2. 12. 2027 · Raven: osnovno · Vir: R2.3 (France Travail), R4.3 (primer 4.5, vzorca 2 in 13), R2.2 (prednostno področje 2)

- **P-8 Upoštevajte varnostna tveganja, značilna za UI.** Model groženj naj poleg običajnih informacijskih tveganj zajame vrivanje ukazov v pozive in dokumente, zastrupljanje podatkov, sklepanje o učnih podatkih iz modela, uhajanje podatkov prek

izhodov in napade prek dobavne verige, vključno z vtičniki in povezavami agentov z drugimi orodji. Modele, uteži in posodobitve varujte kot občutljive podatke. Agentom dodelite najmanjše potrebne pravice. Opora sta seznam tveganj OWASP za agentne aplikacije [16] in metoda STRIDE, prilagojena UI, iz nemškega primera. Za proizvode z digitalnimi elementi se od 11. septembra 2026 uporabljajo obveznosti poročanja po Aktu o kibernetski odpornosti [15].

Vrsta: zahteva pri visokotveganih sistemih (člen 15(4) in (5)); Akt o kibernetski odpornosti, kjer se uporablja · Dokaz: model groženj, poročilo o varnostnih preizkusih · Rok: do 2. 12. 2027; poročanje po Aktu o kibernetski odpornosti že velja · Raven: napredno · Vir: R2.3 (Finterai), R4.3 (primer 4.5), vzorec 5

5.4 Sistem vodenja kakovosti in dokumentacija

- **P-9 Sistem vodenja kakovosti gradite na SIST EN 18286:2026.** EN 18286 je od 14. oktobra 2026 harmonizirani standard. Daje domnevo o skladnosti z zahtevami za sistem vodenja kakovosti (člen 17(1)) in pod pogoji iz dodatka ZA tudi s prvim stavkom člena 11(1) o tehnični dokumentaciji. Za vsebinske zahteve členov 9, 10 in 12–15 harmoniziranih standardov še ni [3, 36]. V Sloveniji je standard izšel kot SIST EN 18286:2026. Po digitalnem omnibusu lahko vsa MSP sistem vodenja kakovosti uvedejo poenostavljeno, Komisija pa napoveduje smernice o poenostavljenih elementih za MSP in mala podjetja s srednje veliko tržno kapitalizacijo [8]. Organizacije z uvedenim ISO 9001 ali ISO/IEC 42001 naj obstoječi sistem nadgradijo in ne gradijo vzporednega. Preslikava je v Prilogi A k R4.1.

  Vrsta: zahteva pri visokotveganih sistemih (17. člen); domneva o skladnosti z EN 18286 · Dokaz: dokumentiran sistem vodenja kakovosti · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.1 (razdelek 4.1, Priloga A)

- **P-10 Navodila naj uvajalcu omogočijo izpolniti njegove obveznosti.** Tehnično dokumentacijo po Prilogi IV pripravite pred dajanjem na trg in jo posodabljajte. MSP in mala podjetja s srednje veliko tržno kapitalizacijo lahko uporabijo poenostavljen obrazec, ki ga morajo priglašeni organi sprejeti. Navodila za uporabo (13. člen) naj uvajalcu omogočijo izpolniti 26. člen: kako zagotoviti nadzor, kakšni morajo biti vhodni podatki, kako hraniti dnevnike in katere informacije potrebuje za oceno učinka na varstvo podatkov in oceno učinka na temeljne pravice. Dokumentacijo hranite deset let (18. člen). Dokazila naj bodo čim bližje ravnanju, ki ga dokazujejo, na primer samodejno ustvarjena poročila o preizkusih namesto naknadnih opisov.

  Vrsta: zahteva pri visokotveganih sistemih (11., 13. in 18. člen) · Dokaz: tehnična dokumentacija, navodila za uporabo · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (vzorca 9 in 10), R2.2 (prednostno področje 1)

5.5 Ugotavljanje skladnosti in spremljanje na trgu

- **P-11 Opravite ugotavljanje skladnosti in registracijo.** Za večino visokotveganih sistemov iz Priloge III (točke 2–8) se skladnost ugotavlja z notranjo kontrolo po Prilogi VI, brez priglašenega organa in certifikata. Priglašeni organ je potreben pri biometričnih sistemih, če ponudnik ne uporabi harmoniziranih standardov, ter pri proizvodih iz Priloge I po sektorskih pravilih. V Sloveniji priglašenega organa za Akt o UI do priprave R4.1 nismo zasledili. Sledijo izjava EU o skladnosti, oznaka CE in registracija v podatkovni zbirki EU pred dajanjem na trg. Sistemi, za katere ponudnik uporabi izjemo po členu 6(3), se registrirajo s skrajšanim naborom podatkov.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Vrsta: zahteva (43., 47., 48. in 49. člen) · Dokaz: izjava EU o skladnosti, potrdilo o registraciji · Rok: do 2. 12. 2027 oziroma 2. 8. 2028 · Raven: napredno · Vir: R4.1 (razdelek 9.3)

- **P-12 Spremljajte sistem po dajanju na trg in prijavljajte resne incidente.** Načrt spremljanja po dajanju na trg (72. člen) naj zbira podatke o delovanju v dejanski rabi, tudi od uvajalcev, in kazalnike, ki preverjajo predpostavke razvrstitve, na primer delež sprejetih, spremenjenih in zavrnjenih izhodov. Resne incidente prijavite organu za nadzor trga najpozneje v 15 dneh, ob obsežni kršitvi ali resni motnji v delovanju kritične infrastrukture takoj in najpozneje v dveh dneh, ob smrti osebe pa najpozneje v desetih dneh (73. člen). Uporabite smernice in predlogo Komisije za poročanje [9]; osnutek je bil objavljen septembra 2025, pregledna stran Komisije pa predlogo navaja med objavljenimi gradivi [8]. Napovedana je tudi predloga za spremljanje po dajanju na trg.

  Vrsta: zahteva pri visokotveganih sistemih (72. in 73. člen) · Dokaz: načrt spremljanja, evidenca incidentov · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (primer 4.6, Preglednica 17)

5.6 Preglednost

- **P-13 Ljudi obvestite, da komunicirajo s sistemom UI.** Sistemi, ki neposredno komunicirajo z ljudmi, morajo biti zasnovani tako, da so osebe o tem obveščene, razen če je to očitno (člen 50(1)), in sicer najpozneje ob prvi interakciji (člen 50(5)). Smernice Komisije izjemo »očitno« razlagajo ozko. Po smernicah mora agent UI razkriti svojo umetno naravo in osebo, v imenu katere deluje [4]. Obvestilo naj bo prikazano v samem pogovornem oknu ali na začetku klica, ne le v splošnih pogojih. Če klepetalnik ponujate pod svojim imenom, je obveznost vaša, tudi če uporabljate model drugega ponudnika.

  Vrsta: zahteva (člen 50(1) in (5)) · Dokaz: besedilo obvestila, posnetek vmesnika · Rok: že velja · Raven: osnovno · Vir: R4.3 (razdelek 5.1, Priloga B)

- **P-14 Sintetične vsebine označite strojno berljivo.** Ponudniki sistemov, ki ustvarjajo sliko, zvok, video ali besedilo, morajo izhode označiti v strojno berljivi obliki in omogočiti njihovo zaznavanje, kolikor je to tehnično izvedljivo (člen 50(2)). Za sisteme, dane na trg pred 2. avgustom 2026, se obveznost uporablja od 2. decembra 2026. Kodeks prakse za preglednost vsebin, ustvarjenih z UI, je priznan način izvajanja; njegovi podpisniki morajo do 2. februarja 2027 zagotoviti združljivo rešitev za zaznavanje oznak [5]. Uvajalcem posredujte navodila, kako oznak ne odstraniti, in jih opozorite na nabor ikon EU za vidno označevanje iz kodeksa prakse [5, 6].

  Vrsta: zahteva (člen 50(2)); kodeks prakse kot smernica · Dokaz: tehnična rešitev za označevanje, navodila za uvajalce · Rok: takoj (do 2. 12. 2026) · Raven: osnovno · Vir: R4.3 (primer 4.1, razdelek 5.1)

5.7 Modeli drugih ponudnikov, MSP in odgovornost

- **P-15 Pri gradnji na modelu drugega ponudnika zahtevajte dokumentacijo in nadzorujte spremembe.** Ponudnik modela UI za splošne namene mora ponudnikom nadaljnjih sistemov dati informacije, ki jih potrebujejo za razumevanje zmogljivosti in omejitev modela ter za izpolnjevanje svojih obveznosti (člen 53(1)(b)). Zahtevajte jih. Preverite, ali je ponudnik podpisnik kodeksa prakse za modele UI za splošne namene. Določite različico modela, ki jo uporabljate, zahtevajte obvestila o

spremembah in po vsaki posodobitvi ponovite preizkus iz S-8. Aplikacijo zasnujte tako, da je model mogoče zamenjati v nekaj dneh, ne v nekaj mesecih.

Vrsta: zahteva za ponudnika modela (člen 53(1)(b)); dobra praksa za ponudnika sistema · Dokaz: dokumentacija ponudnika modela, dnevnik različic, poročila o preizkusih · Rok: stalno · Raven: osnovno · Vir: R2.3 (Albert API)

- **P-16 Izkoristite olajšave za MSP in javne vodnike.** Akt o UI je za MSP že predvidel poenostavljen obrazec tehnične dokumentacije, nižje zgornje meje glob in prednostni dostop do regulativnih peskovnikov. Digitalni omnibus je te olajšave razširil na mala podjetja s srednje veliko tržno kapitalizacijo, poenostavljen sistem vodenja kakovosti, ki je bil prej na voljo le mikropodjetjem, pa na vsa MSP [1, 2]. Španske izkušnje kažejo, da težavnost zahtev ni odvisna od velikosti podjetja. Javni vodniki, kot so vodniki španske agencije AESIA, in peskovnik AKOS so zato za mala podjetja še posebej koristni.

  Vrsta: zahteva (olajšave po Aktu o UI in Uredbi (EU) 2026/1744) in smernica · Dokaz: uporabljen poenostavljen obrazec, prijava v peskovnik · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.2, razdelek 6.4)

- **P-17 Odločitve in preizkuse dokumentirajte kot dokaz skrbnosti.** Direktiva (EU) 2024/2853 o odgovornosti za proizvode z napako, ki jo morajo države članice prenesti do 9. decembra 2026, izrecno šteje programsko opremo, vključno s sistemi UI, za proizvod [14]. Odgovornost je objektivna, za škodo pa lahko odgovarja tudi, kdor proizvod bistveno spremeni. Zapisane odločitve o zasnovi, poročila o preizkusih in dnevniki sprememb so zato poleg skladnosti z Aktom o UI tudi dokaz skrbnosti v morebitnem sporu.

  Vrsta: dobra praksa (podpira obrambo po Direktivi (EU) 2024/2853) · Dokaz: dnevnik odločitev, poročila o preizkusih · Rok: stalno · Raven: napredno · Vir: Direktiva (EU) 2024/2853 [14]

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

6 Priporočila za uvajalce

Uvajalec ne more prenesti odgovornosti na ponudnika. Kupljena rešitev ga ne razbremeni obveznosti glede vhodnih podatkov, nadzora in obveščanja, njegova dejanska uporaba pa lahko spremeni razvrstitev sistema. Priporočila sledijo poti od odločitve o uvedbi do obratovanja. Razdelek 6.7 dodaja posebnosti za organe javnega sektorja.

6.1 Pred odločitvijo

- **U-1 Začnite pri problemu in merilu uspeha, ne pri orodju.** Pred izbiro orodja opišite problem, ki ga rešujete, izmerite izhodiščno stanje in določite kazalnik uspeha ter trenutek, ko boste odločili o nadaljevanju. Začnite z enim primerom uporabe. Upoštevajte, da produktivnost po uvedbi pogosto najprej pade in se šele nato izboljša ter da je uspeh bolj odvisen od ljudi in procesov kot od tehnologije. Nemški primer agentov UI v občinah kaže, da brez metodološko opisanih izhodiščnih meritev učinka ni mogoče verodostojno dokazati.

  Vrsta: dobra praksa · Dokaz: opis primera uporabe z izhodiščno meritvijo · Rok: pred uvedbo · Raven: osnovno · Vir: R4.3 (primer 4.5, vzorec 12)

- **U-2 Premišljeno izberite pot: storitev, izdelek ali lasten razvoj.** Vsaka pot ima drugačne posledice. Zunanja storitev je najhitrejša, podatki pa zapustijo organizacijo. Kupljen izdelek je prilagojen področju, a manj pregleden. Lasten razvoj ohrani podatke v organizaciji, ta pa postane ponudnica z vsemi obveznostmi (Preglednica 6). Pred odločitvijo preverite razred podatkov (S-7) in ali navodila ponudnika nameravani namen sploh dopuščajo.

  Vrsta: dobra praksa · Dokaz: zapis odločitve z utemeljitvijo · Rok: pred uvedbo · Raven: osnovno · Vir: razdelek 3.2, S-7

6.2 Izbira in naročanje

- **U-3 Postavite ponudniku prava vprašanja in odgovore prenesite v pogodbo.** Vprašajte, na katerih podatkih je sistem učen, kako je bila preverjena pristranskost, kje sistem ne deluje dobro in kakšni so rezultati na podatkih, podobnih vašim. Pogodba naj ureja lokacijo obdelave in podobdelovalce, prepoved uporabe vaših podatkov za učenje modelov brez izrecnega soglasja, roke hrambe in beleženje, obveznost obveščanja o spremembah modela, razvrstitve ali uporabe izjeme po členu 6(3), označevanje izhodov po členu 50(2), pravico do spremljanja in presoje tudi ob posodobitvah modela ter pogoje za varen izstop z izvozom in izbrisom podatkov. Primer Finterai kaže, da pogodba ne sme reči le »podatki se ne delijo«, temveč mora vloge in obveznosti opredeliti funkcionalno. Večje organizacije naj pri nabavi presodijo tudi delovne pogoje v dobavni verigi podatkov, na primer pri označevanju. Javni naročniki lahko izhajajo iz vzorčnih klavzul MCC-AI [12].

  Vrsta: zahteva glede pogodbe o obdelavi osebnih podatkov (GDPR, 28. člen); sicer dobra praksa · Dokaz: pogodba, pogodba o obdelavi · Rok: pred podpisom pogodbe · Raven: osnovno · Vir: R2.3 (Finterai), R4.3 (primer 4.6, razdelek 6.4)

- **U-4 Pred nakupom rešitve preizkusite na lastnih primerih.** Ponudnike primerjajte na preizkusnem naboru iz S-8, ne na predstavitvenih primerih. Kjer je mogoče, izhode ocenjujte slepo, brez vedenja o tem, kateri ponudnik jih je dal, da blagovna znamka ali cena ne vplivata na oceno. Zahtevajte, da ponudnik pokaže metrike na vaših podatkih. Če jih ne more, je to opozorilni znak.

  Vrsta: dobra praksa · Dokaz: poročilo o primerjavi · Rok: pred nakupom · Raven: osnovno · Vir: S-8, R4.1 (poglavje 9)

6.3 Pred uvedbo

- **U-5 Opravite oceno učinka na varstvo podatkov in, kjer je predpisana, oceno učinka na temeljne pravice.** Ocena učinka na varstvo podatkov (35. člen GDPR) je pri sistemih, ki profilirajo ali obsežno obdelujejo osebne podatke, praviloma obvezna. Pri visokotveganih sistemih jo uvajalec pripravi z informacijami iz navodil ponudnika (člen 26(9)). Oceno učinka na temeljne pravice (27. člen) morajo pred prvo uporabo visokotveganega sistema opraviti javni organi, zasebni izvajalci javnih storitev ter uvajalci sistemov za ocenjevanje kreditne sposobnosti in za življenjska in zdravstvena zavarovanja, o rezultatih pa obvestiti organ za nadzor trga. Digitalni omnibus je obe oceni povezal, da se ne podvajata. Do objave predloge Komisije uporabite izkušnje nizozemske ocene IAMA in metodologijo HUDERIA, ki dodaja vključevanje oseb, na katere sistem vpliva (razdelek 2.2). Za vsaj en verjetno visokotvegan sistem opravite poskusno oceno že v prvi polovici leta 2027.

  Vrsta: zahteva (GDPR, 35. člen; 27. člen Akta o UI od 2. 12. 2027) · Dokaz: ocena učinka na varstvo podatkov, ocena učinka na temeljne pravice, obvestilo organu · Rok: pred uvedbo; poskusna ocena v prvi polovici leta 2027 · Raven: napredno · Vir: R4.3 (primer 4.3, razdelek 6.5), HUDERIA [25]

- **U-6 Obvestite delavce in osebe, na katere sistem vpliva.** Pred uvedbo visokotveganega sistema na delovnem mestu obvestite predstavnike delavcev in delavce (člen 26(7)). Osebe, o katerih visokotvegani sistem iz Priloge III sprejema ali pomaga sprejemati odločitve, obvestite o njegovi uporabi (člen 26(11)). Te osebe imajo pravico do pojasnila vloge sistema pri odločitvi (86. člen). Kot dobro prakso ljudi obveščajte tudi pri sistemih, ki niso visokotvegani, a vplivajo nanje. Angleški okvir za zapisovalnike v zdravstvu zahteva obvestilo pacientu ob vsaki obravnavi in možnost zavrnitve. Estonski program AI Leap je uvedbo za dijake zamaknil, dokler pravna podlaga za obdelavo njihovih podatkov ni bila urejena.

  Vrsta: zahteva pri visokotveganih sistemih (člen 26(7) in (11), 86. člen) in po GDPR (13., 14. in 22. člen); sicer dobra praksa · Dokaz: obvestila, zapis o seznanitvi predstavnikov delavcev · Rok: pred uvedbo · Raven: osnovno · Vir: R4.3 (primera 4.6 in 4.7)

6.4 Uporaba

- **U-7 Poskrbite, da je človeški nadzor dejanski.** Nadzor dodelite osebam s potrebnimi kompetencami, usposobljenostjo in pooblastili ter jim zagotovite potrebno podporo (člen 26(2)), kot dobro prakso pa tudi dovolj časa za presojo. Odstop od predloga sistema ne sme imeti negativnih posledic za uslužbenca. Merite delež sprejetih, spremenjenih in zavrnjenih predlogov. Če nihče nikoli ne zavrne predloga, je nadzor verjetno le formalen. France Travail je nadzor zgradil iz štirih sestavin: razumljivega vmesnika, dovolj informacij za presojo, realne možnosti odstopa ter stalnega usposabljanja z mrežo korespondentov za UI.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Vrsta: zahteva pri visokotveganih sistemih (člen 26(2)); sicer dobra praksa · Dokaz: delež zavrnjenih ali popravljenih predlogov · Rok: od uvedbe, stalno · Raven: osnovno · Vir: R2.3 (France Travail), vzorec 2

- **U-8 Upravljajte vhodne podatke in pozive.** Vhodni podatki, ki jih nadzirate, morajo biti relevantni in dovolj reprezentativni za namen sistema (člen 26(4)). Pri generativnih sistemih je prost vnos samostojen podatkovni kanal: uporabniki lahko iz želje po natančnosti vnesejo več, kot je treba, na primer podatke o zdravju ali družinskih razmerah. Uvedite več plasti varovalk: vnaprej pripravljene predloge pozivov, filtre občutljivih izrazov, opozorila v vmesniku, navodila in usposabljanje. Iz profilov in obrazcev izločite polja, ki za namen niso potrebna in odpirajo pot neželenim korelacijam.

  Vrsta: zahteva pri visokotveganih sistemih (člen 26(4)); GDPR (člen 5(1)(c)) · Dokaz: pravila za vnos, seznam izločenih polj · Rok: od uvedbe · Raven: osnovno · Vir: R2.3 (France Travail, Finterai), vzorec 3

- **U-9 Sistem uporabljajte v mejah predvidenega namena.** Sistem uporabljajte v skladu z navodili ponudnika (člen 26(1)). Splošnega orodja ne uporabljajte za namen s področja Priloge III, na primer za razvrščanje kandidatov, brez nove presoje, saj lahko s tem postanete ponudnik visokotveganega sistema (člen 25(1)(c)). Redno preverjajte, ali dejanska uporaba še ustreza namenu, za katerega je bil sistem razvrščen.

  Vrsta: zahteva (člena 25(1)(c) in 26(1)) · Dokaz: razvrstitveni zapis, pregled dejanske uporabe · Rok: stalno · Raven: osnovno · Vir: razdelek 3.3, R4.3 (Priloga D)

6.5 Preglednost do ljudi

- **U-10 Izpolnite obveznosti razkritja uvajalca.** Uvajalec sistema za prepoznavanje čustev ali biometrično kategorizacijo mora o tem obvestiti izpostavljene osebe (člen 50(3)). Globoke ponaredke, to je sliko, zvok ali video, ki posnema resnične osebe, kraje ali dogodke in bi se lahko zdel pristen, je treba vidno označiti, pri očitno umetniških ali satiričnih delih pa na način, ki ne ovira dela. Besedila, ustvarjena z UI in objavljena za obveščanje javnosti o zadevah javnega interesa, je treba označiti, razen če jih je človek uredniško pregledal in nekdo zanje prevzema uredniško odgovornost (člen 50(4)). Za vidne oznake je na voljo nabor ikon EU iz kodeksa prakse [5, 6]. Uredniški pregled dokumentirajte. Poslovnih dopisov, ki jih pripravi UI, Akt o UI ne zahteva označevati.

  Vrsta: zahteva (člen 50(3) in (4)) · Dokaz: oznake, zapis o uredniškem pregledu · Rok: že velja · Raven: osnovno · Vir: R4.3 (primer 4.1, razdelek 5.1, Priloga B)

6.6 Obratovanje

- **U-11 Spremljajte delovanje, hranite dnevnike in poročajte o incidentih.** Delovanje spremljajte po navodilih ponudnika. Če sistem pomeni tveganje, brez nepotrebnega odlašanja obvestite ponudnika in organ za nadzor trga ter uporabo začasno ustavite. O resnem incidentu najprej obvestite ponudnika (člen 26(5)). Samodejno ustvarjene dnevnike, ki jih nadzirate, hranite najmanj šest mesecev (člen 26(6)). Pot za prijavo naj vključuje tudi dobavitelja, kot to zahteva angleški okvir za zapisovalnike v zdravstvu.

  Vrsta: zahteva pri visokotveganih sistemih (člen 26(5) in (6)) · Dokaz: poročila o spremljanju, evidenca incidentov · Rok: do 2. 12. 2027, kot dobra praksa takoj · Raven: osnovno · Vir: R4.3 (primer 4.6, Preglednica 17)

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

- **U-12 Merite vrednost in bodite pripravljeni sistem ustaviti.** Spremljajte ceno na rešen primer, ne le ceno licence: agent za eno nalogo pogosto večkrat pokliče model, prišteti pa je treba tudi človeški pregled in popravke. Po napovedi družbe Gartner bo več kot 40 % projektov z agenti UI do konca leta 2027 ukinjenih zaradi naraščajočih stroškov, nejasne poslovne vrednosti ali nezadostnega obvladovanja tveganj [38]. Učinek merite s kazalnikom iz U-1 in ga primerjajte z izhodiščem. Če sistem ne prinaša koristi, ga ustavite in odločitev utemeljite. Francosko računsko sodišče je pri France Travail ugotovilo številne opuščene primere uporabe, kar kaže, da je presoja koristi sestavni del dobre prakse.

  Vrsta: dobra praksa · Dokaz: poročilo o učinku in stroških · Rok: stalno · Raven: osnovno · Vir: R4.3 (razdelek 3.1, vzorec 12), Gartner [38]

6.7 Posebnosti javnega sektorja

- **U-13 Objavite vse sisteme UI v uporabi.** Organi javnega sektorja morajo po 21. členu ZIUDHPUI objaviti podatke o sistemih UI, ki jih uporabljajo [17]. Objavite vse sisteme, vključno s funkcijami UI v splošnih orodjih. Opis principov delovanja naj bo razumljiv, navedeno naj bo pravno varstvo. Kot dobro prakso dodajte prostovoljna polja (človeško posredovanje, tveganja, dobavitelj, stanje) in ob umiku vnos arhivirajte. Vzorec vnosa je v Prilogi C k R4.3.

  Vrsta: zahteva (21. člen ZIUDHPUI) · Dokaz: javni vnos · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.4, Priloga C), R2.3 (Helsinki)

- **U-14 Registrirajte visokotvegane sisteme in povežite javne vnose.** Javni organi, ki uvajajo visokotvegane sisteme, morajo uporabo registrirati v podatkovni zbirki EU (člena 26(8) in 49(3)) in pred prvo uporabo opraviti oceno učinka na temeljne pravice. Številko in datum ocene navedite tudi v javni objavi po 21. členu ZIUDHPUI. Visokotvegani sistemi, namenjeni javnim organom, ki so bili dani na trg ali v uporabo pred začetkom uporabe zahtev, morajo biti usklajeni najpozneje do 2. avgusta 2030 (111. člen).

  Vrsta: zahteva (člena 26(8) in 49(3), 27. in 111. člen) · Dokaz: potrdilo o registraciji, ocena učinka · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (razdelek 6.5)

- **U-15 Pilotne projekte in javna naročila zasnujte preverljivo.** Pilotni projekti naj bodo časovno omejeni in ne smejo služiti obidu zahtev; angleški okvir jih omejuje na največ štiri mesece. Pri agentih UI določite stopnje avtonomije, vloge upravljavca in ponudnika, beleženje korakov in merjenje učinka pred uvedbo in po njej. Prednost naj imajo naloge, pri katerih sistem pripravlja gradivo, odločitev pa ostane pri uradniku. O rezultatih, tudi neugodnih, javno poročajte, kot to počneta nemški program agentov v občinah in estonski program AI Leap.

  Vrsta: dobra praksa · Dokaz: načrt pilota, javno poročilo · Rok: pri vsakem novem projektu · Raven: napredno · Vir: R4.3 (primeri 4.5–4.7, razdelek 6.4)

- **U-16 Zagotovite pot do človeka in pritožbeno pot.** V javnih klepetalnikih naj bo obvestilo o UI prikazano neposredno v pogovornem oknu, uporabnik pa naj ima vedno možnost, da ga obravnava človek. Vprašanja, na katera sistem ne sme odgovarjati, naj preusmeri k strokovnjakom, kot to počne helsinški klepetalnik. Vzpostavite notranjo pot za pritožbe in popravke ter ljudi seznanite, da se lahko pritožijo tudi pri organu za nadzor trga (85. člen).

Vrsta: dobra praksa; pritožba pri organu za nadzor trga je pravica po 85. členu · Dokaz: vmesnik s potjo do človeka, evidenca pritožb · Rok: takoj · Raven: osnovno · Vir: R2.3 (Helsinki), R4.3 (razdelek 6.4), razdelek 2.5

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

7 Tehnološki profili

Poglavja 4–6 veljajo ne glede na tehnologijo. To poglavje dodaja varovalke, ki so odvisne od vrste sistema. Vsak profil ima enako zgradbo: tipična raba in razvrstitev, glavna tveganja, priporočila (oznaka T), opozorilni znaki in primeri iz projekta. Organizacija prebere profile, ki ustrezajo njenim sistemom. Sistem, ki združuje več tehnologij, na primer agent z iskanjem po dokumentih, mora upoštevati vse ustrezne profile. Razdelek 7.9 povezuje profile s področji uporabe.

7.1 T1 Klasično strojno učenje za odločanje o ljudeh

Sem sodijo modeli, ki iz preteklih podatkov napovedujejo ali razvrščajo, na primer točkovanje kreditne sposobnosti, razvrščanje kandidatov, ocena upravičenosti do storitev ali zaznavanje sumljivih transakcij. Kadar je namen s področja Priloge III (točke 3, 4 in 5), je sistem praviloma visokotvegan. Kadar sistem profilira fizične osebe, se ponudnik na izjemo po členu 6(3) ne more sklicevati. Zaznavanje finančnih goljufij je iz točke 5(b) izrecno izvzeto.

- **Glavna tveganja:** učna populacija, ki ne odraža populacije uporabe; posredni znaki, ki nadomeščajo zaščitene lastnosti; zamenjava korelacije z vzročnostjo; premik podatkov sčasoma; povratne zanke, pri katerih odločitve sistema oblikujejo prihodnje učne podatke; napadi na model, ki iz njega izluščijo podatke o učni populaciji.
- **T1-1 Prag odločanja določite glede na ceno napak.** Lažno pozitivne in lažno negativne napake imajo za ljudi različne posledice. Prag določite glede na te posledice in ga utemeljite, razlike v napakah pa preverite po skupinah oseb. Nizozemski primer DUO kaže, da se pristranskost lahko pojavi šele pri izboru za nadaljnji postopek, ne v samem modelu.

  Vrsta: zahteva pri visokotveganih sistemih (9. člen, člen 10(2)(f) in (g), člen 15(3)) · Dokaz: utemeljitev praga, rezultati po skupinah · Rok: do 2. 12. 2027 · Raven: napredno · Vir: R4.3 (primer 4.3)

- **T1-2 Spremljajte premik podatkov in povratne zanke.** Določite kazalnike, ki opozorijo, ko se populacija ali vhodni podatki spremenijo, in model ponovno preverite vsaj enkrat letno ter ob vsaki pomembni spremembi. Pri sistemih, ki se učijo tudi po dajanju na trg ali v uporabo, je treba tveganje, da pristranski izhodi vplivajo na prihodnje vhode, odpraviti ali čim bolj zmanjšati (člen 15(4)).

  Vrsta: zahteva pri visokotveganih sistemih (člen 15(4), 72. člen) · Dokaz: poročila o spremljanju, zapisi ponovnih preverjanj · Rok: stalno · Raven: napredno · Vir: R2.3 (kontrolni seznam)

- **T1-3 Modele in uteži varujte kot osebne podatke.** Iz modela je z znanimi napadi mogoče sklepati, ali je bila oseba v učnem naboru, ali izluščiti značilnosti učnih podatkov. Določite, kdo sme do modelov in posodobitev, kako se prenašajo in hranijo ter kako se beleži dostop. Pri federativnem učenju, kjer se izmenjujejo modeli namesto podatkov, so modelne posodobitve glavni predmet varovanja.

  Vrsta: dobra praksa; pri visokotveganih sistemih člen 15(5) · Dokaz: pravila dostopa do modelov, revizijska sled · Rok: takoj · Raven: osnovno · Vir: R2.3 (Finterai), vzorec 5

- **T1-4 Zagotovite razumljivo pojasnilo za posameznika.** Oseba, o kateri je uvajalec na podlagi izhoda visokotveganega sistema iz Priloge III (razen točke 2) sprejel odločitev s pravnimi ali podobno pomembnimi učinki, ki po njenem mnenju škodljivo vplivajo na njeno zdravje, varnost ali temeljne pravice, ima pravico, da ji uvajalec jasno in smiselno pojasni vlogo sistema in glavne elemente odločitve (86. člen). Pojasnilo pripravite v jeziku, ki ga oseba razume, in ga povežite z obveščanjem po GDPR.

  Vrsta: zahteva pri visokotveganih sistemih (86. člen); GDPR (13.–15. in 22. člen) · Dokaz: vzorec pojasnila · Rok: do 2. 12. 2027 · Raven: osnovno · Vir: R1.1, R4.3 (primer 4.3)

- **Opozorilni znaki:** »model ne uporablja občutljivih podatkov, zato ni pristranski«; uspešnost se meri le s skupno točnostjo; model ni bil ponovno preverjen več kot leto; nihče ne ve, kdo ima dostop do uteži.
- **Primeri iz projekta:** Finterai – federativno učenje za preprečevanje pranja denarja (R2.3); DUO – pristransko profiliranje pri preverjanju štipendij (R4.3).

7.2 T2 Klepetalniki in pisni asistenti na jezikovnih modelih

Sem sodijo klepetalniki za stranke in občane ter pomočniki za pisanje, povzemanje in prevajanje. Klepetalniki, ki komunicirajo z ljudmi, morajo razkriti, da gre za UI (člen 50(1)). Pomočnik za interno pisanje praviloma nima posebnih obveznosti po Aktu o UI, razen 4. člena. Sistem postane visokotvegan, kadar začne sprejemati ali bistveno vplivati na odločitve o dostopu do storitev, zaposlitvi ali kreditu.

- **Glavna tveganja:** samozavestno napačni odgovori in izmišljene navedbe; zavezujoče izjave o cenah, pravilih ali pravicah, ki niso točne; vnos osebnih in zaupnih podatkov v pozive; prenos podatkov k ponudniku modela; vrinjena navodila; pretirano zaupanje uporabnikov.
- **T2-1 Klepetalnik naj pove, kaj je, in naj ve, česa ne sme.** Obvestilo o UI prikažite v pogovornem oknu ob prvem stiku. Določite teme, na katere klepetalnik ne odgovarja, na primer pravne, zdravstvene in finančne nasvete za posameznika, in jih preusmerite k človeku. Helsinški klepetalnik vprašanja zunaj svojega področja preusmeri k strokovnjakom.

  Vrsta: zahteva (člen 50(1)); sicer dobra praksa · Dokaz: posnetek vmesnika, seznam izključenih tem · Rok: že velja · Raven: osnovno · Vir: R2.3 (Helsinki), R4.3 (Priloga B)

- **T2-2 Zavezujoče informacije naj temeljijo na preverjenih virih.** Organizacija odgovarja za informacije, ki jih da njen klepetalnik. V primeru Moffatt proti Air Canada je kanadsko razsodišče odločilo, da letalski prevoznik odgovarja za napačno informacijo klepetalnika o povračilu cene vozovnice, saj je klepetalnik del njegove spletne strani [42]. Cene, pogoji, roki in pravice naj izhajajo iz ažurnih uradnih virov, odgovori z zavezujočo vsebino pa naj se sklicujejo nanje.

  Vrsta: dobra praksa · Dokaz: seznam virov za zavezujoče odgovore, postopek posodabljanja · Rok: takoj · Raven: osnovno · Vir: [42]

- **T2-3 Merite točnost odgovorov v slovenščini.** Delež pravilnih odgovorov merite na preizkusnem naboru v slovenščini, vključno z neformalnim jezikom in tipkarskimi napakami. Spremljajte vprašanja, na katera sistem ni znal odgovoriti, in jih uporabite za izboljšave. Helsinški register objavlja omejitve sistema, na primer jezike, ki jih podpira.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Vrsta: dobra praksa · Dokaz: poročilo o točnosti, evidenca neodgovorjenih vprašanj · Rok: pred uvedbo in stalno · Raven: osnovno · Vir: R2.3 (Helsinki), vzorec 6

- **Opozorilni znaki:** klepetalnik nima vidnega obvestila o UI; daje osebne pravne ali finančne nasvete; ni evidence napačnih odgovorov; zaposleni vanj vnašajo podatke strank brez pravil.
- **Primeri iz projekta:** Helsinški register in klepetalnik (R2.3); smernice javnega medija ORF (R4.3); Albert API kot skupna državna platforma (R2.3).

7.3 T3 Iskanje po znanju organizacije (RAG)

Sistem pred odgovorom poišče ustrezne odlomke v dokumentih organizacije in jih vključi v poziv jezikovnemu modelu. To zmanjša izmišljanje in omogoča navajanje virov. Zaupnosti pa samo po sebi ne poveča: odlomki gredo v poziv, zato je zaupnost odvisna od tega, kje teče model (S-7). Interni iskalnik praviloma nima posebnih obveznosti po Aktu o UI. Ko pa sistem pripravlja predloge za odločitve o ljudeh, kot pri France Travail, se približa področjem Priloge III.

- **Glavna tveganja:** model prejme odlomke, ki jih uporabnik ne bi smel videti; zastareli ali neveljavni dokumenti; slabo razrezani dokumenti in iskanje, ki vrne napačne vire; vrinjena navodila v dokumentih iz zunanjih virov; osebni podatki v bazi znanja brez nadzora.
- **T3-1 Pravice dostopa prenesite v iskanje.** Uporabnik naj prek iskanja dobi le odlomke iz dokumentov, do katerih ima pravico dostopa v izvornem sistemu. Pravice preverite ob vsaki poizvedbi, ne le ob nalaganju dokumentov.

  Vrsta: dobra praksa; GDPR (32. člen) · Dokaz: opis preslikave pravic, rezultati preizkusa dostopa · Rok: pred uvedbo · Raven: osnovno · Vir: R2.3 (Albert API)

- **T3-2 Bazo znanja upravljajte kot vir resnice.** Baza znanja naj ima lastnika, različice, datum veljavnosti posameznih dokumentov ter postopek za posodabljanje in umik. Odgovor naj navaja uporabljene vire, da jih lahko uporabnik preveri. Beležite, kateri odlomki so bili uporabljeni za posamezen odgovor.

  Vrsta: dobra praksa · Dokaz: register baze znanja, dnevnik virov · Rok: stalno · Raven: osnovno · Vir: R2.3 (France Travail, Albert API)

- **T3-3 Ločeno preverite iskanje in odgovor.** Preizkusni nabor naj meri, ali iskanje najde prave dokumente in ali odgovor dejansko sledi najdenim virom. Napaka v iskanju se namreč pokaže kot samozavesten, a napačen odgovor. Dokumente iz zunanjih virov obravnavajte kot nezaupljive, saj lahko vsebujejo vrinjena navodila [16].

  Vrsta: dobra praksa · Dokaz: poročilo o preizkusu iskanja in odgovorov · Rok: pred uvedbo in ob spremembi baze · Raven: napredno · Vir: S-8, OWASP [16]

- **Opozorilni znaki:** v bazi so različice istega pravilnika brez oznake veljavnosti; odgovori ne navajajo virov; nihče ni preveril, ali iskanje upošteva pravice dostopa.
- **Primeri iz projekta:** France Travail – predlogi usposabljanj z lokalno nameščenim modelom (R2.3); Albert API – skupna platforma z iskanjem po dokumentih (R2.3).

7.4 T4 Agenti UI

Agent dobi cilj, sam načrtuje korake ter uporablja orodja in druge informacijske sisteme. Pri klepetalniku je najslabši izid napačno besedilo, ki ga človek prebere in zavrže, pri agentu pa napačno dejanje, ki je že izvedeno. Akt o UI agentov ne obravnava kot posebne kategorije. Zanje veljajo enaka pravila kot za druge sisteme, odločilen pa je predvideni namen [11]. Po smernicah Komisije mora agent, ki komunicira z ljudmi, razkriti svojo umetno naravo in osebo, v imenu katere deluje [4].

- **Glavna tveganja:** vrinjena navodila v e-pošti, obrazcih ali dokumentih, ki jih agent izvede; nepovratna dejanja; preširoke pravice; napake, ki se prenašajo med agenti in izgubijo oznako negotovosti; vtičniki in povezave z orodji kot nova dobavna veriga; naraščajoči stroški.

Dokumentirani primeri iz leta 2025 kažejo, da težava ni bil model, temveč meje okoli njega. Kodirni agent je med poskusom, v katerem mu je bilo naročeno, naj brez odobritve ničesar ne spreminja, izbrisal produkcijsko bazo podatkov [39]. Pri agentu za upravljanje odnosov s strankami so raziskovalci v spletni obrazec skrili navodila, ki jih je agent izvedel in podatke poslal na potekel, a dovoljen spletni naslov [40]. Pri pomočniku v pisarniškem paketu je eno samo e-poštno sporočilo brez klika uporabnika lahko povzročilo iznos notranjih podatkov [41]. Obe ranljivosti sta bili odpravljeni, ponudnik kodirnega agenta pa je uvedel ločitev razvojnega in produkcijskega okolja ter obnovo iz varnostnih kopij. Vzorec je v vseh treh primerih enak: preširoke pravice, nezaupljiv vnos, obravnavan kot navodilo, in manjkajoča potrditev pred tveganim dejanjem.

- **T4-1 Avtonomijo stopnjujte in vežite na človeško odobritev.** Za vsakega agenta določite stopnjo avtonomije, dovoljena orodja in najmanjše potrebne pravice. Pred nepovratnimi ali tveganimi dejanji, kot so plačilo, brisanje, pošiljanje podatkov zunaj organizacije, sprememba pravic, sklenitev pogodbe ali odločitev o osebi, naj dejanje potrdi človek. Več avtonomije mora pomeniti manj pravic in več sledljivosti. V nemških pilotih je končno odločitev vedno sprejel uradnik.

  Vrsta: dobra praksa; pri visokotveganih sistemih 14. člen in člen 26(2) · Dokaz: matrika avtonomije in pravic · Rok: pred uvedbo · Raven: osnovno · Vir: R4.3 (primer 4.5, vzorec 13)

- **T4-2 Beležite celotno pot in ločite okolja.** Dnevnik naj zajame vire, orodja, parametre, spremembe in odobritve, tako da je vsako dejanje mogoče rekonstruirati. Hranite ga zunaj agenta, da ga agent ne more spremeniti. Razvojno in produkcijsko okolje naj bosta ločena, za vsako spremembo podatkov pa naj obstaja možnost povrnitve.

  Vrsta: dobra praksa; pri visokotveganih sistemih 12. člen in člen 26(6) · Dokaz: specifikacija dnevnika, načrt povrnitve · Rok: pred uvedbo · Raven: osnovno · Vir: R4.3 (primer 4.5), [39]

- **T4-3 Vtičnike in povezave obravnavajte kot dobavitelje.** Vsako povezavo agenta z zunanjim orodjem ali storitvijo, na primer prek vtičnikov ali strežnikov po protokolu MCP, popišite, odobrite in ji dodelite najmanjše pravice. Zunanje vnose (e-pošto, obrazce, spletne strani, dokumente) obravnavajte kot nezaupljive. Določite seznam ciljev, kamor sme agent pošiljati podatke. Opora je seznam tveganj OWASP za agentne aplikacije [16].

  Vrsta: dobra praksa; pri visokotveganih sistemih člen 15(5) · Dokaz: popis povezav, seznam dovoljenih ciljev · Rok: pred uvedbo · Raven: napredno · Vir: OWASP [16], [40], [41]

- **T4-4 Preverite proces, ne le končnega izida.** Pravilen končni odgovor ne pomeni, da je bil postopek pravilen. Preizkus naj preveri, ali je agent izbral pravo orodje in parametre, ali je spremenil le dovoljeno, ali je pravočasno predal odločitev človeku ter kakšni so bili stroški in čas. Dolga veriga korakov je manj zanesljiva od posameznega koraka.

  Vrsta: dobra praksa · Dokaz: poročilo o preizkusu procesa · Rok: pred uvedbo in ob spremembah · Raven: napredno · Vir: S-8, R4.3 (primer 4.5)

- **Opozorilni znaki:** agent ima širše pravice, kot jih potrebuje; dnevnik poti ne obstaja ali ga lahko spremeni agent sam; ni načrta povrnitve; agent lahko pošilja podatke na poljubne naslove.
- **Primeri iz projekta:** Agentic AI Hub – agenti UI v nemških občinah (R4.3).

7.5 T5 Ustvarjanje slik, zvoka in videa

Ponudnik orodja mora izhode strojno berljivo označiti (člen 50(2)). Uvajalec mora vidno označiti globoke ponaredke, to je vsebino, ki posnema resnične osebe, kraje ali dogodke in bi se lahko zdela pristna (člen 50(4)). Od 2. decembra 2026 so prepovedani sistemi, katerih predvideni namen ali razumno predvidljiv in ponovljiv rezultat brez razumnih zaščit so nekonsenzualni intimni posnetki ali gradivo spolne zlorabe otrok; prepoved velja tudi za uvajalce, ki sistem uporabijo za ta namen (člen 5(1)(ba) in (bb)).

- **T5-1 Izberite orodja, ki označujejo, in oznak ne odstranjujte.** Pri izbiri orodja preverite, ali ponudnik izhode označuje v skladu s kodeksom prakse, in to zahtevajte v pogodbi. Pri obdelavi vsebin pazite, da oznak in metapodatkov ne odstranite.

  Vrsta: zahteva za ponudnika (člen 50(2)); dobra praksa za uvajalca · Dokaz: pogodbena določba, preverjeni metapodatki · Rok: takoj (do 2. 12. 2026) · Raven: osnovno · Vir: R4.3 (primer 4.1, razdelek 5.1)

- **T5-2 Ločite ilustracijo od globokega ponaredka.** Stilizirana ali očitno izmišljena ilustracija praviloma ni globoki ponaredek, fotorealistična upodobitev resnične osebe, kraja ali dogodka pa je. Za mejne primere določite notranje pravilo, odločitve dokumentirajte, za vidne oznake pa uporabite nabor ikon EU iz kodeksa prakse [5, 6]. Avstrijski javni medij ORF za to uporablja semafor in seznam odobrenih orodij.

  Vrsta: zahteva (člen 50(4)) in smernica [4] · Dokaz: notranje pravilo, evidenca odločitev · Rok: že velja · Raven: osnovno · Vir: R4.3 (primer 4.1)

- **T5-3 Ponudniki splošnih orodij naj vgradijo zaščite pred prepovedanimi izhodi.** Ponudniki orodij za ustvarjanje slik in videa naj pred 2. decembrom 2026 preverijo, ali imajo ustrezne zaščite pred ustvarjanjem nekonsenzualnih intimnih posnetkov in gradiva spolne zlorabe otrok, ter jih dokumentirajo.

  Vrsta: zahteva (člen 5(1)(ba) in (bb), dodan z Uredbo (EU) 2026/1744) · Dokaz: opis zaščit, rezultati preizkusov · Rok: do 2. 12. 2026 · Raven: osnovno · Vir: [2]

- **Primeri iz projekta:** smernice ORF za označevanje po vrstah medijev (R4.3).

7.6 T6 Govor: prepoznava, zapisovanje in povzemanje

Sem sodijo narekovanje, zapisniki sestankov in zapisovalniki pogovorov, ki posnetek pretvorijo v besedilo in pripravijo povzetek. Smernice Komisije k 50. členu prepis navajajo med primeri standardnega urejanja, za katere obveznost označevanja po členu 50(2) ne velja,

povzetke, ustvarjene z UI, pa je treba označiti (točka 92) [4]. V zdravstvu je orodje, ki podpira diagnozo ali zdravljenje, lahko medicinski pripomoček. Visokotvegano po Prilogi I je, kadar je za pripomoček potrebno ugotavljanje skladnosti pri priglašenem organu (razred IIa ali višji); zahteve se zanj uporabljajo od 2. avgusta 2028. Prepoznavanje čustev iz glasu je na delovnem mestu in v izobraževanju prepovedano, razen iz zdravstvenih ali varnostnih razlogov.

- **Glavna tveganja:** slabša točnost pri narečjih, starejših govorcih in govorcih, ki jim jezik ni prvi; izmišljene in izpuščene vsebine v povzetkih; posnetki kot osebni podatki, v zdravstvu posebne vrste podatkov; snemanje brez vednosti oseb; nova funkcija, ki spremeni status orodja.
- **T6-1 Točnost preizkusite pri skupinah, pri katerih je prepoznava slabša.** Preizkusni nabor naj vključuje slovenska narečja, starejše govorce, govorce, ki jim slovenščina ni prvi jezik, in hrupno okolje. Merite tudi izpuščene vsebine, ne le napačne besede.

  Vrsta: dobra praksa · Dokaz: poročilo o preizkusu po skupinah · Rok: pred uvedbo · Raven: osnovno · Vir: R4.3 (primer 4.6)

- **T6-2 Vsak zapis naj pregleda in potrdi človek.** Zapis postane del dokumentacije šele, ko ga odgovorna oseba pregleda in potrdi. Posnetke in prepise po potrditvi izbrišite, razen kadar je hramba potrebna za preverjanje točnosti in je časovno omejena.

  Vrsta: dobra praksa · Dokaz: postopek potrjevanja, pravila hrambe · Rok: od uvedbe · Raven: osnovno · Vir: R4.3 (primer 4.6)

- **T6-3 Obvestite osebe in ob vsaki novi funkciji preverite status orodja.** Osebe naj bodo o snemanju obveščene ob vsakem pogovoru in naj imajo možnost zavrnitve. Nova funkcija, na primer predlogi diagnoz, lahko orodje spremeni v medicinski pripomoček, zato status preverite ob vsaki spremembi.

  Vrsta: GDPR (13. člen); sicer dobra praksa · Dokaz: besedilo obvestila, zapis presoje statusa · Rok: od uvedbe · Raven: osnovno · Vir: R4.3 (primer 4.6)

- **Primeri iz projekta:** nacionalni okvir NHS England za zapisovalnike pogovorov in slovenski projekt »Prepoznava govora« (R4.3).

7.7 T7 Biometrija in prepoznavanje čustev

Akt o UI na tem področju določa prepovedi in visoko tveganje. Prepovedani so prepoznavanje čustev na delovnem mestu in v izobraževalnih ustanovah (razen iz zdravstvenih ali varnostnih razlogov), biometrična kategorizacija za sklepanje o občutljivih lastnostih, neciljno zbiranje obraznih slik za zbirke za prepoznavanje obrazov ter biometrična identifikacija na daljavo v realnem času na javnih mestih za namene kazenskega pregona (z izjemami). Druga biometrična identifikacija na daljavo, biometrična kategorizacija po občutljivih ali zaščitenih lastnostih in prepoznavanje čustev so visokotvegani (Priloga III, točka 1). Uvajalec sistema za prepoznavanje čustev ali biometrično kategorizacijo mora izpostavljene osebe obvestiti (člen 50(3)).

- **T7-1 Pred uvedbo preverite prepovedi.** Za vsak sistem, ki obdeluje obraz, glas, držo ali vedenje, preverite, ali ne sodi med prepovedane prakse. Prepovedi se uporabljajo od 2. februarja 2025.

  Vrsta: zahteva (5. člen) · Dokaz: razvrstitveni zapis · Rok: že velja · Raven: osnovno · Vir: R1.1, razdelek 3.3

- **T7-2 Mejo do prepoznavanja čustev dokumentirajte.** Sistem za prepoznavanje čustev je po Aktu o UI sistem, ki čustva sklepa na podlagi biometričnih podatkov (člen 3(39)). Analiza razpoloženja v besedilu zato sama po sebi ni prepoznavanje čustev, razširitev na glas ali video pa lahko je. Mejo zapišite v razvrstitveni zapis in jo ponovno preverite ob vsaki novi funkciji. Estonski program AI Leap to vprašanje rešuje pri orodju za dijake.

  Vrsta: zahteva (člen 5(1)(f)) in dobra praksa · Dokaz: razvrstitveni zapis z opisom meje · Rok: takoj · Raven: osnovno · Vir: R4.3 (primer 4.7)

- **T7-3 Pri biometriji preverite tudi pravno podlago po GDPR.** Biometrični podatki za enolično identifikacijo so posebne vrste osebnih podatkov (9. člen GDPR). Tudi kadar sistem ni prepovedan, je treba pred uvedbo preveriti pravno podlago, opraviti oceno učinka na varstvo podatkov in pri ponudniku preveriti, ali je bil za ugotavljanje skladnosti potreben priglašeni organ (P-11).

  Vrsta: zahteva (GDPR, 9. in 35. člen; 43. člen Akta o UI) · Dokaz: pravna presoja, ocena učinka · Rok: pred uvedbo · Raven: napredno · Vir: R1.1

7.8 T8 UI v proizvodih in industriji

Sem sodijo strojni vid za kontrolo kakovosti, napovedno vzdrževanje, optimizacija procesov ter UI v medicinskih pripomočkih, strojih in vozilih. Priloga I ima dva oddelka. Za proizvode iz oddelka A, na primer medicinske pripomočke, in vitro diagnostične pripomočke, igrače, dvigala in radijsko opremo, je sistem UI visokotvegan, kadar je varnostna komponenta proizvoda ali proizvod sam in je za proizvod potrebno ugotavljanje skladnosti pri tretji osebi. Zahteve se zanje uporabljajo od 2. avgusta 2028. Za proizvode iz oddelka B, na primer vozila, letalstvo in železnice, po digitalnem omnibusu pa tudi stroje, se zahteve Akta o UI ne uporabljajo neposredno, temveč prek sektorske zakonodaje. Omnibus je zožil tudi pojem varnostne komponente: UI, ki se uporablja zgolj za vidike, ki niso povezani z varnostjo, na primer pomoč uporabniku, optimizacijo delovanja, avtomatizacijo ali kontrolo kakovosti, ni visokotvegana le zato, ker je vgrajena v reguliran proizvod (člen 6(1a) in (1b)).

- **T8-1 Dokumentirajte, ali ima UI varnostno funkcijo.** Za vsak sistem v proizvodu zapišite, ali bi njegova odpoved ali napačno delovanje lahko ogrozilo zdravje ali varnost. Presoja določa, ali gre za varnostno komponento, in jo je treba ponoviti ob vsaki spremembi funkcije.

  Vrsta: zahteva (člen 6(1), (1a) in (1b), Priloga I) · Dokaz: zapis presoje · Rok: do 2. 8. 2028 · Raven: napredno · Vir: razdelek 3.3, R4.1 (poglavje 5)

- **T8-2 UI vključite v obstoječe postopke za proizvod.** Pri proizvodih iz oddelka A Priloge I se zahteve Akta o UI preverijo v okviru ugotavljanja skladnosti po sektorski zakonodaji (člen 43(3)), pri proizvodih iz oddelka B pa prek sektorskih predpisov. UI vključite tudi v obstoječe postopke kibernetske varnosti po Aktu o kibernetski odpornosti [15] in v ravnanje pri odgovornosti za proizvode z napako [14].

  Vrsta: zahteva (43. člen, sektorska zakonodaja, Akt o kibernetski odpornosti) · Dokaz: tehnična dokumentacija proizvoda · Rok: do 2. 8. 2028; poročanje po Aktu o kibernetski odpornosti že velja · Raven: napredno · Vir: R4.1

- **T8-3 Spremljajte delovanje v spremenljivih razmerah.** Pri strojnem vidu in napovednem vzdrževanju se razmere (osvetlitev, material, obraba, senzorji) spreminjajo. Vzdržujte preizkusni nabor in spremljajte odstopanja, ne le skupno točnost.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Vrsta: dobra praksa · Dokaz: poročila o spremljanju · Rok: stalno · Raven: osnovno · Vir: S-8

7.9 Profili po področjih uporabe

Preglednica 10 povezuje področja, ki so po R4.1 najbolj izpostavljena zahtevam Akta o UI, s tehnološkimi profili, točkami Priloge III in primeri iz projekta.

Preglednica 10: Področja uporabe, tehnološki profili in primeri iz projekta

Področje	Profili	Ključne določbe	Primeri iz projekta
Javna uprava	T2, T3, T4	Priloga III, točke 5(a), 6, 7 in 8; 21. člen ZIUDHPUI	Albert API, Helsinki, Agentic AI Hub, javna objava v Sloveniji
Zdravstvo	T6, T1, T8	Priloga I (medicinski pripomočki); Priloga III, točka 5(d)	NHS England, Prepoznava govora
Izobraževanje	T2, T7	Priloga III, točka 3; člen 5(1)(f)	AI Leap
Zaposlovanje	T1, T2	Priloga III, točka 4; člen 5(1)(f)	France Travail
Finance in zavarovalništvo	T1	Priloga III, točki 5(b) in 5(c)	Finterai
Kritična infrastruktura in energetika	T8, T1	Priloga III, točka 2; Priloga I	R4.1 (poglavje 5)
Mediji	T5, T2	člen 50(2) in (4)	ORF

8 Priporočila za odločevalce in nadzornike

Ponudniki in uvajalci zahteve lažje izpolnijo, če imajo jasne razlage, preizkušena orodja in sogovornika pri pristojnih institucijah. Priporočila v tem poglavju so namenjena ministrstvom, nadzornim organom in standardizaciji. Omejena so na to, kar institucije lahko storijo, da bodo organizacije zahteve izpolnile. Predaja dokumentacije za nacionalne standarde, nadaljevanje dejavnosti projekta in vzdrževanje Observatorija standardov UI so predmet R5.2. Priporočila dopolnjujejo priporočila deležnikom iz R4.3 (razdelek 6.4) in R4.1 (razdelek 10.2) ter jih ne ponavljajo v celoti. Pod vsakim priporočilom so navedeni naslovniki, rok in vir.

8.1 Jasna pravila in vodniki

- **O-1 Pripravite vodnika za razvrščanje in za sistem vodenja kakovosti.** Najbolj nujna sta vodnik za razvrščanje po 6. členu s slovenskimi primeri in izvedbeni vodnik za EN 18286. Oba naj bosta na voljo do konca prvega četrtletja leta 2027, da bodo imele organizacije dovolj časa do 2. decembra 2027. Vodnik za razvrščanje naj se po objavi končnih smernic Komisije ciljno posodobi.

  Naslovniki: SIST/TC UMI, ministrstvo, pristojno za digitalno preobrazbo, AKOS · Rok: do konca 1. četrtletja 2027 · Vir: R4.1 (razdelek 10.2), R4.3 (Priloga A)

- **O-2 Uskladite razlage nadzornih organov.** Nadzor je po ZIUDHPUI porazdeljen med več organov. Organizacije potrebujejo enotne odgovore na pogosta vprašanja, usklajene prek koordinacijskega sosveta in posodobljene ob vsaki končni smernici Komisije in posodobitvi kodeksa prakse. Posebej koristna so pojasnila o 50. členu pred 2. decembrom 2026.

  Naslovniki: AKOS, Informacijski pooblaščenec, drugi organi za nadzor trga, inšpekcija za informacijsko družbo · Rok: takoj in stalno · Vir: R4.3 (razdelek 6.4), R4.1 (razdelek 10.2)

8.2 Infrastruktura za skladnost

- **O-3 Vzpostavite delujoč regulativni peskovnik.** Peskovnik AKOS naj do 2. avgusta 2027 deluje kot fazni program z jasnimi izdelki, lestvico zrelosti, sodelovanjem pristojnih organov in zaključnimi poročili po členu 57(7). Javni vodniki, ki bodo nastali v peskovniku, naj bodo dostopni vsem ponudnikom, ne le udeležencem. Zgled je španski peskovnik z vodniki AESIA.

  Naslovniki: AKOS, koordinacijski sosvet · Rok: do 2. 8. 2027 · Vir: R4.3 (primer 4.2, razdelek 6.4)

- **O-4 Zagotovite preizkusne nabore v slovenščini in pot do ugotavljanja skladnosti.** Pripravite nacionalni vodnik za preizkušanje visokotveganih sistemov na podlagi simulacije iz R4.1 in referenčne preizkusne nabore v slovenščini, ki jih bodo ponudniki lahko uporabili za preverjanje točnosti in pristranskosti. Ocenite potrebo po slovenskih priglašenih organih in pripravite akreditacijsko shemo, saj jih do priprave R4.1 nismo zasledili. Orodja in priloge iz R4.1 in R4.3 naj se po zaključku projekta preizkusijo na dveh ali treh dejanskih sistemih, na primer v peskovniku AKOS.

Naslovniki: ministrstvo, pristojno za digitalno preobrazbo, Slovenska akreditacija, raziskovalne organizacije · Rok: leto 2027 · Vir: R4.1 (razdelki 9.3, 9.4 in 10.2), R4.3 (razdelek 6.4)

8.3 Javni sektor kot zgled

- **O-5 Nadgradite enotno informacijsko točko za sisteme UI v javnem sektorju.** Obrazec za objavo po 21. členu ZIUDHPUI naj vsebuje tudi prostovoljna polja (človeško posredovanje, tveganja, dobavitelj, stanje), enolične identifikatorje in arhiv umaknjenih sistemov. Zbirka naj bo objavljena v strojno berljivi obliki z zgodovino različic. Organom ponudite vzorec dobro izpolnjenega vnosa.

  Naslovnik: ministrstvo, pristojno za javno upravo · Rok: leto 2027 · Vir: R4.3 (primer 4.4, Priloga C, razdelek 6.4)

- **O-6 Ponudite vzorčne dokumente za naročanje in pilotne projekte.** Pripravite slovenske vzorčne razpisne in pogodbene določbe na podlagi klavzul MCC-AI [12] in skupni okvir za pilotne projekte z UI in agenti UI v javni upravi: časovna omejitev, izhodiščne meritve, stopnje avtonomije, beleženje in javno poročanje, tudi o neugodnih rezultatih.

  Naslovniki: ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za digitalno preobrazbo · Rok: leto 2027 · Vir: R4.3 (primeri 4.5–4.7, razdelek 6.4)

8.4 Sektorski okviri

- **O-7 Zdravstvo: pripravite okvir za zapisovalnike in prepoznavo govora.** Če bo nacionalna rešitev za prepoznavo govora dobila funkcije povzemanja ali bodo izvajalci uvajali tržne zapisovalnike, naj pristojne institucije pripravijo minimalna merila za dobavitelje, vzorec ocene učinka na varstvo podatkov, pravila za obveščanje pacientov z možnostjo zavrnitve in pot za prijavo napak. Obvezen pregled vsakega zapisa naj ostane pri izvajalcu zdravstvene dejavnosti.

  Naslovniki: ministrstvo, pristojno za zdravje, NIJZ, JAZMP · Rok: pred širšo uvedbo · Vir: R4.3 (primer 4.6)

- **O-8 Izobraževanje: pred uvedbo orodij za učence uredite pravno podlago.** Pred uvedbo orodij UI za učence in dijake naj ministrstvo preveri pravno podlago za obdelavo njihovih podatkov, zagotovi oceno učinka in neodvisno oceno tveganj, preveri razvrstitev po točki 3 Priloge III in prepoved prepoznavanja čustev ter predvidi javno poročanje o uporabi in učinkih.

  Naslovnik: ministrstvo, pristojno za izobraževanje · Rok: pred uvedbo · Vir: R4.3 (primer 4.7)

8.5 Kompetence

- **O-9 Pismenost razumite kot razvoj presoje, ne kot formalno usposabljanje.** Pri nadzoru nad 4. členom naj inšpekcija preverja, ali so ukrepi sorazmerni vlogam in tveganjem, ne pa potrdil ali enotnih programov. Država naj v skladu s členom 4(2) podpira zlasti MSP. Generativna UI povečuje razkorak med izkazanimi in dejanskimi kompetencami, saj prepričljiv izdelek še ne pomeni razumevanja. Izobraževalni sistem in delodajalci naj zato krepijo zmožnost presoje in preverjanja izhodov, ne le spretnosti uporabe orodij.

  Naslovniki: inšpekcija za informacijsko družbo, ministrstva, pristojna za izobraževanje in digitalno preobrazbo · Rok: stalno · Vir: R4.3 (razdelek 5.4)

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

8.6 Suverenost in odvisnost od ponudnikov

- **O-10 Javne rešitve zasnujte tako, da omogočajo zamenjavo ponudnika.** Nacionalna strategija UI do leta 2030 kot ključni poudarek navaja suverenost in zmanjšanje odvisnosti od zaprtih komercialnih rešitev [18]. Javne rešitve naj zato podpirajo zamenjavo modela in ponudnika, kot to počneta francoska skupna platforma Albert API in estonski program AI Leap. Skupna državna platforma z odobrenim okoljem lahko organom javne uprave prihrani podvajanje infrastrukture in znanja. Pri tem je treba upoštevati, da lokalna postavitev tveganj ne odpravi, temveč jih prenese na upravljavca.

  Naslovnik: ministrstvo, pristojno za digitalno preobrazbo · Rok: pri načrtovanju nacionalnih rešitev · Vir: R2.3 (Albert API), R4.3 (primer 4.7), NsUI 2030 [18]

8.7 Mednarodno sodelovanje

- **O-11 Okrepite sodelovanje v mednarodnih procesih.** Slovenski strokovnjaki naj aktivno sodelujejo v CEN-CENELEC JTC 21, zlasti pri standardih, ki še niso harmonizirani. Slovenija naj presodi podpis in ratifikacijo Okvirne konvencije Sveta Evrope, slovenske izkušnje, na primer javno objavo sistemov UI po 21. členu ZIUDHPUI, pa predstavi v okviru OECD, UNESCO in Globalnega dialoga o upravljanju UI. Slovenska podjetja, ki razvijajo napredne sisteme UI, lahko prostovoljno poročajo po okviru OECD za poročanje po hirošimskem procesu, kar povečuje njihovo prepoznavnost na mednarodnih trgih.

  Naslovniki: ministrstvo, pristojno za digitalno preobrazbo, ministrstvo, pristojno za zunanje zadeve, SIST · Rok: stalno · Vir: poglavje 2, R4.1 (razdelek 10.2)

8.8 Spremljanje

- **O-12 Spremljajte izvajanje s kazalniki.** Nacionalna strategija UI do leta 2030 predvideva okrepljeno vlogo opazovalnice za UI in kazalnike uspešnosti [18]. Kazalniki o izvajanju Akta o UI naj vključujejo delež organov javnega sektorja z objavo po 21. členu ZIUDHPUI, število sistemov v peskovniku in zaključenih poročil, število razvrstitvenih zapisov in ocen učinka na temeljne pravice v javnem sektorju ter število prijavljenih resnih incidentov. Predlog kazalnikov za organizacije je v poglavju 9.

  Naslovniki: ministrstvo, pristojno za digitalno preobrazbo, AKOS · Rok: leto 2027 · Vir: R4.3 (razdelek 6.5), NsUI 2030 [18]

9 Časovni načrt in kazalniki

Preglednica 11 razvršča priporočila po obdobjih, v katerih naj bodo izvedena, da bo organizacija dosegla zakonske roke. Ne ponavlja rokov iz razdelka 3.1, temveč iz njih izpelje, kdaj mora biti posamezen ukrep končan.

Preglednica 11: Časovni načrt izvajanja priporočil

Obdobje	Ponudniki	Uvajalci	Odločevalci
Takoj (do 2. 12. 2026)	S-1–S-7; P-1, P-13, P-14, P-16; T5-3	S-1–S-7; U-10, U-13, U-16	O-2
Prva polovica leta 2027	S-8–S-10; P-2, P-4, P-15; razvrstitveni zapisi za vse sisteme s področij Priloge III	S-8–S-10; U-3, U-4; poskusna ocena učinka na temeljne pravice (U-5)	O-1 (do konca 1. četrtletja), O-4, O-5, O-6, O-12
Do 2. 8. 2027	P-3, P-5, P-6, P-8, P-9 (v izvajanju)	U-6 (priprava obvestil)	O-3
Do 2. 12. 2027	P-5–P-12 za visokotvegane sisteme iz Priloge III	U-5, U-6, U-7, U-11, U-14	–
Do 2. 8. 2028	P-5–P-12 in T8-1, T8-2 za proizvode iz Priloge I	kot zgoraj za proizvode iz Priloge I	–
Stalno	S-3, S-11–S-13; P-15, P-17	S-3, S-11–S-13; U-9, U-12	O-9–O-11

Za spremljanje izvajanja v organizaciji predlagamo kazalnike iz Preglednice 12. Kazalniki naj se spremljajo vsaj vsakih šest mesecev in ob vsaki večji spremembi sistema.

Preglednica 12: Predlog kazalnikov za organizacije

Kazalnik	Kaj meri	Povezava
Delež sistemov UI z razvrstitvenim zapisom	Pregled nad sistemi	S-1, S-2
Delež sistemov, pri katerih je bila po zadnji spremembi opravljena ponovna presoja	Sledenje spremembam	S-3
Delež zaposlenih v ključnih vlogah, ki so se udeležili ukrepov pismenosti za svoj sistem	Pismenost po vlogah	S-5
Delež sistemov s preizkusnim naborom in vnaprej določenimi merili	Kakovost	S-8
Delež sprejetih, spremenjenih in zavrnjenih predlogov sistema	Dejanski človeški nadzor	U-7
Največja razlika v točnosti med skupinami oseb	Pristranskost	P-5, T1-1
Število prijavljenih napak, incidentov in pritožb ter čas do odziva	Odzivnost	S-10, U-11

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Kazalnik	Kaj meri	Povezava
Cena na rešen primer v primerjavi z izhodiščem	Vrednost	U-1, U-12
Delež dejanj agentov z učinkom na ljudi, pri katerih je zabeležena človeška odobritev	Nadzor nad agenti	T4-1

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

10 Zaključek

Projekt NOSI-AI je v dveh letih preučil, kako se zahteve Akta o UI prevedejo v tehnične in organizacijske ukrepe. Glavna ugotovitev tega poročila je, da tveganja sistema UI pogosto ne določa tehnologija, temveč namen in način uvedbe. Ista tehnologija je lahko neškodljiv pripomoček ali visokotvegani sistem, odvisno od tega, za kaj se uporablja in kdo ima zadnjo besedo. Zato je skupno jedro priporočil, ki velja za vse, pomembnejše od posameznih tehnoloških rešitev: popis, razvrstitev po namenu, jasne vloge, pismenost, merila pred uvedbo in pot za napake.

Primeri iz projekta kažejo, da se dobra praksa ne konča z uvedbo. Organizacije, ki so javno poročale tudi o nedoseženih ciljih, ki so sistem ustavile, ko ni prinašal koristi, ali ki so uvedbo zamaknile, dokler ni bila urejena pravna podlaga, so ravnale odgovorno. Utemeljen negativen izid je del dobre prakse, ne neuspeh.

Odlog obveznosti za visokotvegane sisteme do decembra 2027 in avgusta 2028 daje čas za pripravo, ne za odlašanje. Harmonizirani standardi bodo večinoma objavljeni šele v letu 2027, smernice Komisije pa so deloma še v pripravi. Organizacije, ki bodo do tedaj uredile skupno jedro in dokumentirale svoje odločitve, bodo nove zahteve lahko vključile brez večjih sprememb.

Akt o UI je del širšega mednarodnega okvira, ki temelji na skupnih načelih OECD, UNESCO in Sveta Evrope. Organizacija, ki izvaja priporočila iz tega poročila, izpolni večino pričakovanj teh okvirov in je pripravljena tudi na trge zunaj Evropske unije. Slovenija lahko s prevodi, vodniki, preizkusnimi nabori v slovenščini in delujočim peskovnikom bistveno olajša izpolnjevanje zahtev, zlasti za mala podjetja in javni sektor. Kako bodo dejavnosti projekta nadaljevane, opredeljuje R5.2.

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Viri

Povezave so bile preverjene 25. oktobra 2026. Pri rezultatih projekta NOSI-AI je naveden datum zadnje različice.

Pravni in izvedbeni viri Evropske unije in Slovenije

1. Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci). UL L, 2024/1689, 12. 7. 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
2. Uredba (EU) 2026/1744 Evropskega parlamenta in Sveta z dne 8. julija 2026 o spremembi uredb (EU) 2024/1689, (EU) 2018/1139 in (EU) 2023/1230 (digitalni omnibus o UI). UL L, 2026/1744, 24. 7. 2026. https://eur-lex.europa.eu/eli/reg/2026/1744/oj
3. Izvedbeni sklep Komisije (EU) 2026/2274 z dne 12. oktobra 2026 o harmoniziranih standardih za visokotvegane sisteme UI (sklic na EN 18286:2026). UL L, 14. 10. 2026. https://eur-lex.europa.eu/eli/dec_impl/2026/2274/oj
4. Evropska komisija (2026). Smernice o izvajanju obveznosti glede preglednosti za nekatere sisteme UI po 50. členu Akta o UI (vsebina potrjena s C(2026) 5054, 20. 7. 2026). https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems
5. Evropska komisija (2026). Kodeks prakse za preglednost vsebin, ustvarjenih z UI – vprašanja in odgovori (končna različica 10. 6. 2026). https://digital-strategy.ec.europa.eu/en/faqs/code-practice-transparency-ai-generated-content
6. Evropska komisija (2026). Varnejša in preglednejša umetna inteligenca (začetek uporabe pravil o preglednosti, nabor ikon EU), 2. 8. 2026. https://commission.europa.eu/news-and-media/news/safer-and-more-transparent-ai-2026-08-02_sl
7. Evropska komisija (2026). Osnutek smernic za razvrščanje visokotveganih sistemov UI, 19. 5. 2026. https://digital-strategy.ec.europa.eu/en/library/draft-guidelines-high-risk
8. Evropska komisija (2025–2026). Supporting the implementation of the AI Act with clear guidelines (pregled objavljenih in napovedanih smernic), posodobljeno 31. 7. 2026. https://digital-strategy.ec.europa.eu/en/news/supporting-implementation-ai-act-clear-guidelines
9. Evropska komisija (2025). Osnutek smernic in predloge za poročanje o resnih incidentih po 73. členu Akta o UI, 26. 9. 2025. https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks
10. Evropska komisija (2025–2026). AI literacy – questions and answers. https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
11. Evropska komisija, služba za pomoč pri Aktu o UI (2026). How are AI agents addressed within the AI Act? https://ai-act-service-desk.ec.europa.eu/en/ai-act/faq/how-are-ai-agents-addressed-within-ai-act-0
12. Evropska komisija, Public Buyers Community (2025). Updated EU AI model contractual clauses (MCC-AI). https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses
13. Evropski nadzornik za varstvo podatkov (2025). Orientations for ensuring data protection compliance when using Generative AI systems, različica 2, 28. 10. 2025. https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf
14. Direktiva (EU) 2024/2853 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o odgovornosti za proizvode z napako. UL L, 2024/2853, 18. 11. 2024. https://eur-lex.europa.eu/eli/dir/2024/2853/oj

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

15. Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi (Akt o kibernetski odpornosti). UL L, 2024/2847, 20. 11. 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj
16. OWASP GenAI Security Project (2025). OWASP Top 10 for Agentic Applications for 2026, december 2025. https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/
17. Zakon o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci (ZIUDHPUI). Uradni list RS, št. 85/25. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2025-01-3035/zakon-o-izvajanju-uredbe-eu-o-dolocitvi-harmoniziranih-pravil-o-umetni-inteligenci-ziudhpui
18. Vlada Republike Slovenije (2026). Vlada sprejela nacionalno strategijo umetne inteligence do 2030 za suvereno in zaupanja vredno UI, 5. 3. 2026. https://www.gov.si/novice/2026-03-05-vlada-sprejela-nacionalno-strategijo-umetne-inteligence-do-2030-za-suvereno-in-zaupanja-vredno-ui/

Mednarodni viri

19. OECD (2019, posodobljeno 2024). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
20. UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137
21. UNESCO (2023). Readiness assessment methodology: a tool of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000385198
22. UNESCO (2023). Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000386276
23. Svet Evrope (2026). European Union ratifies the Council of Europe Framework Convention on Artificial Intelligence, 15. 5. 2026. https://www.coe.int/en/web/artificial-intelligence/-/european-union-ratifies-the-council-of-europe-framework-convention-on-artificial-intelligence
24. Svet Evrope (2026). Framework Convention marks two years: anniversary conference to advance trustworthy AI, september 2026. https://www.coe.int/en/web/artificial-intelligence/-/framework-convention-marks-two-years-anniversary-conference-to-advance-trustworthy-ai
25. Svet Evrope (2025–2026). HUDERIA – risk and impact assessment of AI systems (metodologija, potrjena 26. 2. 2025; model, potrjen 25. 2. 2026). https://www.coe.int/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems
26. Združeni narodi (2026). Independent International Scientific Panel on AI – pogosta vprašanja (resolucija 79/325, Globalni dialog o upravljanju UI). https://www.un.org/independent-international-scientific-panel-ai/en/faq
27. Vlada Indije, NeGD (2026). AI Impact Summit 2026 concludes with adoption of New Delhi Declaration, 5. 3. 2026. https://negd.gov.in/press_release/ai-impact-summit-2026-concludes-with-adoption-of-new-delhi-declaration/
28. OECD (2026). OECD Due Diligence Guidance for Responsible AI, 19. 2. 2026. https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-ai_41671712-en.html
29. OECD.AI (2026). Hiroshima AI Process Reporting Framework 2.0 – launch, 28. 5. 2026. https://oecd.ai/en/haip-2-launch
30. Vlada Republike Slovenije (2024). GPAI and OECD promote international efforts for trustworthy AI, 15. 7. 2024. https://www.gov.si/en/news/2024-07-15-gpai-and-oecd-promote-international-efforts-for-trustworthy-ai/
31. Vlada Republike Slovenije (2024). Slovenia hosts the Global Forum on the Ethics of Artificial Intelligence, 9. 2. 2024. https://www.gov.si/en/news/2024-02-09-slovenia-hosts-the-global-forum-on-the-ethics-of-artificial-intelligence/

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Rezultati projekta NOSI-AI

32. Škrjanc, M., Škrjanc, M. (2025). Rezultat 1.1: Pregled in ocena regulativnega okvira, določenega v Aktu o UI za UI z visoko stopnjo tveganja. CRP V2-24065 NOSI-AI, IJS, 30. 3. 2025.
33. Škrjanc, M., Škrjanc, M. (2025). Rezultat 1.3: Seznam standardov za preverjanje skladnosti rešitev UI. CRP V2-24065 NOSI-AI, IJS, 30. 6. 2025.
34. Škrjanc, M., Škrjanc, M. (2025/2026). Poročilo 2.2: Seznam relevantnih EU in mednarodnih standardov in predlog za pripravo nacionalnih standardov. CRP V2-24065 NOSI-AI, IJS, 30. 12. 2025, dopolnjeno 27. 2. 2026.
35. Škrjanc, M., Škrjanc, M. (2025/2026). Poročilo 2.3: Dobre prakse uvajanja UI sistemov. CRP V2-24065 NOSI-AI, IJS, 30. 12. 2025, dopolnjeno 27. 2. 2026.
36. Škrjanc, M., Škrjanc, M. (2026). Poročilo 4.1: Predlog prilagoditev nacionalnih standardov (tehnični vidik). CRP V2-24065 NOSI-AI, IJS, oktober 2026.
37. Škrjanc, M., Škrjanc, M. (2026). Poročilo 4.3: Dobre prakse uvajanja UI sistemov – dopolnitev. CRP V2-24065 NOSI-AI, IJS, 20. 10. 2026, dopolnjeno 25. 10. 2026.

Drugi viri

38. Gartner (2025). Gartner predicts over 40% of agentic AI projects will be canceled by end of 2027, 25. 6. 2025. https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027
39. eWeek (2025). »Catastrophic failure«: AI agent wipes production database, then lies about it (primer Replit in SaaStr), 22. 7. 2025. https://www.eweek.com/news/replit-ai-coding-assistant-failure/
40. The Hacker News (2025). Salesforce patches critical ForcedLeak bug exposing CRM data via AI prompt injection, 25. 9. 2025. https://thehackernews.com/2025/09/salesforce-patches-critical-forcedleak.html
41. The Hacker News (2025). Zero-click AI vulnerability exposes Microsoft 365 Copilot data without user interaction (CVE-2025-32711), 12. 6. 2025. https://thehackernews.com/2025/06/zero-click-ai-vulnerability-exposes.html
42. American Bar Association, Business Law Today (2024). BC Tribunal confirms companies remain liable for information provided by AI chatbot (Moffatt proti Air Canada, 14. 2. 2024). https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-february/bc-tribunal-confirms-companies-remain-liable-information-provided-ai-chatbot/
43. Strokovna skupina na visoki ravni za umetno inteligenco (2019). Etične smernice za zaupanja vredno umetno inteligenco. Evropska komisija, 8. 4. 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
44. Predstavništvo Evropske komisije v Sloveniji (2024). Podpis Okvirne konvencije Sveta Evrope o umetni inteligenci, 5. 9. 2024. https://slovenia.representation.ec.europa.eu/novice-dogodki/novice-0/podpis-okvirne-konvencije-sveta-evrope-o-umetni-inteligenci-2024-09-05_sl

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Priloga A: Pregled mednarodnih okvirov in drugih predpisov

Priloga dopolnjuje Preglednico 3 z mednarodnimi instrumenti iz poglavja 2 in s predpisi Evropske unije zunaj Akta o UI, na katere se sklicujejo priporočila. Stanje je navedeno na dan 25. 10. 2026.

Preglednica 13: Mednarodni okviri in drugi predpisi, na katere se sklicujejo priporočila

Instrument	Vrsta	Stanje	Kje v poročilu
Priporočilo Sveta OECD o umetni inteligenci [19]	nezavezujoče	sprejeto 2019, posodobljeno 2024	2.1, Priloga F
Priporočilo UNESCO o etiki umetne inteligence; orodji RAM in EIA [20–22]	nezavezujoče	sprejeto 2021; orodji 2023	2.1, 2.4
Vodilna načela in kodeks ravnanja G7 (hirošimski proces); okvir za poročanje 2.0 [29]	prostovoljno	kodeks 2023; okvir 2.0 od 28. 5. 2026	2.1, 2.4, O-11
Okvirna konvencija Sveta Evrope o UI (CETS št. 225) [23, 24]	mednarodna pogodba	21 podpisnic; EU ratificirala 15. 5. 2026; še ne velja	2.2, O-11
Metodologija in model HUDERIA [25]	nezavezujoče	potrjena 2025 in 2026	2.2, U-5
Globalni digitalni dogovor; znanstveni panel in Globalni dialog o upravljanju UI [26]	politična zaveza; mehanizma ZN	panel od 2025; prvo zasedanje dialoga julija 2026	2.3
Smernice OECD o potrebni skrbnosti za odgovorno UI [28]	nezavezujoče	objavljene 19. 2. 2026	2.4, 2.5, S-10
ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005	mednarodni standardi	objavljeni	2.4, S-12, P-9
Seznam tveganj OWASP za agentne aplikacije [16]	strokovni vir	december 2025	P-8, T3-3, T4-3
GDPR (Uredba (EU) 2016/679)	zavezujoče	velja	vse
Direktiva (EU) 2024/2853 o odgovornosti za proizvode z napako [14]	zavezujoče po prenosu	rok za prenos 9. 12. 2026	P-17, T8-2
Akt o kibernetski odpornosti (Uredba (EU) 2024/2847) [15]	zavezujoče	poročanje od 11. 9. 2026, večina obveznosti od 11. 12. 2027	P-8, T8-2

Priloga B: Kontrolni seznam za uvajanje UI

Kontrolni seznam nadgrajuje zasnovo iz R2.3 in kontrolne točke iz Preglednice 17 v R4.3. Skupni del izpolnite za vsak sistem, dodatek glede na vrsto sistema ali oba, če sistem združuje obe vrsti. Vprašanja so zapisana kot preverljive trditve. Oznaka ▲ pomeni, da je točka posebej pomembna, če je sistem lahko visokotvegan ali vpliva na odločitve o ljudeh. Za vsako točko zapišite dokaz, lastnika in stanje (da, delno, ne). »Da« brez dokaza štejte kot »delno«, »ne« in »delno« pa vodita v načrt ukrepov z rokom. Seznam izpolnite pred uvedbo, ob novem modelu, novi funkciji ali razširjenem namenu ter vsaj vsakih šest mesecev. Seznam ni pravna kvalifikacija tveganosti.

Preglednica 14: Kontrolni seznam – skupni del

Št.	Kontrolna trditev	Primer dokaza	Priporočilo
	Zasnova		
1	Namen sistema in izključene rabe so zapisani.	razvrstitveni zapis, navodila	S-2, P-2
2 ▲	Jasno je, kdo ima zadnjo besedo pri odločitvah, ki vplivajo na ljudi.	matrika odgovornosti	S-4, U-7
3	Vloga organizacije po Aktu o UI je določena in zapisana.	popis sistemov	S-1, P-1
4	Podatki, ki vstopajo v sistem, so razvrščeni po zaupnosti; kjer je potrebna, je opravljena ocena učinka na varstvo podatkov.	razvrstitev podatkov, ocena učinka	S-7, U-5
5 ▲	Razvrstitev po Aktu o UI je dokumentirana skupaj s predpostavkami.	razvrstitveni zapis	S-2
	Podatki in razvoj		
6	Znano je, kateri podatki vstopajo v sistem, vključno s prostimi vnosi.	podatkovni zemljevid	S-1, U-8
7	Polja, ki za namen niso potrebna, so izločena.	seznam izločenih polj	U-8, P-4
8	Vsebina interakcij je ločena od telemetrije, roki hrambe so določeni.	politika beleženja	S-9
	Preizkušanje		
9 ▲	Merila uspeha in preizkusni nabor so določeni pred preizkusom.	preizkusni nabor, merila	S-8, U-4
10 ▲	Rezultati so izmerjeni ločeno po skupinah oseb.	poročilo po skupinah	P-5, T1-1
11	Omejitve sistema so zapisane in sporočene uporabnikom.	navodila, gradiva za uporabnike	P-10
	Uvedba		
12	Znani so lokacija obdelave, dobavitelji in podobdelovalci.	presoja ponudnika	S-7, U-3

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Št.	Kontrolna trditev	Primer dokaza	Priporočilo
13	Vloge in obveznosti so urejene v pogodbi, vključno z obveščanjem o spremembah in varnim izstopom.	pogodba	U-3, S-11
14	Dostopi so sledljivi in omejeni na potrebne.	pravila dostopa, dnevnik	T3-1, T4-1
15	Uporabniki so usposobljeni za konkretni sistem.	evidenca ukrepov pismenosti	S-5
16	Osebe, na katere sistem vpliva, so obveščene o uporabi UI.	besedilo obvestila	P-13, U-6, U-10
	Obratovanje in umik		
17 ▲	Človeški nadzor dejansko deluje: odgovorni razumejo izhode, smejo jih zavrniti, delež zavrnitev pa se meri.	delež zavrnjenih ali popravljenih predlogov	U-7, P-7
18	Kakovost in vrednost se merita tudi med obratovanjem, ne le z obsegom rabe.	poročila o spremljanju	U-12, P-12
19 ▲	Obstaja postopek za napake, incidente in pritožbe.	postopek, evidenca	S-10, U-11, U-16
20	Ob novem modelu, funkciji ali razširjenem namenu se presoja ponovi; umik je načrtovan.	dnevnik sprememb, načrt izstopa	S-3, S-11

Preglednica 15: Kontrolni seznam – dodatek A za generativno UI in agente

Št.	Kontrolna trditev	Primer dokaza	Priporočilo
A1	Vhodi so upravljani s predlogami, filtri, opozorili in navodili.	pravila za vnos	U-8
A2	Hramba pozivov in izhodov ima določen namen, rok in dostop.	politika beleženja	S-9
A3	Baza znanja ima lastnika, različice in pravice dostopa, ki sledijo izvornim sistemom.	register baze znanja	T3-1, T3-2
A4	Odgovori navajajo vire; delež izmišljenih navedb se meri.	poročilo o preizkusu	T2-3, T3-3
A5	Pri zunanjem ponudniku so znani lokacija obdelave, uporaba podatkov za učenje in različica modela.	pogodba, dnevnik različic	U-3, P-15
A6 ▲	Zunanji vnosi se obravnavajo kot nezaupljivi (zaščita pred vrinjenimi navodili).	model groženj	P-8, T4-3
A7 ▲	Agent ima najmanjše potrebne pravice.	matrika avtonomije in pravic	T4-1
A8 ▲	Pred nepovratnimi ali tveganimi dejanji je potrebna potrditev človeka.	točke odobritve	T4-1
A9	Dnevnik zajame celotno pot agenta in ga agent ne more spremeniti.	specifikacija dnevnika	T4-2
A10	Preizkus preverja proces, ne le končnega izida.	poročilo o preizkusu procesa	T4-4

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Preglednica 16: Kontrolni seznam – dodatek B za klasično strojno učenje

Št.	Kontrolna trditev	Primer dokaza	Priporočilo
B1 ▲	Učna populacija je reprezentativna za populacijo uporabe; vrzeli so znane.	podatkovni list	P-4
B2 ▲	Preverjeno je, ali posredni znaki nadomeščajo zaščitene lastnosti.	analiza značilk	P-5
B3	Podatki se zbirajo šele, ko so za namen res potrebni.	zapis o minimizaciji	U-8
B4	Modeli in uteži so varovani kot osebni podatki.	pravila dostopa do modelov	T1-3
B5 ▲	Prag odločanja je določen glede na ceno napak in utemeljen.	utemeljitev praga	T1-1
B6	Premik podatkov se spremlja.	poročila o spremljanju	T1-2
B7	Povratne zanke so prepoznane in obvladovane.	analiza povratnih zank	T1-2
B8 ▲	Za posameznika je na voljo razumljivo pojasnilo odločitve.	vzorec pojasnila	T1-4
B9	Model je bil preverjen na podatkih, ki niso bili uporabljeni pri razvoju.	poročilo o zunanji validaciji	P-6

Priloga C: Delovni list za presojo lastnega primera

Delovni list je namenjen hitri prvi presoji sistema, preden organizacija izpolni celoten kontrolni seznam. Kratki zapiski zadoščajo. Odgovori usmerijo k točkam kontrolnega seznama in priporočilom, ki zahtevajo pozornost.

Preglednica 17: Osem vprašanj za presojo lastnega primera

Tema	Vprašanje	Kontrolni seznam in priporočila
1 Namen	Kaj sistem počne in kdo ga uporablja?	točka 1; S-1, S-2
2 Odločanje	O čem odloča ali kaj predlaga in kdo ima zadnjo besedo?	točki 2 in 17; U-7
3 Podatki	Kateri podatki vstopajo, tudi prosti vnosi, in v kateri razred zaupnosti sodijo?	točki 4 in 6, A1; S-7, U-8
4 Dobavitelj	Kje teče model in kdo je dobavitelj?	točki 12 in 13, A5; U-3
5 Akt o UI	Kakšna je vloga organizacije in ali je primer blizu Priloge III?	točki 3 in 5; razdelka 3.2 in 3.3
6 Kakovost	Kako boste vedeli, da sistem deluje dobro za vse uporabnike?	točke 9, 10 in 18; S-8, P-5
7 Napake	Kaj se zgodi, ko se sistem zmoti, in kdo to opazi?	točki 17 in 19; S-10
8 Opozorilni znaki	Kateri opozorilni znaki iz tehnoloških profilov veljajo za vaš sistem?	poglavje 7

Priloga D: Preslikava priporočil na vire

Preglednica navaja za vsako priporočilo vrsto in vir v rezultatih projekta ali v drugih virih. Oznaka »zahteva« pomeni, da priporočilo vsaj deloma izhaja iz zavezujočega predpisa; podrobnosti so v vrstici pod priporočilom.

Preglednica 18: Preslikava priporočil na vire

Oznaka	Priporočilo	Vrsta	Vir
S-1	Popišite vse sisteme UI, tudi neformalno rabo	dobra praksa / zahteva	R4.3 (primer 4.4), R2.3 (Helsinki)
S-2	Za vsak sistem pripravite razvrstitveni zapis	zahteva	R4.3 (razdelek 5.2, Prilogi A in D), R4.1 (poglavje 8)
S-3	Razvrstitev ponovite ob vsaki spremembi	dobra praksa / zahteva	R4.3 (vzorec 8, Priloga D)
S-4	Določite vloge in odgovornosti	dobra praksa	R2.3, R4.3 (primer 4.5)
S-5	Ukrepe za pismenost načrtujte po vlogah	zahteva	R4.3 (razdelek 5.4, Preglednica 15)
S-6	Sprejmite pravilnik o rabi generativne UI	dobra praksa	R4.3 (primer 4.1 ORF)
S-7	Najprej razvrstite podatke, nato izberite rešitev	dobra praksa / zahteva	R2.3 (France Travail, Albert API), vzorec 4
S-8	Pred uvedbo določite merila uspeha in pripravite preizkusni nabor	dobra praksa / zahteva	R4.1 (poglavje 9, Priloga B.3), vzorca 6 in 12
S-9	Vsebino interakcij ločite od telemetrije	zahteva	R2.3 (Albert API, Helsinki), vzorec 1
S-10	Vzpostavite pot za napake, incidente in pritožbe	zahteva	R4.3 (primer 4.6), Smernice OECD o potrebni skrbnosti [28]
S-11	Umik načrtujte ob uvedbi	dobra praksa	R4.3 (razdelek 3.4, vzorec 12)
S-12	Ureditev zasnujte tako, da pokrije več okvirov	dobra praksa	poglavje 2, R4.1 (Priloga A)
S-13	Izberite sorazmeren model in spremljajte porabo virov	dobra praksa	razdelek 2.5, R4.3 (vzorec 12)
P-1	Ugotovite, ali ste ponudnik	zahteva	razdelek 3.2
P-2	Predvideni namen in izključene rabe zapišite jasno in dosledno	zahteva	R4.3 (primer 4.6, razdelek 5.2)
P-3	Uredite sodelovanje v vrednostni verigi	zahteva	R4.3 (vzorec 7)
P-4	Dokumentirajte nabore podatkov	zahteva	R1.3, R2.2

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Oznaka	Priporočilo	Vrsta	Vir
P-5	Pristranskost merite po skupinah in v celotnem postopku	zahteva	R4.3 (primer 4.3, vzorec 11), R4.1 (Priloga B.3)
P-6	Sistem preizkusite po vnaprej določenih merilih	zahteva	R4.1 (poglavje 9, Priloga B.3), R4.3 (primer 4.2)
P-7	Človeški nadzor zasnujte v sistemu	zahteva	R2.3 (France Travail), R4.3 (primer 4.5, vzorca 2 in 13), R2.2 (prednostno področje 2)
P-8	Upoštevajte varnostna tveganja, značilna za UI	zahteva	R2.3 (Finterai), R4.3 (primer 4.5), vzorec 5
P-9	Sistem vodenja kakovosti gradite na SIST EN 18286:2026	zahteva	R4.1 (razdelek 4.1, Priloga A)
P-10	Navodila naj uvajalcu omogočijo izpolniti njegove obveznosti	zahteva	R4.3 (vzorca 9 in 10), R2.2 (prednostno področje 1)
P-11	Opravite ugotavljanje skladnosti in registracijo	zahteva	R4.1 (razdelek 9.3)
P-12	Spremljajte sistem po dajanju na trg in prijavljajte resne incidente	zahteva	R4.3 (primer 4.6, Preglednica 17)
P-13	Ljudi obvestite, da komunicirajo s sistemom UI	zahteva	R4.3 (razdelek 5.1, Priloga B)
P-14	Sintetične vsebine označite strojno berljivo	zahteva	R4.3 (primer 4.1, razdelek 5.1)
P-15	Pri gradnji na modelu drugega ponudnika zahtevajte dokumentacijo in nadzorujte spremembe	zahteva	R2.3 (Albert API)
P-16	Izkoristite olajšave za MSP in javne vodnike	zahteva	R4.3 (primer 4.2, razdelek 6.4)
P-17	Odločitve in preizkuse dokumentirajte kot dokaz skrbnosti	dobra praksa	Direktiva (EU) 2024/2853 [14]
U-1	Začnite pri problemu in merilu uspeha, ne pri orodju	dobra praksa	R4.3 (primer 4.5, vzorec 12)
U-2	Premišljeno izberite pot: storitev, izdelek ali lasten razvoj	dobra praksa	razdelek 3.2, S-7
U-3	Postavite ponudniku prava vprašanja in odgovore prenesite v pogodbo	zahteva	R2.3 (Finterai), R4.3 (primer 4.6, razdelek 6.4)
U-4	Pred nakupom rešitve preizkusite na lastnih primerih	dobra praksa	S-8, R4.1 (poglavje 9)
U-5	Opravite oceno učinka na varstvo podatkov in, kjer je predpisana, oceno učinka na temeljne pravice	zahteva	R4.3 (primer 4.3, razdelek 6.5), HUDERIA [25]
U-6	Obvestite delavce in osebe, na katere sistem vpliva	zahteva	R4.3 (primera 4.6 in 4.7)
U-7	Poskrbite, da je človeški nadzor dejanski	zahteva	R2.3 (France Travail), vzorec 2

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Oznaka	Priporočilo	Vrsta	Vir
U-8	Upravljajte vhodne podatke in pozive	zahteva	R2.3 (France Travail, Finterai), vzorec 3
U-9	Sistem uporabljajte v mejah predvidenega namena	zahteva	razdelek 3.3, R4.3 (Priloga D)
U-10	Izpolnite obveznosti razkritja uvajalca	zahteva	R4.3 (primer 4.1, razdelek 5.1, Priloga B)
U-11	Spremljajte delovanje, hranite dnevnike in poročajte o incidentih	zahteva	R4.3 (primer 4.6, Preglednica 17)
U-12	Merite vrednost in bodite pripravljeni sistem ustaviti	dobra praksa	R4.3 (razdelek 3.1, vzorec 12), Gartner [38]
U-13	Objavite vse sisteme UI v uporabi	zahteva	R4.3 (primer 4.4, Priloga C), R2.3 (Helsinki)
U-14	Registrirajte visokotvegane sisteme in povežite javne vnose	zahteva	R4.3 (razdelek 6.5)
U-15	Pilotne projekte in javna naročila zasnujte preverljivo	dobra praksa	R4.3 (primeri 4.5–4.7, razdelek 6.4)
U-16	Zagotovite pot do človeka in pritožbeno pot	dobra praksa	R2.3 (Helsinki), R4.3 (razdelek 6.4), razdelek 2.5
T1-1	Prag odločanja določite glede na ceno napak	zahteva	R4.3 (primer 4.3)
T1-2	Spremljajte premik podatkov in povratne zanke	zahteva	R2.3 (kontrolni seznam)
T1-3	Modele in uteži varujte kot osebne podatke	dobra praksa	R2.3 (Finterai), vzorec 5
T1-4	Zagotovite razumljivo pojasnilo za posameznika	zahteva	R1.1, R4.3 (primer 4.3)
T2-1	Klepetalnik naj pove, kaj je, in naj ve, česa ne sme	zahteva	R2.3 (Helsinki), R4.3 (Priloga B)
T2-2	Zavezujoče informacije naj temeljijo na preverjenih virih	dobra praksa	[42]
T2-3	Merite točnost odgovorov v slovenščini	dobra praksa	R2.3 (Helsinki), vzorec 6
T3-1	Pravice dostopa prenesite v iskanje	dobra praksa	R2.3 (Albert API)
T3-2	Bazo znanja upravljajte kot vir resnice	dobra praksa	R2.3 (France Travail, Albert API)
T3-3	Ločeno preverite iskanje in odgovor	dobra praksa	S-8, OWASP [16]
T4-1	Avtonomijo stopnjujte in vežite na človeško odobritev	dobra praksa	R4.3 (primer 4.5, vzorec 13)
T4-2	Beležite celotno pot in ločite okolja	dobra praksa	R4.3 (primer 4.5), [39]
T4-3	Vtičnike in povezave obravnavajte kot dobavitelje	dobra praksa	OWASP [16], [40], [41]
T4-4	Preverite proces, ne le končnega izida	dobra praksa	S-8, R4.3 (primer 4.5)

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Oznaka	Priporočilo	Vrsta	Vir
T5-1	Izberite orodja, ki označujejo, in oznak ne odstranjujte	zahteva	R4.3 (primer 4.1, razdelek 5.1)
T5-2	Ločite ilustracijo od globokega ponaredka	zahteva	R4.3 (primer 4.1)
T5-3	Ponudniki splošnih orodij naj vgradijo zaščite pred prepovedanimi izhodi	zahteva	[2]
T6-1	Točnost preizkusite pri skupinah, pri katerih je prepoznava slabša	dobra praksa	R4.3 (primer 4.6)
T6-2	Vsak zapis naj pregleda in potrdi človek	dobra praksa	R4.3 (primer 4.6)
T6-3	Obvestite osebe in ob vsaki novi funkciji preverite status orodja	GDPR (13. člen)	R4.3 (primer 4.6)
T7-1	Pred uvedbo preverite prepovedi	zahteva	R1.1, razdelek 3.3
T7-2	Mejo do prepoznavanja čustev dokumentirajte	zahteva	R4.3 (primer 4.7)
T7-3	Pri biometriji preverite tudi pravno podlago po GDPR	zahteva	R1.1
T8-1	Dokumentirajte, ali ima UI varnostno funkcijo	zahteva	razdelek 3.3, R4.1 (poglavje 5)
T8-2	UI vključite v obstoječe postopke za proizvod	zahteva	R4.1
T8-3	Spremljajte delovanje v spremenljivih razmerah	dobra praksa	S-8
O-1	Pripravite vodnika za razvrščanje in za sistem vodenja kakovosti	priporočilo odločevalcem	R4.1 (razdelek 10.2), R4.3 (Priloga A)
O-2	Uskladite razlage nadzornih organov	priporočilo odločevalcem	R4.3 (razdelek 6.4), R4.1 (razdelek 10.2)
O-3	Vzpostavite delujoč regulativni peskovnik	priporočilo odločevalcem	R4.3 (primer 4.2, razdelek 6.4)
O-4	Zagotovite preizkusne nabore v slovenščini in pot do ugotavljanja skladnosti	priporočilo odločevalcem	R4.1 (razdelki 9.3, 9.4 in 10.2), R4.3 (razdelek 6.4)
O-5	Nadgradite enotno informacijsko točko za sisteme UI v javnem sektorju	priporočilo odločevalcem	R4.3 (primer 4.4, Priloga C, razdelek 6.4)
O-6	Ponudite vzorčne dokumente za naročanje in pilotne projekte	priporočilo odločevalcem	R4.3 (primeri 4.5–4.7, razdelek 6.4)
O-7	Zdravstvo: pripravite okvir za zapisovalnike in prepoznavo govora	priporočilo odločevalcem	R4.3 (primer 4.6)
O-8	Izobraževanje: pred uvedbo orodij za učence uredite pravno podlago	priporočilo odločevalcem	R4.3 (primer 4.7)
O-9	Pismenost razumite kot razvoj presoje, ne kot formalno usposabljanje	priporočilo odločevalcem	R4.3 (razdelek 5.4)
O-10	Javne rešitve zasnujte tako, da omogočajo zamenjavo ponudnika	priporočilo odločevalcem	R2.3 (Albert API), R4.3 (primer 4.7), NsUI 2030 [18]

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Oznaka	Priporočilo	Vrsta	Vir
O-11	Okrepite sodelovanje v mednarodnih procesih	priporočilo odločevalcem	poglavje 2, R4.1 (razdelek 10.2)
O-12	Spremljajte izvajanje s kazalniki	priporočilo odločevalcem	R4.3 (razdelek 6.5), NsUI 2030 [18]

Priloga E: Slovar izrazov

Izrazi so povzeti po slovenski različici Akta o UI. Opredelitve so skrajšane; pravno zavezujoče je besedilo uredbe.

Preglednica 19: Izrazi, uporabljeni v poročilu

Izraz	Pomen v poročilu	Akt o UI
sistem UI	Strojni sistem, ki deluje z različno stopnjo samostojnosti in iz vhodnih podatkov sklepa, kako ustvariti izhode, kot so napovedi, vsebine, priporočila ali odločitve.	člen 3(1)
ponudnik	Kdor sistem UI ali model UI za splošne namene razvije ali ga da razviti in ga da na trg ali v uporabo pod svojim imenom ali znamko.	člen 3(3)
uvajalec	Kdor uporablja sistem UI v svoji pristojnosti, razen pri osebni nepoklicni dejavnosti; v naslovu poročila »uporabnik«.	člen 3(4)
dajanje v uporabo	Dobava sistema za prvo uporabo neposredno uvajalcu ali za lastno rabo.	člen 3(11)
predvideni namen	Uporaba, za katero ponudnik namenja sistem, kot jo opišejo navodila, promocijsko gradivo in tehnična dokumentacija.	člen 3(12)
razumno predvidljiva napačna uporaba	Uporaba, ki ni v skladu s predvidenim namenom, a je lahko posledica razumno predvidljivega človeškega vedenja.	člen 3(13)
bistvena sprememba	Nenačrtovana sprememba po dajanju na trg, ki vpliva na skladnost ali spremeni predvideni namen.	člen 3(23)
resni incident	Incident ali okvara sistema UI, ki neposredno ali posredno povzroči smrt ali resno škodo zdravju, resno in nepopravljivo motnjo upravljanja ali delovanja kritične infrastrukture, kršitev obveznosti po pravu Unije, namenjenih varstvu temeljnih pravic, ali resno škodo premoženju ali okolju.	člen 3(49)
sistem za prepoznavanje čustev	Sistem, ki prepoznava ali sklepa o čustvih ali namerah oseb na podlagi njihovih biometričnih podatkov.	člen 3(39)
globoki ponaredek	Z UI ustvarjena ali spremenjena slika, zvok ali video, ki posnema obstoječe osebe, predmete, kraje ali dogodke in bi se lahko komu zdel pristen.	člen 3(60)
model UI za splošne namene	Model, ki je zelo splošen in lahko opravlja širok nabor nalog ter se vključuje v različne sisteme.	člen 3(63)
pismenost na področju UI	Spretnosti, znanje in razumevanje, ki ponudnikom, uvajalcem in osebam, na katere sistem vpliva, omogočajo informirano uvajanje sistemov UI ter zavedanje priložnosti, tveganj in morebitne škode.	člen 3(56)

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Izraz	Pomen v poročilu	Akt o UI
regulativni peskovnik	Nadzorovano okolje pristojnega organa, v katerem se sistemi UI razvijajo in preizkušajo po dogovorjenem načrtu.	člen 3(55)
ocena učinka na temeljne pravice	Ocena, ki jo pred prvo uporabo nekaterih visokotveganih sistemov opravi uvajalec.	27. člen
harmonizirani standard	Evropski standard, sprejet na zahtevo Komisije; objava sklica v UL EU da domnevo o skladnosti.	člen 3(27), 40. člen
agent UI	Sistem UI, ki samostojno načrtuje korake ter uporablja orodja in druge sisteme. Akt o UI ga ne opredeljuje posebej.	–

CRP NOSI-AI (št. V2-24065), ki ga (so)financirata Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost RS (ARIS) in Ministrstvo za digitalno preobrazbo (MDP)

Priloga F: Preslikava mednarodnih okvirov na Akt o UI in priporočila

Preglednica povezuje teme, ki so skupne mednarodnim okvirom, z določbami Akta o UI in s priporočili iz tega poročila. Namenjena je organizacijam, ki želijo z eno ureditvijo pokriti več okvirov (S-12).

Preglednica 20: Mednarodni okviri, Akt o UI in priporočila R5.1

Tema	Mednarodni okviri	Akt o UI	Priporočila R5.1
Človekove pravice, pravičnost, nediskriminacija	OECD (načelo 1.2); UNESCO; Svet Evrope	člena 9 in 10, 27. člen	P-5, U-5, T1-1
Preglednost in razložljivost	OECD (načelo 1.3); UNESCO; Svet Evrope	člena 13 in 50, 86. člen	P-10, P-13, P-14, U-10, T1-4
Robustnost, varnost in zaščita	OECD (načelo 1.4); OWASP	15. člen	P-6, P-8, T4-3
Odgovornost in vloge	OECD (načelo 1.5); smernice OECD o potrebni skrbnosti (korak 1)	člena 16 in 26, 25. člen	S-4, P-1, P-3
Ocena tveganj in vpliva	smernice OECD o potrebni skrbnosti (koraka 2 in 3); HUDERIA; UNESCO EIA	člena 9 in 27	S-2, U-5
Vključevanje deležnikov	smernice OECD o potrebni skrbnosti; HUDERIA	člen 26(7)	U-5, U-6
Spremljanje in obveščanje	smernice OECD o potrebni skrbnosti (koraka 4 in 5); okvir za poročanje po hirošimskem procesu	člena 72 in 73; 21. člen ZIUDHPUI	P-12, U-11, U-13, O-12
Pravna sredstva	smernice OECD o potrebni skrbnosti (korak 6); HUDERIA	člena 85 in 86, člen 27(1)(f)	S-10, U-16
Pismenost in kompetence	UNESCO (izobraževanje); OECD	4. člen	S-5, O-9
Okolje in trajnost	UNESCO (okolje in ekosistemi); OECD (načelo 1.1)	95. člen (prostovoljno)	S-13