Projekt: CRP V2-24065 – NOSI-AI

Rezultat 1.1: Pregled in ocena regulativnega okvira, določenega v Aktu o UI za UI z visoko stopnjo tveganja

Maja Škrjanc, Maruša Škrjanc

Inštitut Jožef Stefan

Datum: 30.3.2025

Kazalo

1 Uvod

Namen poročila

Namen tega poročila je podati praktičen in normativno utemeljen pregled zahtev Uredbe (EU) 2024/1689 o umetni inteligenci (»Akt o UI«, AIA) za sisteme z visoko stopnjo tveganja ter ponuditi jasen, izvedljiv okvir za ocenjevanje skladnosti v praksi. Dokument je namenjen ponudnikom, uvajalcem, proizvajalcem proizvodov z vgrajeno UI, pooblaščenim zastopnikom, uvoznikom in distributerjem ter regulatornim deležnikom. Poudarek je na povezovanju zakonskih zahtev s procesi v organizacijah (upravljanje tveganj, kakovost podatkov, tehnična dokumentacija, vodenje evidenc, človeški nadzor, točnost/robustnost/kibernetska varnost) in na pripravi uporabnih predlog (FRIA – ocena vplivov na temeljne pravice; PIA/DPIA – ocena učinka na varstvo podatkov) ter spremljajočih artefaktov za sledljivost (»artefact passport«). Posebej upoštevamo nacionalni kontekst Republike Slovenije: institucionalne in standardizacijske temelje, obstoječe zmogljivosti nadzora in nadgradnje, potrebne za učinkovito izvajanje AIA na ravni države in organizacij.

Izhodišča in metodologija

Vsebina poročila temelji na uradnem besedilu AIA in njegovih prilogah (zlasti Priloga I, III, IV, VI–VIII), uradnih slovenskih prevodih ter na povezanih aktih EU (varnost proizvodov in CE-okonformnost, Splošna uredba o varstvu podatkov – GDPR, Direktiva (EU) 2022/2555 – NIS2, Akt o digitalnih storitvah – DSA). Uporabljeni so tudi mednarodni standardi in dobre prakse (npr. EN ISO/IEC 23894 – upravljanje tveganj za UI; EN ISO/IEC 23053 – arhitekturne meje in sledljivost; ISO/IEC 5259-1/-3 – kakovost podatkov; ISO/IEC 42001 – sistem vodenja za UI; ISO/IEC TS 8200 – obvladljivost/človeški nadzor; ETSI TS 104 223 – kibernetska varnost AI), saj premoščajo pravne obveznosti v preverljive tehnične zahteve.

Metodološko poročilo sledi trostopenjskemu pristopu: (1) sistematizacija zakonskih zahtev in njihova preslikava v jasne odločilne točke; (2) operativni prevod v procese, kontrolne sezname in dokazila (tehnična dokumentacija, evidence, PMS – spremljanje po dajanju na trg); (3) priprava predlog FRIA/PIA in vzorčnih obrazcev za »artefact passport« ter smernic za presojo skladnosti. Kjer so predvidene smernice Evropske komisije (npr. za klasifikacijo po členih 6–7), je v dokumentu jasno označeno, da bodo ustrezni deli posodobljeni po njihovi objavi.

Normativni okvir in interpretativna načela

Akt o UI je uredba s splošno uporabo in neposrednim učinkom v državah članicah EU. Uporablja se za ponudnike in uvajalce v EU ter za subjekte iz tretjih držav, kadar se izhodi sistema UI uporabljajo v Uniji (ekstrateritorialni doseg). Za sisteme UI, ki so varnostne komponente proizvodov pod harmonizirano zakonodajo EU (Priloga I), se postopki skladnosti po AIA uskladijo s postopki po sektorskih predpisih (npr. MDR/IVDR, stroji, železnice, letalstvo). AIA soobstaja z GDPR, NIS2, DSA in sektorskimi akti; obveznosti se dopolnjujejo.

Pri razlagi uporabljamo načelo sorazmernosti, tveganjsko utemeljen pristop, tehnično nevtralnost in sledljivost odločitev ter sprememb. Za Republiko Slovenijo upoštevamo tudi nacionalni implementacijski okvir: določitev pristojnih organov, nastajajočo vlogo priglašenih organov

(notified bodies) in akreditacije, povezavo z Informacijskim pooblaščencem (IP-RS) in Uradom Vlade RS za informacijsko varnost (URSIV), vlogo Slovenske akreditacije (SA) ter Slovenskega inštituta za standardizacijo (SIST). Nacionalni predlogi so neobvezujoči in pripravljeni kot mehke usmeritve, skladne z razpoložljivimi informacijami in pričakovanimi evropskimi smernicami.

Struktura dokumenta

Uvod (to poglavje) opredeli namen, metodologijo in normativni okvir, z dodatnimi poudarki nacionalnega konteksta RS. Sledi pregled področja uporabe in izključitev; terminologija; klasifikacija visoko tveganih sistemov (vključno s praktičnimi primeri in seznamom potrebnih dokazil); zahteve za visoko tvegane sisteme (členi 8–15 AIA); obveznosti deležnikov v dobavni verigi; standardi, presoja skladnosti, certifikati in registracije; posebni sklopi (npr. biometrija, pregon, testiranje v realnih razmerah); upravljanje in nadzor trga; časovnica in prehodne določbe ter priporočila za implementacijo v Sloveniji, vključno s kontrolnimi seznami, predlogi FRIA/PIA in vzorci »artefact passport«. Vsebinske dopolnitve bodo po potrebi usklajene z nadaljnjimi smernicami Evropske komisije.

2 Področje uporabe in izključitve

To poglavje povzeto in pojasnjeno predstavlja uradno slovensko besedilo Uredbe (EU) 2024/1689 (Akt o umetni inteligenci – AI Akt), *[EUR-Lex, uradni slovenski jezik]*.

2.1 Osebni in teritorialni domet

Člen 2(1) natančno določa, za koga se uredba uporablja. Uredba se uporablja za naslednje skupine zavezancev:

- ponudnike, ki dajejo na trg ali v uporabo sisteme UI ali modele UI za splošne namene v Uniji (ne glede na to, ali imajo sedež v EU ali v tretji državi) – čl. 2(1)(a);
- uvajalce sistemov UI, ki imajo sedež ali se nahajajo v Uniji – čl. 2(1)(b);
- ponudnike in uvajalce s sedežem v tretjih državah, kadar se izhodni podatki sistema UI uporabljajo v Uniji (ekstrateritorialna uporaba) – čl. 2(1)(c);
- uvoznike in distributerje sistemov UI – čl. 2(1)(d);
- proizvajalce proizvodov, ki dajejo sistem UI na trg ali v uporabo skupaj s svojim proizvodom in pod svojim imenom ali znamko – čl. 2(1)(e);
- pooblaščene zastopnike ponudnikov, ki nimajo sedeža v EU – čl. 2(1)(f);
- osebe, ki jih zadeva in se nahajajo v Uniji – čl. 2(1)(g).

Posebno pravilo za visokotvegane sisteme, ki so varnostne komponente proizvodov pod harmonizirano zakonodajo EU, določa člen 2(2): v takih primerih se primarno uporabljajo čl. 6(1), 102–109 in 112 (ter čl. 57, če so zahteve AI Akt vključene v relevantno harmonizacijsko zakonodajo).

2.2 Materialni domet in izključitve

Uredba določa jasne izključitve iz področja uporabe (čl. 2(3) do (12)):

- Področja izven prava Unije in nacionalna varnost: uredba se ne uporablja za področja izven prava EU in ne posega v pristojnosti držav članic glede nacionalne varnosti. Prav tako se ne uporablja za sisteme UI, ki so dani na trg, v uporabo ali se uporabljajo izključno za vojaške, obrambne ali nacionalnovarnostne namene; enako velja, če se izhodni podatki sicer uporabijo v Uniji, vendar izključno za navedene namene – čl. 2(3) in 2(4).
- Mednarodno sodelovanje organov pregona in pravosodja: uredba se ne uporablja za javne organe tretjih držav ali mednarodne organizacije, kadar uporabljajo UI v okviru sporazumov z EU/državami članicami na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodnega sodelovanja, pod pogojem ustreznih zaščitnih ukrepov – čl. 2(5).
- Odgovornost posredniških storitev: uredba ne posega v poglavje II Uredbe (EU) 2022/2065 (DSA) – čl. 2(6).
- Sistemi ali modeli UI posebej razviti in dani v uporabo zgolj za namene znanstvenih raziskav in razvoja: izvzeti iz področja uporabe – čl. 2(7).

- Raziskave, testiranje in razvoj pred dajanjem na trg ali v uporabo: ti R&D postopki so izvzeti, vendar morajo biti skladni z veljavnim pravom EU; izjema: ‘testiranje v realnih razmerah’ ni izvzeto – čl. 2(8).
- Uredba ne posega v pravila EU o varstvu potrošnikov in varnosti proizvodov – čl. 2(9).
- Fizične osebe kot uvajalci pri povsem osebni, nepoklicni uporabi: izvzete iz obveznosti uvajalcev – čl. 2(10).
- Ne posega v nacionalne/eu ukrepe, ki za delavce zagotavljajo ugodnejše varstvo pri delodajalčevi uporabi UI – čl. 2(11).
- Odprtokodno objavljeni sistemi UI: objava pod prostimi in odprtokodnimi licencami je izvzeta, razen če je tak sistem dan na trg ali v uporabo kot visokotvegan, ali pa gre za sistem iz člena 5 (prepovedane prakse) ali člena 50 (transparentnostne obveznosti) – čl. 2(12).

2.3 Razlaga in praktične posledice

- Ekstrateritorialnost (čl. 2(1)(c)): če se izhod sistema UI uporablja v EU, se obveznosti lahko uporabijo tudi za subjekte izven EU. To je pomembno za globalne ponudnike in uvajalce, ki ciljajo na uporabnike ali postopke v EU.
- R&D in testiranje (čl. 2(7) in 2(8)): raziskave in razvoj pred trgom sta na splošno izvzeta, vendar ‘testiranje v realnih razmerah’ ni. Za realne preizkuse veljajo posebna pravila (glej čl. 60 in povezana poglavja poročila).
- Osebna nepoklicna uporaba (čl. 2(10)): posamezniki, ki uporabljajo UI povsem zasebno, niso uvajalci v smislu obveznosti AI Akt, vendar ostala pravila (npr. varstvo podatkov, potrošniška zakonodaja) lahko še vedno veljajo glede na okoliščine.
- Odprta koda (čl. 2(12)): sama objava odprtokodnega modela ali sistema UI ne sproži obveznosti, razen če se sistem ponudi kot visokotvegan ali kot sistem iz čl. 5 ali 50. Če se odprtokodni sistem integrira v proizvod/storitev, ki se daje na trg v EU, se pravila lahko začnejo uporabljati za operaterje take rešitve.
- Varnostne komponente pod harmonizirano zakonodajo (čl. 2(2)): kadar je UI varnostna komponenta proizvoda, veljajo posebne napotitve na oddelek o postopkih ugotavljanja skladnosti v povezani harmonizacijski zakonodaji in določbah AI Akt.

2.4 Povzetek: področje uporabe in izključitve (AI Act, čl. 2)

Vidik	Ključna pravila	Pravna podlaga (člen)
Osebni/teritorialni domet	Ponudniki, uvajalci (tudi izven EU, če so izhodi uporabljeni v EU), uvozniki, distributerji, proizvajalci (z UI), pooblaščeni zastopniki, osebe v EU	čl. 2(1)
Varnostne komponente pod harmon. zakonodajo	Poseben režim napotuje na čl. 6(1), 102–109, 112 (+57 po pogojih)	čl. 2(2)

Nacionalna varnost/obramba	Izključitev (vključno z izhodom, če se uporablja izključno za vojaške itd.)	čl. 2(3)–(4)
Mednarodno sodelovanje na področju pregona/pravosodja	Izključitev pod pogoji zaščitnih ukrepov	čl. 2(5)
DSA posredniške storitve	Ne posega v določbe odgovornosti posrednikov	čl. 2(6)
R&R zgolj za znanstvene namene	Sistemi ali modeli UI zgolj za raziskave in razvoj so izvzeti	čl. 2(7)
R&D pred trgom/testiranje	Raziskave/testiranje pred trgom izvzeti; 'testiranje v realnih razmerah' NI izvzeto	čl. 2(8)
Varstvo potrošnikov in varnost proizvodov	AI Act ne posega v ta pravila EU	čl. 2(9)
Osebna nepoklicna uporaba	Fizične osebe kot uvajalci pri povsem osebni rabi – izvzete	čl. 2(10)
Delovno pravo	Ne posega v ugodnejše ureditve za delavce	čl. 2(11)
Odprtokodna objava	Objava pod prostimi/odprtokodnimi licencami izvzeta, z izjemami (HR, čl. 5, čl. 50)	čl. 2(12)

3 Terminologija

V tem poglavju povzemamo ključne pojme iz Uredbe (EU) 2024/1689 o umetni inteligenci (»AI akt«) in uradnega slovenskega prevoda. Opisi so zgoščeni povzetki uradnih definicij (člen 3, razen pismenosti iz člena 4) in so namenjeni dosledni rabi izrazov v tem poročilu.

Sistem umetne inteligence (sistem UI) – čl. 3(1):

Strojno zasnovan sistem, zasnovan za delovanje z različnimi stopnjami avtonomije, ki lahko po uvedbi izkazuje prilagodljivost in z uporabo inferenčnih tehnik obdeluje vhodne podatke ter za dosego ciljev, določenih s strani človeka, ustvarja izhode (npr. napovedi, vsebine, priporočila ali odločitve), ki lahko vplivajo na fizična ali virtualna okolja.

Tveganje (v kontekstu AI akta):

Kombinacija verjetnosti in resnosti škodljivih posledic za zdravje, varnost ali temeljne pravice posameznikov (ter, kjer je ustrezno, za okolje, demokratične procese ali pravno varnost), ki lahko izhajajo iz zasnove, razvoja, uvedbe ali uporabe sistema UI.

Ponudnik – čl. 3(3):

Fizična ali pravna oseba, javni organ, agencija ali drug subjekt, ki razvije sistem UI ali ga da na trg ali v uporabo pod svojim imenom ali blagovno znamko, ne glede na to, ali je sistem razvil sam ali je bil razvit s strani tretje osebe.

Opombe za uporabo v poročilu: Ponudnik je primarni nosilec obveznosti skladnosti (čl. 8–15) ter postopkov ugotavljanja skladnosti in registracije (čl. 49, 51, 60).

Uvajalec – čl. 3(4):

Fizična ali pravna oseba, javni organ, agencija ali drug subjekt, ki v okviru svoje poklicne dejavnosti uporablja sistem UI. Uvajalec ne postane ponudnik, če sistem uporablja brez sprememb namena in pod enakimi pogoji, kot jih je določil ponudnik.

Opombe za uporabo v poročilu: Uvajalci imajo obveznosti glede uporabe sistemov UI v skladu z navodili, človeškega nadzora, vodenja evidenc in poročanja o resnih incidentih (npr. čl. 29–31).

Pooblaščeni zastopnik – čl. 3(7):

Fizična ali pravna oseba s sedežem v Uniji, ki jo pisno pooblasti ponudnik s sedežem zunaj Unije za opravljanje določenih nalog v njegovem imenu v zvezi z obveznostmi po AI aktu.

Opombe za uporabo v poročilu: V praksi skrbi za komunikacijo z nadzornimi organi, hranjenje tehnične dokumentacije in sodelovanje pri nadzoru trga (čl. 61 in nasl.).

Uvoznik – čl. 3(6):

Fizična ali pravna oseba s sedežem v Uniji, ki da na trg Unije sistem UI iz tretje države.

Opombe za uporabo v poročilu: Uvoznik preveri, ali je ponudnik izvedel ustrezen postopek ugotavljanja skladnosti, ali je sistem opremljen z zahtevano dokumentacijo, oznakami in navodili (čl. 26).

Distributer – čl. 3(5):

Fizična ali pravna oseba v dobavni verigi, razen ponudnika ali uvoznika, ki daje sistem UI na voljo na trgu do trenutka njegovega dajanja v uporabo.

Opombe za uporabo v poročilu: Distributer preveri, ali sistem nosi zahtevane oznake in spremljajočo dokumentacijo ter ali je bil skladiščen/transportiran tako, da skladnost ni ogrožena (čl. 27).

Operater – čl. 3(2):

Krovni pojem, ki zajema vse subjekte v dobavni in vrednostni verigi sistema UI, vključno s ponudniki, uvajalci, uvozniki, distributerji in pooblaščenimi zastopniki (ter, kjer je ustrezno, proizvajalci proizvodov, ki na trg dajejo proizvode z vgrajenimi sistemi UI pod svojim imenom).

Opombe za uporabo v poročilu: V poročilu izraz »operater« uporabljamo, kadar se obveznost ali odgovornost nanaša na več vlog hkrati in je natančna razmejitev določena v posameznem členu AI akta.

Pismenost na področju UI – čl. 4

Stopnja znanja, spretnosti in razumevanja, potrebnih za učinkovito in odgovorno interakcijo s sistemi UI. AI akt zahteva, da ponudniki in uvajalci sprejmejo ukrepe za zagotavljanje ustrezne pismenosti osebja, ki sodeluje pri zasnovi, razvoju, uvedbi ali uporabi sistemov UI; države članice in Komisija pa spodbujajo širšo pismenost v družbi.

Opombe za uporabo v poročilu: V praksi to pomeni usposabljanja o omejitvah, tveganjih, človeškem nadzoru, razlagi metrik (točnost, robustnost), zasebnosti in obvladovanju incidentov.

4 Klasifikacija: kdaj je sistem 'visokotvegan' (čl. 6–7)

To poglavje pojasnjuje logiko razvrščanja sistemov umetne inteligence (UI) med visoko tvegane po Aktu o UI (AUI). Zasnovano je tako, da najprej predstavimo obe poti (A in B), nato možnost utemeljitve, da sistem iz Priloge III ni visoko tvegan, časovnico obveznosti ter praktičen povzetek v obliki odločitvenega drevesa. V zaključku poglavja podamo pregled priporočene dokumentacije in tipičnih robnih situacij z razumljivimi primeri iz prakse.

4.1 Pregled logike klasifikacije

Akt o UI določa dva načina (»poti«), po katerih je sistem UI visoko tvegan:
• Pot A (čl. 6(1)): sistem UI je varnostna komponenta proizvoda, ki sodi pod enega izmed sektorskih predpisov EU iz Priloge I (npr. medicinski pripomočki, stroji, dvigala, železnice, letalstvo ipd.), in je za ta proizvod predpisana tretjeosebna ocena skladnosti pred dajanjem na trg.
• Pot B (čl. 6(2)): sistem UI spada v enega od primerov uporabe, navedenih v Prilogi III (npr. biometrija, kritična infrastruktura, izobraževanje, delo, bistvene storitve, pregon, migracije/meje/azil, pravosodje/demokratični procesi).

4.2 Pot A – Priloga I (varnostna komponenta v proizvodu pod harmonizirano zakonodajo)

Pot A se uporabi, kadar je UI varnostna komponenta proizvoda, ki je reguliran po enem izmed harmonizacijskih predpisov EU (Priloga I), in je zanj potrebna tretjeosebna presoja. Primeri predpisov iz Priloge I (neizčrpno):

• Uredba (EU) 2017/745 (medicinski pripomočki); Uredba (EU) 2017/746 (in-vitro diagnostika)
• Uredba (EU) 2023/1230 (stroji)
• Direktiva 2014/33/EU (dvigala); Direktiva 2014/35/EU (nizkonapetostna oprema); Direktiva 2014/53/EU (radijska oprema)
• Uredba (EU) 2018/1139 (civilno letalstvo); Direktiva (EU) 2016/797 (interoperabilnost železnic)

Praktično: če UI skrbi za varno ustavljanje kolaborativnega robota v stroju, ki zahteva tretjeosebno oceno, je tak UI visoko tvegan (pot A) – uporabijo se zahteve poglavja III AUI (upravljanje tveganj, podatki, dokumentacija, človeški nadzor, robustnost, kibernetska varnost, CE-označevanje).

4.3 Pot B – Priloga III (primeri uporabe)

Pot B se uporabi, kadar UI sodi v eno od kategorij iz Priloge III, ne glede na to, ali je del proizvoda iz Priloge I.

Kategorije (povzetek):

1) Biometrija: oddaljena biometrična identifikacija (real-time ali ex post), biometrična kategorizacija po občutljivih atributih, prepoznavanje čustev.
2) Kritična infrastruktura: UI kot varnostne komponente v upravljanju kritične digitalne infrastrukture, prometa, energentov, vode.
3) Izobraževanje/usposabljanje: dostop/sprejem, ocenjevanje, razvrščanje, nadzor izpitov.
4) Zaposlovanje/HR: rekrutiranje, selekcija, ocenjevanje kandidatov, odločanje o pogojih dela, napredovanjih, dodeljevanju nalog; spremljanje uspešnosti.
5) Bistvene storitve in prejemki: odločanje o upravičenosti do javnih storitev/pomoči; kreditna sposobnost/ocenjevanje fizičnih oseb (z izjemo sistemov zgolj za zaznavanje goljufij).
6–8) Pregon; migracije/meje/azil; pravosodje in demokratični procesi: različne uporabe UI, kadar jih uporabljajo pristojni organi v navedenih kontekstih.

4.4 Možnost utemeljene ocene, da sistem iz Priloge III ni »visokotvegan«

Ponudnik lahko – v izjemnih, jasno utemeljenih okoliščinah – pokaže, da konkretni sistem iz Priloge III v predvidenem kontekstu uporabe ne povzroča znatnega tveganja za zdravje, varnost ali temeljne pravice, zato naj se ne obravnava kot »visoko tvegan«. Ta možnost je »izpodbojna« (organ jo lahko zavrne) in zahteva: (1) podrobno utemeljitev na podlagi ocene tveganj in vplivov na temeljne pravice (FRIA); (2) popolno tehnično dokumentacijo; (3) registracijo v evidenci EU in obvestilo pristojnemu organu; (4) okrepljen post-market nadzor.

Organ nadzora trga lahko utemeljitev preveri in odločitev spremeni: sistem se nato obravnava kot visoko tvegan, z vsemi obveznostmi poglavja III.

4.5 Časovnica (ključni mejniki)

- 1. 8. 2024: začetek veljavnosti AUI.
- 2. 8. 2026: splošna uporaba večine določb (2 leti po veljavnosti).
- do 2. 2. 2026: smernice Komisije za klasifikacijo (čl. 6–7).
- 2. 8. 2027: začetek uporabe obveznosti za visoko-tvegane sisteme (poglavje III).

4.6 Odločitveno drevo za klasifikacijo (povzetek)

1) Je UI varnostna komponenta proizvoda iz Priloge I in je za ta proizvod predpisana tretjeosebna presoja skladnosti?
   → DA: visoko tvegan (pot A) – uporabite režim poglavja III.
   → NE: nadaljujte.
2) Spada UI v katerokoli kategorijo iz Priloge III?
   → DA: visoko tvegan (pot B), razen če je utemeljeno dokazano, da tveganja niso znatna (glej

4.4) in je izvedena obvezna registracija.
→ NE: sistem ni visoko tvegan po čl. 6–7 (lahko pa veljajo druge obveznosti AUI).

4.7 Dokumentacija in dokazila: kaj pripraviti (nad minimumom) – razširjeno, poljudno

Spodnji seznam je praktičen kontrolni seznam za ekipe v podjetjih in javnem sektorju. Namen je, da ob presoji klasifikacije hitro pokažete »na papirju«, zakaj ste se odločili tako in kako tveganja obvladujete.

A) Kratek povzetek klasifikacije (1–2 strani):

• Opis namena sistema in konteksta uporabe (kdo, kdaj, za kaj).
• Sklic na pot A ali B (ustrezna točka Priloge I/III) – ali pojasnilo, da ne sodi v nobeno.
• Če uveljavljate izjemo »ni visoko tvegan« za sistem iz Priloge III: kratka obrazložitev, zakaj tveganja niso znatna, ter seznam varoval (npr. človeški pregled, omejen obseg, omejeni podatki).

B) Tehnična dokumentacija (osnovni paket):

• Opis arhitekture in meja sistema (komponente, podatkovni tokovi, odločitvene točke; lahko po vzoru EN ISO/IEC 23053).
• Opis podatkov (izvor, kakovost, uravnoteženost, postopki čiščenja, metapodatki; sklic na ISO/IEC 5259-1/-3).
• Rezultati testov (točnost, robustnost, pristranskosti po podskupinah, kibernetska varnost – npr. osnovni evasion/poisoning testi po ETSI TS 104 223).
• Človeški nadzor/obvladljivost (vloge, pravila za »override«/»safe-stop«, pragovi zaupanja; po ISO/IEC TS 8200).

C) Upravljanje tveganj in temeljne pravice:

• Register tveganj po ISO/IEC 23894 (verjetnost × vpliv, mitigacije, odgovorne osebe, pragi »go/no-go«).
• FRIA (ocena vplivov na temeljne pravice): kdo je lahko prizadet, kakšne so možne škode, kako jih blažite.
• Če gre za osebne podatke: PIA/DPIA (po IEEE 7002 oz. GDPR praksi) ter dokazila o minimizaciji in zakonitosti obdelave.

D) Sledljivost in evidence:

• »Artefact passport«: povezave med modelom, verzijo podatkov, konfiguracijo in testi; podpis/odobritev pred uvedbo.
• Dnevniki odločitev (kdo je odobril uvedbo, na podlagi česa) in sprememb (change control z razlogi in rezultati regresijskih testov).

• PMS (post-market) načrt: kaj spremljamo (drift, incidenti, pritožbe), kako hitro ukrepamo (MTTR), kdaj izvedemo retrening ali rollback.

E) Komunikacija in preglednost (za uporabnike in nadzorne organe):

• »Transparency profile« (po IEEE 7001): namen, omejitve, znane napake, razlage metrik, kontakt za pomoč/pritožbe.
• Navodila za varno uporabo (kaj sistem zna in česa ne sme nadomestiti; kdaj je obvezen človeški pregled).

4.8 Primeri robnih situacij (z razlago za nepoznavalce)

Primer 1: Biometrija – verifikacija vs. identifikacija

• Verifikacija: sistem preverja, ali ste res vi (1-na-1 ujemanje, npr. odklep z obrazom na telefonu). To praviloma NE pade v točko o oddaljeni biometrični identifikaciji v Prilogi III.

• Identifikacija: sistem išče ujemanje med vašo sliko in večjo bazo ljudi (1-na-N). To JE vključeno v Prilogo III (visoko tveganje).

Zakaj razlika? Pri identifikaciji so tveganja za napačne zadetke, sta sledenje in poseg v zasebnost bistveno večja. Če vaš sistem dela le verifikacijo, vseeno preverite: ali mogoče počne še kaj drugega (npr. čustva ali kategorizacijo po občutljivih lastnostih)? Če da, lahko spadete v druge točke Priloge III.

Primer 2: Kreditna ocena vs. odkrivanje goljufij

• Kreditna ocena (scoring) fizičnih oseb je izrecno v Prilogi III → visoko tveganje.
• Odkrivanje finančnih goljufij je iz te točke izvzeto (ni avtomatsko visoko tveganje). Vendar lahko še zmeraj pridejo v poštev druge obveznosti (npr. preglednost, varnost, zasebnost) – in če tak sistem vpliva na pravice posameznika (npr. avtomatska blokada), tveganja ponovno ocenite.

Primer 3: Kritična infrastruktura – proizvod izven Priloge I, a uporaba po Prilogi III

Tudi če UI ni varnostna komponenta proizvoda, ki je izrecno pod Prilogo I, je lahko visoko tvegan po Prilogi III(2), če dejansko opravlja varnostno funkcijo v upravljanju kritične infrastrukture (npr. energetska omrežja, oskrba z vodo). Osredotočite se na dejanski vpliv v okolju rabe.

Primer 4: »Peskovnik« ali pilot z močno omejitvijo tveganj – možnost utemeljitve »ni visoko tvegan«

Če sistem spada v Prilogo III, pa ga preizkujete v zelo omejenem okolju: majhna skupina uporabnikov, človeški pregled vseh odločitev, nobenih trajnih posledic za pravice ljudi, takojšnja zaustavitev ob odstopanjih ipd. – lahko poskusite z utemeljitvijo, da tveganja niso znatna. Pazite:

dokazno breme je na vas, utemeljitev mora biti natančna, sistem morate registrirati in organ lahko kljub temu zahteva poln režim HR.

Primer 5: Orodja za pomoč zaposlenim (npr. priporočila nalog) vs. avtomatizirane odločitve o zaposlitvi

Priporočilni pomočniki (asistenti), ki ne sprejemajo avtomatiziranih odločitev o zaposlitvi, napredovanju ali odpustih in delujejo pod stalnim človeškim nadzorom, bodo lahko izven HR (odvisno od funkcij). Kadar pa UI filtrira prijave, razvršča kandidate, dodeljuje naloge ali ocenjuje uspešnost in ima učinke na pravice delavcev, gre praviloma za HR po Prilogi III(4).

Primer 6: Ocene znanja študentov – sprotna pomoč vs. odločanje o napredovanju

Sistemi, ki zgolj usmerjajo učenje ali nudijo povratno informacijo študentu, so lahko izven HR. Ko pa UI sodeluje pri odločanju o sprejemu, razvrstitvi, napredovanju ali končni oceni, spada v Prilogo III(3) → visoko tveganje.

5 Zahteve za visokotvegane sisteme UI (čl. 8–15)

5.1 Sistem za obvladovanje tveganja (čl. 9)

Člen 9 zahteva, da je upravljanje tveganj za visoko-tvegane sisteme UI kontinuiran, iterativen in dokumentiran proces, ki poteka skozi celoten življenjski cikel sistema – od zasnove do umika iz uporabe. Proces mora vključevati opredelitev konteksta, identifikacijo in ocenjevanje tveganj (tudi za ranljive skupine), načrtovanje in izvajanje omilitvenih ukrepov, preverjanje učinkovitosti ter redne ponovne ocene ob spremembah modela, podatkov ali operativnega okolja.

- Merila sprejemljivosti: vnaprej določeni pragovi (kvantitativni in kvalitativni), vključno z metrikami po podskupinah uporabnikov.
- Testiranje na vnaprej določene metrike/prage: robustnostni testi, 'worst-case' scenariji in validacije po podskupinah.
- Posebna pozornost ranljivim skupinam in kontekstom z velikim vplivom na temeljne pravice.

Priporočeni artefakti/dokazila: register tveganj, matrika odločitev in razlogov, načrt mitigacij, poročila o testih, zapisniki odobritev ('release gates').

Povezava na standarde (priporočeno)

- EN ISO/IEC 23894 – metodika upravljanja tveganj za UI (proces).
- EN ISO/IEC 23053 – arhitekturne meje, kontrolne točke in sledljivost artefaktov.
- ISO/IEC 42001 – AIMS (QMS) za vgradnjo RMF v organizacijske procese.
- ETSI TS 104 223 – varnostne kontrole in preskusi, povezani z art. 15.
- IEEE 7003 – obravnava pristranskosti v RMF, IEEE 7002 – PIA v kontekstu čl. 10.

ID tveganja	Opis in prizadete skupine	Metrika/prag	Mitigacija	Status / dokazilo
R-HR-001	Pristranskost pri odločitvah; vpliv na ranljive skupine	ΔTPR ≤ 3 p.p. med skupinami	Pre-processing rebalans + človeški pregled	Validacijsko poročilo v repozitoriju #842

5.2 Podatki in upravljanje podatkov (čl. 10)

Člen 10 zahteva, da so podatki, uporabljeni za učenje, validacijo in testiranje, ustrezni, reprezentativni, brez zavedne pristranskosti in kakovostno dokumentirani. Potrebna je sledljivost

izvora, transformacij in pogojev uporabe. Za sisteme brez učenja ('no-learning' sistemi) se zahteve preslikajo v strožje zahteve za testne nabori in scenarije uporabe.

- Kakovost in reprezentativnost: merjenje po ISO/IEC 5259-1; segmentno (po podskupinah) za HR kontekste.
- Upravljanje kakovosti: procesne zahteve po ISO/IEC 5259-3 (vloge, kontrole, evidence).
- Dokumentiranje izvora in priprave: datasheeti, 'data lineage', licenčni in pravni status, PIA/DPIA evidenca (IEEE 7002).
- Sistemi brez učenja: razširjena testna baterija, ki pokrije realistične in 'worst-case' vhode; pragi za 'go/no-go'.

Priporočeni artefakti/dokazila

- Datasheet za vsak dataset (izvor, pokritost, znane pristranskosti, licence).
- Evidence transformacij ('lineage') in različic; povezava na modele (EN ISO/IEC 23053).
- Poročila o kakovosti po 5259-1 ter načrti kakovosti po 5259-3.
- PIA/DPIA – obrazci, ocene in sprejete mitigacije (IEEE 7002).

5.3 Tehnična dokumentacija (čl. 11, Priloga IV)

Tehnična dokumentacija mora biti pripravljena pred dajanjem na trg ali v uporabo in mora dokazovati skladnost z zahtevami čl. 8–15. Priloga IV določa minimalno vsebino: opis sistema in namena, arhitekturo in meje, vire podatkov, metode učenja in validacije, merila uspešnosti, ukrepe človeškega nadzora, varnostne in robustnostne kontrole, PMS ter navodila za uporabo (IFU). Za MSP je predviden poenostavljen obrazec (po objavi Komisije).

Kontrolni seznam (izvleček Priloge IV)

- Opis namena in področja uporabe; meje sistema in kontekst.
- Arhitektura (EN ISO/IEC 23053) in sledljivost model–dataset–konfiguracija–test.
- Upravljanje podatkov (čl. 10): kakovost, poreklo, licence, PIA/DPIA.
- Upravljanje tveganj (čl. 9): register, pragovi, poročila o testih.
- Človeški nadzor (čl. 14) in obvladljivost (TS 8200): vloge, 'override', 'safe-stop'.
- Točnost, robustnost, kibernetska varnost (čl. 15): metrike, pragi, testi; ETSI TS 104 223.
- PMS: načrt nadzora po dajanju na trg, kazalniki, incidenti, CAPA.

5.4 Vodenje evidenc (čl. 12)

Sistem mora omogočati samodejno beleženje relevantnih dogodkov in parametrov, ki so potrebni za razumevanje, spremljanje in revidiranje obratovanja ter za post-market spremljanje (PMS). Obseg in granularnost dnevniških zapisov morata biti sorazmerna tveganjem in vplivu sistema.

Minimalne evidence (primer)

Kategorija zapisa	Vsebina (primer)	Hramba
Inferenčni klici	Čas, ID modela/konfiguracije, vhodni tip, zaupanje/negotovost, odločitev	≥ 1 leto (primer)
Spremembe modelov	Verzija, podpis/izvor, odobritev, razlog, rezultati testov	Življenjski cikel + 1 leto
Dogodki PMS	Incidenti, alarmi, override/safe-stop, CAPA reference	≥ 1 leto
Dostopi	Kdo, kdaj, kaj (model, podatki); uspeh/neuspeh	≥ 6 mesecev
BIOMETRIJA – realni čas*	Čas, referenčna baza, uporabljeni vhodi/senzorji, identiteta preverjevalcev	po predpisih/sektorsko

*Za biometrijo v realnem času se uporabljajo strožji režimi vodenja dnevnikov, z dodatnimi kontrolami dostopa in sledljivostjo uporabe referenčnih baz.

5.5 Preglednost in informacije uvajalcem (čl. 13)

Ponudnik mora zagotoviti jasna in popolna navodila za uporabo (IFU), ki uvajalcu omogočajo varno in pravilno uporabo sistema. IFU morajo vsebovati omejitve, predpostavke, zahteve glede vhodov in okolja, ravni točnosti/robustnosti/kibernetske varnosti, pogoje človeškega nadzora, postopke vzdrževanja in PMS.

IFU – obvezne vsebine (primer predloge)

Namen in meje	Opis predvidene rabe, izključitve in omejitve konteksta.
Vhodi in kvaliteta	Specifikacije vhodnih podatkov/senzorjev; minimalne zahteve kakovosti.
Zmogljivosti/metrike	Dosežene metrike (tudi po podskupinah); negotovosti; pragi sprejemljivosti.
Robustnost/kibernetska varnost	Preskusi, znane omejitve, pričakovani scenariji napadov in obramba.
Človeški nadzor	Kdo, kdaj in kako lahko poseže; ‘override’, ‘safe-stop’, pragi za eskalacijo.
Vzdrževanje/posodobitve	Politike sprememb, zahteve za reteste, način obveščanja uporabnikov.
PMS in incidenti	Kako poročati incidente; kazalniki; kontaktne točke.
Skladnost in reference	Sklici na čl. 8–15, standarde in izvedene kontrole.

5.6 Človeški nadzor (čl. 14)

• Zasnova in organizacijski ukrepi; zmanjšanje automation bias; možnost neuporabe izhoda in varne zaustavitve. [dopolnite]

Sistem mora biti zasnovan in organiziran tako, da usposobljene osebe lahko učinkovito nadzirajo delovanje UI, prepoznajo tveganja, zmanjšujejo 'automation bias' in po potrebi ne uporabijo ali preglasijo izhoda sistema ter varno zaustavijo delovanje.

- Organizacijski ukrepi: vloge in odgovornosti, usposabljanja, 'drills' za override/safe-stop; merjenje MTTR in uspešnosti posegov.
- Ergonomija vmesnikov: jasno prikazane negotovosti, opozorila in status modela; preprečevanje kognitivne preobremenitve operaterjev.
- Pravila eskalacij: pragovi, pri katerih je obvezen človeški pregled ali zaustavitev; dokumentirani postopki.

Standardi in dobra praksa

- ISO/IEC TS 8200 – obvladljivost avtomatiziranih AI sistemov (override, safe-stop, testni scenariji).
- IEEE 7001 – informacije za operaterje/revizorje; sledenje odločitev.
- EN ISO/IEC 23053 – označitev točk človeškega nadzora v arhitekturi.

5.7 Točnost, robustnost in kibernetska varnost (čl. 15)

Sistemi morajo dosegati ustrezne ravni točnosti, robustnosti in kibernetske varnosti skozi celoten življenjski cikel. Metrike in pragovi morajo biti navedeni v navodilih za uporabo (IFU) ter potrjeni v testnih poročilih. Organizacije morajo upravljati povratne zanke pristranskosti (feedback loops) in degradacije metrik ter izvajati PMS.

- Točnost: jasne definicije metrik in sprejemljivih pragov, tudi po podskupinah; sledljivost do podatkov in konfiguracij.
- Robustnost: preskusi odpornosti na motnje, drift in 'adversarial' scenarije; 'worst-case' testiranje.
- Kibernetska varnost: zaščita modelov, podatkov in pipeline; SBoM, integriteta, kontrola dostopov, monitoring anomalij.
- Povratne zanke pristranskosti: spremljanje, alarmi in korektivni ukrepi ob zaznanih odmikih.

Povezave na standarde in preskuse

- ETSI TS 104 223 – osnovne varnostne zahteve in preskusi za AI modele/sisteme.
- ETSI TS 104 050 – ontologija groženj; enotno označevanje testov in incidentov.
- EN ISO/IEC 23894 – RMF za določanje pragov in ponovne ocene.
- EN ISO/IEC 23053 – sledljivost artefaktov in kontrolne točke.

- ISO/IEC 5259-1/-3 – podatkovna kakovost kot predpogoj točnosti/robustnosti.
- IEEE 7003 – spremljanje pravičnosti; IEEE 7002 – zasebnost podatkov.

6 Obveznosti deležnikov

To poglavje povzema obveznosti ključnih deležnikov pri sistemih umetne inteligence, pri čemer je posebno poudarjena skladnost za visokotvegane (HR) sisteme po Uredbi o umetni inteligenci (AI Act). Povzetek je pripravljen za praktično uporabo v organizacijah v Sloveniji in je usklajen z logiko novega zakonodajnega okvira EU.

6.1 Ponudniki (providers) – nosilci skladnosti za HR-sisteme

- Vzpostavijo in ohranjajo sistem za upravljanje umetne inteligence (QMS/AIMS): politike, vloge, notranje presoje in CAPA; upravljanje sprememb verzij modelov in podatkov.
- Izvedejo sistematično upravljanje tveganj čez življenjski cikel (iterativni RMF): kontekst, identifikacija, ocena, ublažitve, spremljanje in evidenca odločitev.
- Zagotavljajo upravljanje podatkov (kakovost, reprezentativnost, pristranskosti): dokumentirajo izvor, pripravo in pravne podlage; za sisteme brez učenja – zahteve na validacijskih/testnih naborih.
- Pripravijo tehnično dokumentacijo (pred dajanjem na trg): arhitektura, meje sistema, podatkovni tokovi, konfiguracije, modeli, testi, nadzor in PMS; izjava EU o skladnosti.
- Omogočijo vodenje evidenc (logiranje): samodejno beleženje relevantnih dogodkov, metrik in odločitev za podporo PMS in preiskavam incidentov.
- Zagotavljajo preglednost in informacije za uvajalce (IFU): namen/uporaba, omejitve, ravni točnosti/robustnosti/kibernetske varnosti, zahteve za vhodne podatke, človeški nadzor, vzdrževanje in posodobitve.
- Vključijo učinkovite ukrepe človeškega nadzora: možnost neuporabe izhoda AI, ročni ‘override’ in varna zaustavitev (safe-stop); usposabljanje operaterjev.
- Dosežejo ustrezne ravni točnosti/robustnosti/kibernetske varnosti: določijo metrike in prage, načrtujejo preskuse (tudi ‘worst case’) in nadzor zank pristranskosti.
- Izvedejo postopke ugotavljanja skladnosti (conformity assessment) za HR-sisteme; pred dajanjem na trg registrirajo sistem v ustrezno EU bazo, kjer je to predpisano; namestijo oznako CE, kadar je to zahtevano.
- Vzpostavijo post-market monitoring (PMS): spremljanje delovanja, incidentov, degradacij metrik, drift-a podatkov; mehanizmi za korektivne ukrepe, retrening in rollback.
- Resne incidente in disfunkcije prijavijo pristojnim organom ter sodelujejo z nadzornimi organi; vodijo in hranijo evidence (običajno najmanj 10 let).
- Če tretjim osebam dajo na voljo generativne ali temeljne modele za integracijo, zagotovijo ustrezna navodila, varnostne informacije, licence in omejitve uporabe; jasno določijo odgovornosti v pogodbah.

6.2 Uvajalci (deployers/operaterji) – odgovorna raba in nadzor

- Uporabljajo sistem v skladu z navodili proizvajalca/ponudnika (IFU) ter vnaprej določenimi postopki in pragi.
- Zagotavljajo ustreznost in kakovost vhodnih podatkov v realni rabi; vzpostavijo nadzor vhodov za preprečevanje zlorab (npr. ‘prompt injection’).

- Imenujejo odgovorne osebe/operaterje, ki so usposobljeni za človeški nadzor; izvajajo ročni ‘override’ in eskalacije, ko je to potrebno.
- Vodijo dnevnike uporabe in odločitev ter hranijo evidence, potrebne za PMS in presojo; ob resnih incidentih takoj obvestijo ponudnika in pristojne organe po veljavnih pravilih.
- Izvedejo oceno vplivov na temeljne pravice (FRIA) in/ali PIA, kadar je to zahtevano: opredelijo prizadete skupine, tveganja in ublažitve; zabeležijo rezultate in odločitve.
- Skrbijo za redno preverjanje delovanja v svojem kontekstu (»operational validation«) in spremljanje zavajajočih vhodov ali degradacije metrik; izvajajo korektivne ukrepe ali začasno izključitev AI, ko pragi niso doseženi.
- Če uvajalec spremeni namen ali bistveno spremeni sistem (npr. retrening z novimi podatki, sprememba arhitekture), lahko pridobi vlogo ponudnika in prevzame povezane obveznosti za skladnost.

6.3 Uvozniki – preverjanje skladnosti pred dostopom na trg EU

- Preverijo, da je sistem označen z CE (kjer je zahtevano), ima EU izjavo o skladnosti, tehnično dokumentacijo in registracijo v EU bazi (za HR-sisteme, kjer je predpisana).
- Na izdelku/embalaži zagotovijo svoje ime, registriran trgovski naziv ali registrirano blagovno znamko ter naslovi za stik v EU.
- Ne dajo na trg sistema, za katerega utemeljeno sumijo neskladnost; od ponudnika zahtevajo korektivne ukrepe in obvestijo pristojne organe, če je potrebno.
- Zagotavljajo pogoje shranjevanja in transporta, ki ne ogrožajo skladnosti ali varnosti; hranijo dokumentacijo in sodelujejo z nadzornimi organi.

6.4 Distributerji – skrbniški pregled in sledljivost

- Pred dobavo preverijo, da so prisotni zahtevani označbi/oznake, navodila in EU skladnostna dokumentacija; preverijo jezikovne zahteve za navodila v državi prodaje.
- Če zaznajo neskladnost ali tveganje, sistem ne sme biti dobavljen, dokler ponudnik ne izvede korektivnih ukrepov; o resnih zadevah obvestijo pristojne organe.
- Zagotavljajo, da skladiščenje in logistika ne poslabšata varnosti/robustnosti; na zahtevo omogočajo vpogled v evidence dobav in serijskih/različic.

6.5 Proizvajalci proizvodov z vgrajeno UI – pot A (Priloga I) in integracija skladnosti

- Kadar je UI varnostna komponenta proizvoda, ki spada pod poseben harmoniziran predpis EU (npr. medicinski pripomočki, stroji), proizvajalec izvede ustrezen postopek skladnosti po ‘pot A’ in zagotovi, da UI komponenta izpolnjuje relevantne AI zahteve.
- Arhitekturo in interakcije med UI ter ‘klasičnimi’ varnostnimi funkcijami opiše v tehnični dokumentaciji proizvoda; določi ‘safe-state’, postopke za varno zaustavitev in vzdrževanje.
- Če UI del vpliva na klasifikacijo tveganja proizvoda, proizvajalec to utemelji v oceni tveganja ter predloži dodatne teste/mitigacije; zagotovi navodila za operaterje in servisne postopke.

6.6 Pooblaščeni zastopniki (authorized representatives) – mandat v EU

- Na podlagi pisnega mandata izvajajo naloge v imenu ponudnika: hranjenje izjave o skladnosti in relevantnih delov tehnične dokumentacije, sodelovanje z nadzornimi organi, posredovanje korektivnih ukrepov.
- Skrbijo, da so kontaktni podatki in dokumenti dostopni pristojnim organom; ob sumu resnih tveganj posredujejo ustrezna obvestila.

6.7 Dobavna veriga in tretje osebe – podatki, modeli, orodja in infrastruktura

- Dobavitelji podatkov: zagotovijo pravne podlage/licence, opise kakovosti in porekla, dokumentirane transformacije ter omejitve uporabe; podpišejo 'data contract' z metrikami kakovosti in SLO.
- Dobavitelji modelov/komponent: predložijo 'artefact passport' (izvor, različice, odvisnosti, licence, rezultati testov robustnosti/pristranskosti, varnostne oznake); podajo navodila za varno integracijo.
- Ponudniki oblačnih storitev/infrastrukture: zagotavljajo varnostne funkcije (npr. TEEs, SBoM, monitoring), politike posodobitev in postopke odziva na incidente; pogodbeno uredijo razdelitev odgovornosti.
- V pogodbah za dobavno verigo se določijo obvezne evidence, pravice do audita, obvestilni roki ob incidentih in poročanje metrik, ki so potrebne za PMS in presojo skladnosti.

6.8 Post-market nadzor (PMS), incidenti in korektivni ukrepi

- Ponudniki pripravijo PMS načrt: spremljanje metrik (točnost, robustnost, zanesljivost), drift-a podatkov, pristranskosti po podskupinah, varnostnih opozoril in incidentov; določijo sprožilce za retrening/rollback.
- Uvajalci vodijo operativno spremljanje v svojem kontekstu in poročajo o resnih incidentih brez odlašanja; sodelujejo pri preiskavah in korektivnih ukrepih.
- Vzpostavi se proces CAPA: odpravljanje vzrokov, validacija učinkovitosti in dokumentiranje; po potrebi se izvede začasna izključitev AI ali odpoklic različice modela.
- Komunikacija do uporabnikov/regulatorjev: jasna obvestila o vplivih, posodobitvah in omejitvah; posodobitev IFU in transparentnost evidence sprememb.

6.9 Registracije, oznake in spremljajoči dokumenti

- Registracija HR-sistemov v EU bazo (kjer je predpisana) pred dajanjem na trg ali uporabo; zagotavljanje točnih in posodobljenih podatkov o različicah in konfiguracijah.
- Oznaka CE (kadar je zahtevana) ter EU izjava o skladnosti; sledljivost verzij modelov/datasetov/konfiguracij v tehnični dokumentaciji.
- Hranjenje dokumentacije in evidence za obdobje, določeno v predpisih (tipično najmanj 10 let) ter omogočen dostop pristojnim organom.
- Usklajenost jezikov: navodila in ključni povzetki v uradnem jeziku države uporabe (v Sloveniji – slovenski jezik).

7 Standardi, presoja skladnosti, certifikati, registracija

To poglavje sistematično pojasni, kako Uredba (EU) 2024/1689 o umetni inteligenci (»Akt o UI«) ureja standarde, presojo skladnosti, certifikate in registracijo za visokotvegane sisteme UI.

7.1 Harmonizirani in skupni standardi (domneva skladnosti)

• Harmonizirani standardi: Evropska komisija lahko zaprosi evropske organizacije za standardizacijo (CEN, Cenelec, ETSI), da pripravijo harmonizirane standarde. Kadar ponudnik visokotveganega sistema UI pravilno uporabi veljavne harmonizirane standarde, se vzpostavi domneva skladnosti z ustreznimi zahtevami Akta o UI (čl. 40 AIA).

• Skupne specifikacije (Common Specifications – CS): Če harmonizirani standardi ne obstajajo, so nepopolni ali so objavljeni z omejitvami, lahko Komisija sprejme zavezujoče skupne specifikacije. Uporaba CS prav tako vzpostavi domnevo skladnosti za področja, ki jih CS pokrivajo (čl. 41 AIA).

• Prednostni vrstni red: ponudniki najprej uporabijo harmonizirane standarde; če ti ne obstajajo ali so le delno primerni, uporabijo CS. Če se ponudnik odloči, da standardov/CS ne bo uporabil ali jih bo uporabil le delno, mora skladnost izkazati na drug način (glej 7.3).

7.2 Vloga tehničnih specifikacij in obvladovanje razhajanj

Harmonizirani standardi in/ali skupne specifikacije prevajajo zakonske obveznosti čl. 8–15 AIA v preverljive tehnične zahteve in postopke (npr. zahteve glede podatkovnih naborov, vodenja evidenc, preglednosti, človeškega nadzora, kibernetske varnosti). Ponudniki morajo dokumentirati, kateri standardi/CS so uporabljeni, na kateri različici, ter upravljati »vrzeli skladnosti« tam, kjer standardov/CS še ni ali kjer jih ponudnik namerno ne uporablja.

7.3 Presoja skladnosti: kako poteka (čl. 43, Priloge VI–VII)

Akt o UI predvideva več poti presoje skladnosti za visokotvegane sisteme UI. Izbira postopka je odvisna od tega, ali so na voljo harmonizirani standardi/CS in ali je sistem hkrati zajet v drugi horizontalni zakonodaji EU o proizvodih z obveznim sodelovanjem priglašenega organa.

Ključne poti presoje skladnosti:

• A) Notranja kontrola (»internal control«) po Prilogi VI – brez neposredne udeležbe priglašenega organa. Ta pot je na voljo praviloma, kadar ponudnik v celoti uporablja ustrezne harmonizirane standarde (čl. 43(2) AIA).

• B) Presoja sistema vodenja kakovosti in tehnične dokumentacije z udeležbo priglašenega organa po Prilogi VII – obvezna, kadar harmonizirani standardi še ne obstajajo, CS niso na voljo ali jih ponudnik ne uporablja oziroma so standardi objavljeni z omejitvami (čl. 43(3) AIA).

• C) Kadar je visokotvegan sistem UI varnostna komponenta proizvoda, ki je že zajet v drugi zakonodaji EU (npr. medicinski pripomočki, železniški sistem ipd.), se uporabijo postopki in priglašeni organi po teh aktih; priglašeni organ mora izpolnjevati tudi dodatne zahteve iz čl. 31 AIA (čl. 43(4) AIA).

Tipičen potek presoje skladnosti:

• 1) Opredelitev namena uporabe (intended purpose) in klasifikacije po AIA (čl. 6–7; hramba v tehnični dokumentaciji po Prilogi IV).

• 2) Vzpostavitev sistema vodenja kakovosti (QMS) za AIA, ki pokriva načrtovanje, razvoj, preverjanje/validacijo, PMS in poročanje (Priloga VII, točka 3).

• 3) Priprava tehnične dokumentacije (Annex IV): arhitektura, podatkovni nabori, metode za obvladovanje pristranskosti, rezultati testiranj, IFU, načrt PMS ipd.

• 4) Izbira poti presoje: (a) notranja kontrola po Prilogi VI, ali (b) vključitev priglašenega organa po Prilogi VII (QMS + presoja tehnične dokumentacije).

• 5) Če je izbrana pot (b): izbor ustreznega priglašenega organa (NB), oddaja vloge, začetni pregled QMS in tehnične dokumentacije, morebitne zahteve po dopolnitvah, ter izdaja certifikata v primeru pozitivnega izida (glej 7.4).

• 6) EU deklaracija o skladnosti in označevanje CE (glej 7.5 in 7.6).

• 7) Registracija visokotveganega sistema v EU podatkovno zbirko (glej 7.7).

• 8) Postmarket nadzor (PMS) in stalno spremljanje učinkovitosti, varnosti in skladnosti; upravljanje sprememb in (ne)substantialnih modifikacij; sodelovanje z organi.

7.4 Certifikati (čl. 44)

Certifikate izdajo priglašeni organi (NB) v postopkih po Prilogi VII. Certifikat je izdan za določeno obdobje in se lahko podaljšuje. Najdaljše trajanje veljavnosti: do 5 let za sisteme iz Priloge I ter do 4 let za sisteme iz Priloge III. Priglašeni organi morajo v nacionalni pristojni organ redno poročati o izdanih, razširjenih, zavrnjenih, omejenih, začasno ustavljenih ali preklicanih certifikatih.

Certifikat pokriva: (i) ugotovitve presoje sistema vodenja kakovosti, (ii) oceno tehnične dokumentacije (vključno s podatkovnimi nabori, preizkusi, metrikami in pragi zmogljivosti), (iii) opredeljeno konfiguracijo in namen uporabe, ter (iv) pogoje/omejitve, ki jih mora ponudnik spoštovati v izkoriščanju.

7.5 EU deklaracija o skladnosti (čl. 47)

Pred dajanjem na trg ali uporabo mora ponudnik pripraviti in podpisati EU deklaracijo o skladnosti, s katero potrdi, da visokotvegan sistem UI izpolnjuje vse zahteve AIA. Deklaracija se lahko združi z deklaracijami po drugih aktih EU (»enotna deklaracija«), kadar je to ustrezno.

Deklaracija mora biti povezljiva s tehnično dokumentacijo, certifikatom (kadar obstaja) in predvidenim namenom uporabe; hraniti jo je treba tako, da je dostopna nadzornim organom in priglašenim organom.

7.6 Oznaka CE (čl. 48)

Po uspešno zaključenem postopku presoje skladnosti ponudnik namesti oznako CE na visokotvegani sistem UI ali na njegovo embalažo oziroma spremno dokumentacijo. Z oznako CE ponudnik potrjuje skladnost s AIA in, kjer je relevantno, z drugimi akti EU. Oznaka CE mora biti vidna, čitljiva in neizbrisna; omejitve uporabe oznak, ki bi lahko zavajale glede pomena CE, se uporabljajo smiselno.

7.7 Registracija v EU podatkovno zbirko za visokotvegane sisteme UI (čl. 49, Priloga VIII)

Ponudniki morajo vpisati določene podatke o visokotveganih sistemih UI v EU podatkovno zbirko (ne-javni del je dostopen pristojnim organom). Vpis vključuje nabor obveznih polj iz Priloge VIII (sekcije A in B), med drugim: identifikacijo ponudnika in sistema, namen uporabe, status skladnosti (vključno s sklici na certifikat/tehnično dokumentacijo), ključne parametre in omejitve, kontakte za PMS ipd. Uvajalci, ki so organi kazenskega pregona ali druge z zakonom določene entitete, vpisujejo dodatke iz sekcije C Priloge VIII, kjer je to predvideno.

Podatke v bazo praviloma vnese ponudnik ali njegov pooblaščeni zastopnik; za specifične uporabe (npr. kazenski pregon) dopolnitve vnese uvajalec. Komisija vodi funkcionalne specifikacije podatkovne zbirke in lahko jih posodablja; ob prvi objavi in posodobitvah sodeluje Odbor (Board).

7.8 Priglašeni organi, priglasitev in nadzor (čl. 31–39, 74–77)

Priglašeni organi (NB) so neodvisna tretja oseba, imenovana in priglašena s strani države članice, ki izvaja ocenjevanje skladnosti po Prilogi VII. Priglasitev je mogoča le, če organ izpolnjuje organizacijske, strokovne in nepristranske pogoje iz čl. 31 AIA (vključno z upravljanjem kompetenc za UI). Države članice izvajajo nadzor nad NB; Komisija in države članice vodijo register priglašenih organov in področij njihovega delovanja.

Organ za nadzor trga (market surveillance) nadzira proizvode na trgu in lahko zahteva tehnično dokumentacijo, izvaja inšpekcijske preglede, naloži popravne ukrepe, omejitve ali umik/odpoklic. Ponudniki in uvajalci morajo sodelovati, poročati o resnih incidentih in vzpostaviti ter izvajati PMS.

7.9 Praktični napotki za podjetja (delovni postopek)

• Klasifikacija in namembnost: potrdite, da gre za visokotvegani sistem (čl. 6–7).

• Strategija standardov: identificirajte in sprejmite ustrezne EN/ISO/IEC harmonizirane standarde; kjer ni standardov, spremljajte CS.

• QMS za AIA: razširite obstoječi ISO 9001/ISO 27001/ISO 42001 ipd. tako, da pokriva čl. 8–15 in Prilogo VII (npr. RMF, podatke, testiranja, evidenco, PMS).

• Tehnična dokumentacija: vzpostavite strukturo po Prilogi IV; uporabljajte revizijsko sled (evidence, modeli, metrike, pragi).

• Izvedba presoje: izberite notranjo kontrolo (Annex VI) ali vključite priglašen organ (Annex VII) in upravljajte časovni načrt ter stroške.

• Deklaracija in CE: po uspešni presoji izdajte EU deklaracijo o skladnosti in namestite oznako CE.

• Registracija: vnesite zahtevane podatke v EU podatkovno zbirko v skladu z roki in navodili Komisije.

• PMS in incidenti: izvajajte spremljanje po trgu, posodabljajte modele in dokumentacijo, prijavljajte resne incidente pristojnim organom.

7.10 Časovnica in prehodne določbe (poudarki)

• Akt o UI je bil objavljen 12. 7. 2024 in začne veljati 1. 8. 2024. Večina obveznosti za visokotvegane sisteme se začne uporabljati 36 mesecev po začetku veljavnosti (predvidoma 2. 8. 2027). Posebne obveznosti (npr. prepovedane prakse) se uporabljajo prej, skladno z AIA.

8 Posebni sklopi

To poglavje pojasnjuje posebna pravila Akta o umetni inteligenci (Uredba (EU) 2024/1689; v nadaljevanju: AIA) za tri občutljiva področja: (8.1) biometrija, (8.2) pregon kaznivih dejanj in (8.3) testiranje v realnih razmerah.

8.1 Biometrija

AIA ureja sisteme za biometrično identifikacijo in preverjanje ter prepoveduje določene biometrične prakse. Pri tem razlikuje med: (a) oddaljeno biometrično identifikacijo v realnem času v javno dostopnih prostorih, (b) biometrično kategorizacijo na podlagi občutljivih atributov ter (c) prepoznavanjem čustev.

Oddaljena biometrična identifikacija (v realnem času, v javno dostopnih prostorih) – pogoji in omejitve:

- Načeloma je uporaba za namene pregona strogo omejena in dovoljena le v posebej utemeljenih primerih, s predhodnim dovoljenjem sodnega ali neodvisnega upravnega organa, omejena po času, prostoru in osebah.
- Uporaba je dovoljena zgolj za potrjevanje identitete specifično ciljnega posameznika in le, kolikor je to nujno potrebno.
- Pred uporabo je treba opraviti oceno učinka na temeljne pravice; pristojne tržne in podatkovnovarstvene organe je treba obveščati, na ravni EU pa se objavljajo letna zbirna poročila o takih uporabah.
- Nacionalno pravo mora določiti podrobna pravila o vložitvi zahtev, izdaji, izvrševanju, nadzoru in poročanju o dovoljenjih.

Biometrična kategorizacija po občutljivih atributih – prepoved:

- Prepovedano je dajanje na trg, dajanje v uporabo ali uporaba sistemov UI za biometrično kategorizacijo oseb po občutljivih atributih (npr. rasa, politična mnenja, verska ali filozofska prepričanja, spolna usmerjenost), razen če je to izrecno dovoljeno v AIA.
- Prepoved velja ne glede na kontekst uporabe (javni ali zasebni sektor).

Prepoznavanje čustev – omejitve in prepovedi:

- AIA močno omejuje uporabo sistemov za prepoznavanje čustev; v določenih okoljih (npr. delovno mesto, izobraževanje) je uporaba prepovedana.
- Kjer je uporaba dovoljena, veljajo stroge zahteve preglednosti, dokumentiranja in človeškega nadzora.
- Uporabniki (osebe, na katerih se sistem uporablja) morajo biti o uporabi obveščeni, kadar to zahteva AIA (npr. obveznost obveščanja pri uporabi sistemov za prepoznavanje čustev ali biometrične kategorizacije).

Dnevniški zapisi in transparentnost:

- Biometrični sistemi morajo podpirati vodenje dnevnikov (logov) z namenom omogočanja poznejše sledljivosti in nadzora skladnosti.
- Za oddaljeno identifikacijo v realnem času se vodijo dodatne evidence (npr. čas uporabe, referenčne zbirke, vhodni podatki, identiteta preverjevalcev), skladno s tehničnimi in postopkovnimi zahtevami AIA.
- Zadevne informacije se vključujejo v navodila za uporabo (IFU) in tehnično dokumentacijo, ki mora omogočati presojo skladnosti.

8.2 Pregon kaznivih dejanj

AIA v posebnih določbah ureja uporabo nekaterih sistemov UI s strani pristojnih organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Uporaba oddaljene biometrične identifikacije v realnem času v javno dostopnih prostorih je v osnovi prepovedana, razen v izjemnih primerih, kjer je nujna in sorazmerna za posebej določene cilje, ob predhodnem dovoljenju in pod strogimi zaščitnimi pogoji.

- Dovoljenje mora izdati sodni organ ali neodvisni upravni organ; izjemoma je mogoče naknadno dovoljenje v nujnih primerih, sicer se podatki izbrišejo.
- Uporaba je omejena na potrjevanje identitete točno določenega posameznika in le v obsegu, ki je nujen glede na resnost in verjetnost grožnje ali kaznivega dejanja.
- Obvezni so: ocena učinka na temeljne pravice, registracija sistema (kjer tako določa AIA), obveščanje nadzornih organov ter letno poročanje Komisiji.
- AIA ne posega v uporabo biometrične identifikacije v kontekstih, ki niso pregon kaznivih dejanj; zanje veljajo druga pravila AIA in/ali nacionalno pravo.

Razmerje do drugih aktov EU in nacionalnih pravil:

- Uporaba UI s strani pristojnih organov mora biti skladna z AIA, hkrati pa skladna z relevantnimi pravili EU o varstvu podatkov in nacionalnim pravom, ki določa podrobnosti (npr. procesna pravila za dovoljenja).
- AIA zahteva, naj države članice natančno določijo postopke za izdajo, izvrševanje, nadzor in poročanje o dovoljenjih ter zagotovijo nadzor nad uporabo v praksi.

8.3 Testiranje v realnih razmerah (člen 60 AIA)

AIA omogoča testiranje visoko tveganih sistemov UI v realnih razmerah, ko laboratorijsko/testno okolje ne zadošča za preverjanje skladnosti ali delovanja. Testiranje je dovoljeno le, če je nujno, pod strogimi pogoji in z odobritvijo pristojnih organov; praviloma ne sme nalagati obveznosti posameznikom, razen če je to izrecno dovoljeno in ustrezno zavarovano.

Ključni pogoji za testiranje v realnih razmerah:

- Odmik od oglaševanja ali komercialne uporabe: testiranje se ne sme zavajajoče predstavljati kot del storitve ali proizvoda, ki je že na trgu.

- Varnost, temeljne pravice in zasebnost: preprečevanje materialne škode in resnega posega v pravice posameznikov; sprejeti je treba ustrezne zaščitne ukrepe.
- Odobritev pristojnega organa: ponudnik ali uvajalec pridobi odobritev v skladu s postopkom iz člena 60, vključno z opisom ciljev, metod, trajanjem, območjem in zavarovanji.
- Odgovornost in nadzor: imenovanje odgovorne osebe, ureditev človeškega nadzora, načrt upravljanja tveganj in postopkov ob incidentih.
- Povezava z RMF in PMS: pred testiranjem in med njim se izvajajo ukrepi v okviru sistema za obvladovanje tveganj (čl. 9) in spremljanje po dajanju na trg (PMS).
- Če se testiranje izvaja na visoko tveganih sistemih za potrebe pristojnih organov, se upoštevajo tudi posebna pravila za kazenski pregon, če je to relevantno.

Organ, ki odobri testiranje, lahko določi posebne pogoje (npr. skrajšanje trajanja, omejitve obsega, zahteve glede obveščanja oseb ali dodatne tehnične zaščitne ukrepe). Po zaključku testiranja je treba izvesti oceno rezultatov, zabeležiti incidente, posodobiti tehnično dokumentacijo in po potrebi prilagoditi ukrepe skladnosti.

Sklici na določbe AIA

- Člen 5 (Prepovedane prakse UI) – določbe o prepovedi biometrične kategorizacije, omejitve in pogoji za oddaljeno biometrično identifikacijo v realnem času; uvodni izjavi (35)–(39) podrobno pojasnjujeta pogoje uporabe in dovoljevanja.
- Člen 50 in povezane določbe – obveznosti preglednosti za določene sisteme, vključno z obveščanjem posameznikov pri uporabi sistemov za prepoznavanje čustev ali biometrično kategorizacijo, kjer je to zahtevano.
- Člen 60 – testiranje v realnih razmerah: postopki, pogoji, odobritve in zaščitni ukrepi; zahteve glede povezave z RMF (čl. 9) in PMS.

9 Upravljanje, nadzor trga in izvrševanje

To poglavje povzema in sistematično razlaga ureditev upravljanja, nadzora trga in izvrševanja po Uredbi (EU) 2024/1689 o umetni inteligenci (»Akt o UI«).

9.1 Ureditev na ravni EU

Urad za umetno inteligenco (AI Office) pri Evropski komisiji

AI Office je organizacijska enota v okviru Komisije, pristojna za dosledno izvajanje Akta o UI, zlasti za nadzor nad obveznostmi za modele splošnega namena (GPAI), podporo usklajenemu izvajanju po državah članicah, pripravo navodil, kodeksov ravnanja in smernic ter za mednarodno sodelovanje. AI Office ima tudi vlogo zbiranja in analiziranja informacij, koordiniranja nadzora za čezmejne zadeve in podpore postopkom izvrševanja na ravni EU (prim. člena 64–67).

Odbor za umetno inteligenco (AI Board)

Odbor za UI sestavljajo predstavniki držav članic. Odbor svetuje Komisiji, posreduje good-practice, pospešuje usklajevanje pristopov nadzornih organov in prispeva k pripravi smernic in skupnih stališč. Odbor sprejme svoj poslovnik in deluje kot platforma za sodelovanje med nacionalnimi organi in Komisijo (prim. člena 69–71).

Svetovalni forum deležnikov

Svetovalni forum zagotavlja raznoliko zastopanost deležnikov (industrija, zagonska podjetja, MSP, akademija, civilna družba, socialni partnerji in relevantne agencije EU). Forum daje mnenja in priporočila Odboru in Komisiji ter lahko ustanavlja podskupine. Sestaja se najmanj dvakrat letno, pripravlja pa tudi letno poročilo o svojih dejavnostih (prim. člen 67).

Znanstveni odbor neodvisnih strokovnjakov

Znanstveni odbor (scientific panel) je telo neodvisnih strokovnjakov, ki Komisiji in Odboru zagotavlja znanstveno podporo – npr. pri modelih splošnega namena in na področjih, kjer je potrebna poglobljena tehnična ocena. Odbor lahko pripravlja mnenja, tehnične analize in metodološke predloge (prim. člen 68).

9.2 Nacionalni organi, priglasitveni in priglašeni organi

Pristojni nacionalni organi in organi za nadzor trga

Vsaka država članica določi enega ali več pristojnih organov za nadzor nad izvajanjem Akta o UI, vključno z organi za nadzor trga, ki izvajajo nadzor v skladu z okvirom NLF in Uredbo (EU) 2019/1020. Ti organi imajo preiskovalna in izvršilna pooblastila, lahko zahtevajo informacije, izvajajo inšpekcijske preglede, odrejajo korektivne ukrepe in sprejemajo začasne ukrepe, kadar obstaja resno tveganje (prim. poglavje o nadzoru trga).

Priglasitveni organi (notifying authorities)

Države članice imenujejo priglasitvene organe, odgovorne za priglasitev in spremljanje priglašenih organov. Priglasitveni organi zagotavljajo, da priglašeni organi izpolnjujejo zahteve glede nepristranskosti, neodvisnosti, usposobljenosti in zavarovanja odgovornosti (prim. člene 30–33).

Priglašeni organi (notified bodies)

Priglašeni organi izvajajo postopke ugotavljanja skladnosti za visokotvegane sisteme UI v primerih, ko je potrebna tretja stranka (npr. sistemski pristopi po členu 43). Imeti morajo ustrezno tehnično, pravno in znanstveno usposobljenost, vzpostavljene postopke, zavarovanje odgovornosti ter sodelovati v usklajevalnih dejavnostih. Seznami podizvajalcev morajo biti javno objavljeni; odgovornost za njihovo delo ostaja pri priglašenem organu (prim. člene 31–34).

9.3 Nadzor trga in postopki izvrševanja

Instrumenti nadzora trga

Organi za nadzor trga spremljajo sisteme UI, ki so dani na trg ali v uporabo, ter preverjajo skladnost s poglavji III in IV Akta o UI. Če ugotovijo neskladnost ali resno tveganje, lahko odrede izločitve, omejitve ali umik s trga, od ponudnika/uvajalca zahtevajo korektivne ukrepe, na primer posodobitve, onemogočanje funkcij, spremembe nastavitev ali prilagoditve navodil za uporabo. V nujnih primerih so možni začasni ukrepi, vključno s prepovedjo (prim. člene o nadzoru trga).

Incidente, reklamacije in postmarket nadzor (PMS)

Ponudniki visokotveganih sistemov UI morajo imeti vzpostavljen načrt PMS ter poročati o incidentih in resnih napakah, ki so lahko kršitev zahtev iz členov 8–15. Organi za nadzor trga lahko zahtevajo podatkovne dnevnike, tehnično dokumentacijo ter rezultate testov in spremljajo korektivne ukrepe do odprave neskladnosti (prim. člena 61–62).

Čezmejni primeri in vloga AI Office

Pri zadevah, ki zadevajo več držav članic ali obveznosti modelov splošnega namena, AI Office v Komisiji koordinira dejanja, posreduje smernice in lahko sproži postopke na ravni EU. Odbor za UI prispeva k usklajenosti razlag in ukrepov (prim. člena 64–71).

9.4 Sankcije (upravne globe in druga izvršilna sredstva)

Akt o UI predvideva sorazmerne, odvračilne in učinkovite upravne globe, ki jih izrekajo države članice. Najvišje mejne vrednosti so določene na ravni EU (člen 101):

- za kršitve prepovedanih praks ali zahtev o podatkih za usposabljanje modelov splošnega namena: do 35 000 000 EUR ali do 7 % celotnega letnega svetovnega prometa podjetja (kar je višje);
- za druge kršitve Akta o UI: do 15 000 000 EUR ali do 3 % celotnega letnega svetovnega prometa podjetja (kar je višje);
- za posredovanje napačnih, nepopolnih ali zavajajočih informacij pristojnim organom: do 7 500 000 EUR ali do 1 % celotnega letnega svetovnega prometa podjetja (kar je višje).

Za mikro, mala in srednja podjetja (vključno z zagonskimi podjetji) so v Aktu določene nižje zgornje meje glob. Poleg denarnih kazni lahko pristojni organi naložijo tudi druge ukrepe: začasne ali trajne omejitve delovanja sistema, umik s trga, poročanje o popravnih ukrepih, javno objavo odločb ali izdajo opozoril.

9.5 Registracija in javni registri

Visokotvegani sistemi UI iz Priloge III se pred dajanjem na trg ali v uporabo vpišejo v javni evropski register, ki ga vodi Komisija. Ponudniki zagotovijo popolnost in točnost vpisanih podatkov, vključno z identifikacijo, opisom namena, navodili za uporabo, informacijami o skladnosti in kontaktom (prim. člen 71).

9.6 CE-označevanje in izjava EU o skladnosti

Za visokotvegane sisteme UI, ki uspešno opravijo ustrezen postopek ugotavljanja skladnosti, se izda izjava EU o skladnosti; sistem se opremi z oznako CE. Označevanje CE potrjuje, da sistem izpolnjuje zahteve iz členov 8–15 in da je bil uporabljen ustrezen postopek presoje skladnosti (prim. člene 48–49).

9.7 Časovnica za vzpostavitev upravljanja in nadzora

Uredba je začela veljati 1. avgusta 2024, posamezne obveznosti pa se uporabljajo postopno. Prepovedane prakse se uporabljajo prej, obveznosti za modele splošnega namena in za visokotvegane sisteme pa po prehodnih rokih, kot so določeni v prehodnih določbah Akta o UI. Države članice morajo imenovati nacionalne pristojne organe in zagotoviti učinkovite mehanizme nadzora in izvrševanja v predpisanih rokih.

10 Časovnica uveljavitve in prehodne določbe

To poglavje povzema časovnico uveljavitve in ključne prehodne določbe Uredbe (EU) 2024/1689 o umetni inteligenci ("Akt o umetni inteligenci", AIA). Datumi in roki so navedeni za načrtovanje skladnosti deležnikov v EU in v Sloveniji.

10.1 Vstop v veljavo in splošna uporaba

- Objavljeno v UL EU: 12. julij 2024.
- Vstop v veljavo: 1. avgust 2024 (20 dni po objavi).
- Splošna uporaba Uredbe: od 2. avgusta 2026, razen izjem, navedenih spodaj.

10.2 Uporaba po fazah glede na vsebino

- Prepovedane prakse (poglavje I–II, vključno z definicijami in pismenostjo na področju UI): od 2. februarja 2025.
- Upravni in nadzorni okvir ter presoja skladnosti (poglavja o upravljanju, priglašeni organi, kazni): od 2. avgusta 2025.
- Obveznosti za modele splošnega namena (GPAI), vključno s sistemsko dokumentacijo in skladnostjo s kodeksi ravnanja ali skupnimi pravili: od 2. avgusta 2025 (kodeksi ravnanja naj bi bili pripravljeni do 2. maja 2025).
- Obveznosti za visoko tvegane sisteme UI po členu 6(1): od 2. avgusta 2027.
- Preostala večina določb (splošna uporaba): od 2. avgusta 2026.

10.3 Prehodne določbe in posebni roki

- Obstoječi visoko tvegani sistemi, dani na trg ali dani v uporabo pred 2. avgustom 2026, morajo izpolniti zahteve AIA le, če se po tem datumu bistveno spremenijo v zasnovi ("significant changes").
- Ponudniki in uvajalci visoko tveganih sistemov, ki so namenjeni za uporabo pri javnih organih, morajo v vsakem primeru doseči skladnost najpozneje do 2. avgusta 2030.
- Ponudniki modelov splošnega namena (GPAI), ki so bili dani na trg pred 2. avgustom 2025, morajo izpolniti obveznosti iz AIA do 2. avgusta 2027.
- Države članice morajo do 2. avgusta 2025 določiti pravila o sankcijah (vključno z upravnimi globami) in priglasiti enotne kontaktne točke, ter zagotoviti zadostne vire za nacionalne pristojne organe.
- Regulatorni preskusni poligoni (regulatory sandboxes) morajo biti operativni najpozneje do 2. avgusta 2026.

10.4 Ključni mejniki (povzetek)

Datum/mejnik	Vsebina obveznosti / učinek
12. 7. 2024	Objava AIA v UL EU.
1. 8. 2024	Vstop AIA v veljavo.

2. 2. 2025	Začetek uporabe prepovedanih praks; uporaba poglavij I–II (definicije, načela, pismenost na področju UI).
2. 5. 2025	Ciljni datum za pripravo kodeksov ravnanja za modele splošnega namena (GPAI).
2. 8. 2025	Začetek uporabe določb o upravljanju in nadzoru (npr. AI Office, odbor, priglašeni organi), kazni; začetek obveznosti za GPAI.
2. 8. 2026	Splošna uporaba AIA; regulatorni preskusni poligoni operativni.
2. 8. 2027	Začetek uporabe obveznosti, vezanih na člen 6(1) (visoko tvegani sistemi).
2. 8. 2030	Skladnost obvezna za visoko tvegane sisteme, namenjene za uporabo pri javnih organih; izjema za velike informacijske sisteme EU do konca 2030.
2. 8. 2028 / 2029 / 2031	Ocene in poročila Komisije o izvajanju, sankcijah, standardizaciji in morebitnih spremembah (periodična poročila).

10.5 Sektorske posebnosti in povezave s pravnim redom EU/RS

- AIA sobiva z obstoječo sektorsko zakonodajo EU iz Priloge I (npr. medicinski pripomočki, igrače, stroji ipd.). Za proizvode, ki že imajo obvezno ocenjevanje skladnosti po harmonizirani zakonodaji, se zahteve AIA upoštevajo v okviru istega postopka CE.
- Za velike informacijske sisteme EU (naštete v prilogi k AIA) veljajo posebne prehodne določbe: skladnost najkasneje do konca leta 2030.
- Slovenija mora do 2. 8. 2025 določiti pristojne organe, enotno kontaktno točko in pravila o sankcijah ter priglasiti priglašene organe (če/kadar bodo imenovani). Postopki sprejema nacionalnih pravil o izvrševanju in sankcijah potekajo v okviru redne zakonodajne procedure v RS.

10.6 Praktična priporočila za deležnike (načrt skladnosti)

- Naredite popis sistemov UI in ugotovite, ali sodijo med prepovedane, transparentnostno zavezane, GPAI ali visoko tvegane sisteme.
- Za GPAI vzpostavite sledljivost izvora podatkov/modelov, pripravite model card/tehnično dokumentacijo ter spremljajte objavo kodeksov ravnanja ali skupnih pravil.
- Za visoko tvegane sisteme začnite z oceno skladnosti po čl. 8–15 (RMF, podatki, tehnična dokumentacija, vodenje evidenc, preglednost, človeški nadzor, točnost/robustnost/kibernetska varnost) in načrtujte presojo skladnosti (NB) ter registracijo v EU zbirki.
- Vključite pravne službe in DPO/pooblaščence za varstvo podatkov, zlasti pri biometriji, zaposlovanju, izobraževanju in kritični infrastrukturi.
- Pripravite notranje politike PMS (post-market surveillance) in postopke za prijavo resnih incidentov.

11 Priporočila za implementacijo v Sloveniji

• Organizacijski model skladnosti; kontrolni seznami; integracija z GDPR DPIA/NIS2; dobavna veriga; pogodbeni mehanizmi; notranje revizije. [dopolnite]

11 Priporočila za implementacijo v Sloveniji

POJASNILO: Spodnja priporočila temeljijo na trenutno javno dostopnih informacijah o Uredbi o umetni inteligenci Evropske unije (AI Act – Uredba (EU) 2024/1689) ter na dobrih praksah iz standardov. Niso pravni nasvet in se lahko spremenijo z objavo novih smernic, harmoniziranih standardov in nacionalnih izvedbenih aktov. Organizacije naj pred sprejemom odločitev preverijo najnovejše uradne vire.

11.1 Organizacijski model skladnosti

Cilj: zagotoviti, da so zahteve Uredbe o umetni inteligenci (AI Act) sistematično vgrajene v procese in vloge organizacije ter da je mogoče skladnost dokazati z evidencami.

• **Upravljanje (governance):** Uvedite 'AI odbor za skladnost', ki vključuje vodstvo, lastnike poslovnih procesov, vodjo skladnosti, predstavnika za varstvo osebnih podatkov (DPO – Data Protection Officer) in vodjo informacijske varnosti (CISO – Chief Information Security Officer). Odbor določi politiko rabe UI, odgovornosti in pristope k odobritvam izdaje modelov (release gates).

• **Sistem vodenja za UI:** Vzpostavite sistem vodenja za umetno inteligenco (AIMS – Artificial Intelligence Management System) skladno z ISO/IEC 42001. AIMS poveže načrtovanje, upravljanje tveganj, nadzor po dajanju na trg (PMS – Post-Market Surveillance) in stalne izboljšave (CAPA – Corrective and Preventive Actions).

• **Vloge in odgovornosti:** Določite 'lastnika primera rabe', 'skrbnika podatkov' (Data Steward), 'odgovorno osebo za model' (Model Owner) in 'odgovorno osebo za skladnost UI'. Za vsako vlogo pripravite opis nalog, pravice odločanja in odgovornost za evidence.

• **Usposabljanje in pismenost:** Uvedite program pismenosti na področju UI (AI literacy) za ključne deležnike (vodstva, razvijalci, operaterji, pravna služba). Vsebina naj zajema razumevanje tveganj, pristranskosti, človeškega nadzora in omejitev modelov.

• **Integracija z obstoječimi sistemi:** Poravnajte procese z obstoječimi sistemi vodenja kakovosti (QMS – Quality Management System) in informacijske varnosti (ISMS – Information Security Management System). Namesto vzporednih postopkov uporabite skupne predloge, kontrolne sezname in evidence.

11.2 Kontrolni seznami (check-listi) za ključne faze

Predlagani minimalni kontrolni seznami (prilagodite kontekstu rabe):

– Pred začetkom projekta:

Opredeljen namen uporabe, primer rabe in deležniki; potrjen lastnik primera rabe.

Klasifikacija glede na AI Akt (nizko tveganje / visoko tveganje) in izbrana 'pot' skladnosti (Priloga I ali Priloga III).

Preliminarna ocena tveganj (RMF – Risk Management Framework) in odločitev o potrebi po oceni vplivov na temeljne pravice (FRIA – Fundamental Rights Impact Assessment) ter oceni učinka na varstvo podatkov (DPIA – Data Protection Impact Assessment) po Splošni uredbi o varstvu podatkov (GDPR – General Data Protection Regulation).

– Pred učenjem modela:

Dokumentirani viri podatkov, zakonitost obdelave (GDPR), licenciranje, pogodbe in omejitve uporabe.

Merila kakovosti podatkov (ISO/IEC 5259-1) in načrt upravljanja kakovosti podatkov (ISO/IEC 5259-3).

Načrt testiranja pravičnosti in pristranskosti (IEEE 7003) z metrikami in pragovi po podskupinah.

– Pred uvedbo (pre-release gate):

Tehnična dokumentacija skladno s členom 11 in Prilogo IV (AI Act) – popolna, pregledana in podpisana.

Dokazi o robustnosti in kibernetski varnosti (ETSI TS 104 223) ter o obvladljivosti/človeškem nadzoru (ISO/IEC TS 8200).

'Artefact passport' (pasport artefakta) z izvorom, različicami, odvisnostmi, licencami in rezultati testov.

– Po uvedbi (PMS – nadzor po dajanju na trg):

Vzpostavljene metrike za natančnost, robustnost, pristranskost in varnost; pragovi alarmiranja.

Postopki za prijavo incidentov, 'override' in 'safe-stop'; zabeleženi razlogi in učinki na uporabnike.

Periodični pregledi FRIA/DPIA in ponovna ocena tveganj (ISO/IEC 23894).

11.3 Integracija z GDPR (Splošna uredba o varstvu podatkov) – DPIA in z Direktivo NIS2

Za projekte z osebnimi podatki izvedite oceno učinka na varstvo podatkov (DPIA – Data Protection Impact Assessment) in jo povežite z oceno tveganj po AI Akt. Za operaterje ključnih in pomembnih storitev vključite zahteve Direktive (EU) 2022/2555 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2 – Network and Information Security Directive).

Praktični koraki:

• Uskladite registre obdelav, FRIA (ocena vplivov na temeljne pravice) in DPIA v enoten tok odločanja; izogibajte se podvajanju vprašalnikov.

• Za NIS2 določite povezavo med varnostnimi nadzori in robustnostjo modelov (npr. varnostne teste, odvisnosti, SBoM – Software Bill of Materials).

• V kazalu tehnične dokumentacije dodajte križne sklice: 'tveganja' ↔ 'zasebnost' ↔ 'kibernetska varnost'.

11.4 Dobavna veriga (modeli, podatki, orodja, infrastruktura)

Vzpostavite obvladovanje dobavne verige AI: pogodbe, preverjanje licenc, integritete in izvorov. Pri modelih tretjih oseb uporabite 'artefact passport' in zahtevo po minimalnih varnostnih kontrolah (ETSI TS 104 223).

• Zahtevajte SBoM za modele in pipeline (seznam komponent, verzij in licenc).

• Preverjajte integriteto artefaktov (podpisi, 'hash') in vzdržujte revizijsko sled uvozov/posodobitev.

• Določite 'no-go' pogoje (npr. neznan izvor podatkov, nezdružljive licence, manjkajoči testi pristranskosti).

11.5 Pogodbeni mehanizmi

V razpisih in pogodbah vključite zahteve za skladnost z Uredbo o umetni inteligenci (AI Act) in relevantnimi standardi ter pravico do presoje (audit) in dostopa do evidenc.

• Zahteva po tehnični dokumentaciji po členu 11 (Priloga IV) ter 'transparency profile' (IEEE 7001) za uporabnike/operaterje.

• Minimalni varnostni nabor (ETSI TS 104 223), vključno s preskusi evasion/poisoning in politikami za 'safe-stop'.

• Kakovost podatkov (ISO/IEC 5259-1 in 5259-3) ter obvezna FRIA/DPIA, kjer je primerno.

• SLA/KPI za PMS: roki za prijavo incidentov, MTTR (Mean Time To Restore), pragovi za 'override' in pogoji za 'rollback'.

11.6 Notranje revizije in stalne izboljšave

Vzpostavite letni program notranjih presoj skladnosti UI. Presoje naj pokrivajo celoten življenjski cikel (podatki, modeli, orodja, uvajanje, PMS) in naj bodo vezane na merila iz AI Akt in internih politik.

Priporočila:

• Uporabite matriko 'zahteva → kontrola/test → dokazilo' za sledljivost.

• Izvedite 'red team' preglede za robustnost in pristranskost; dokumentirajte rezultate in CAPA.

• Vzpostavite register izboljšav z lastniki, roki in prioritetami (risk-based).

11.7 Praktični napotki: 90-dnevni plan

Primer faznega pristopa za organizacije, ki začenjajo z implementacijo:

• **Dnevi 1–30:** Inventura primerov rabe; preliminarna klasifikacija po AI Akt; imenovanje vlog; osnutek politike UI; izbor predlog za FRIA/DPIA; priprava osnovnih kontrolnih seznamov.

• **Dnevi 31–60:** Vzpostavitev AIMS (ISO/IEC 42001) v minimalnem obsegu; prilagoditev QMS/ISMS; oblikovanje 'artefact passport' in registra modelov; pilotski FRIA/DPIA; načrt PMS (metrike, pragovi).

• **Dnevi 61–90:** Uradna odobritev pre-release 'gates'; testni zagon PMS dashboarda; izobraževanje ključnih deležnikov; izvedba prve notranje presoje in CAPA načrta.

11.8 Predlog kazalnikov (KPI/SLO) za spremljanje

• Natančnost in robustnost po podskupinah; trend drift-a vhodnih podatkov.

• Stopnja in čas 'override/safe-stop'; MTTR/MTBF (Mean Time Between Failures).

• Število in resnost incidentov; delež pravočasno obravnavanih FRIA/DPIA; status CAPA.

• Delež modelov z veljavno tehnično dokumentacijo in aktualnimi 'artefact passport' zapisi.

11.9 Predloge dokumentov (na kratko)

V prilogi priporočamo vzorce: kontrolni seznam pre-release, predloga za FRIA (ocena vplivov na temeljne pravice), predloga za DPIA (ocena učinka na varstvo podatkov), ter 'artefact passport' za modele in podatkovne nabore.

11.10 Meje priporočil in nadaljnji koraki

Ker se praksa in sekundarna zakonodaja še razvijata (npr. smernice Evropske komisije in morebitni harmonizirani standardi), naj organizacije načrtujejo polletne posodobitve politik, kontrolnih seznamov in predlog dokumentacije. Ob spremembah naj se izvede ponovna ocena tveganj in posodobitev tehnične dokumentacije.

11.12 Od stanja do ukrepanja: neobvezujoči predlogi za prihodnje korake

Spodnje točke so pripravljene kot neobvezujoči predlogi, zasnovani na trenutno razpoložljivih informacijah. Namenjene so kot usmeritve za razmislek in postopno izvedbo, z možnostjo prilagoditve glede na nadaljnje usklajevanje, razpoložljive vire in prihodnja evropska navodila (npr. harmonizirani standardi, smernice Evropske komisije).

1) Kaj je v Sloveniji že vzpostavljeno (strnjeno)

- Horizontalni izvedbeni pristop: v pripravi je poseben nacionalni zakon za izvajanje Uredbe (EU) o umetni inteligenci (AI Act), ki naj bi med drugim določil pristojne organe, prekrške, registre in postopke.
- Standardizacijska osnova: Slovenski inštitut za standardizacijo (SIST) že omogoča dostop do pomembnih evropskih izdaj EN ISO/IEC za področja, kot so upravljanje tveganj, arhitektura in terminologija, kar olajša sklicevanje v razpisih in pogodbah.
- Obstoječe regulatorne kapacitete: Informacijski pooblaščenec (IP-RS) na področju varstva osebnih podatkov (Splošna uredba o varstvu podatkov – GDPR), Urad Vlade RS za informacijsko varnost (URSIV) na področju kibernetske varnosti (Direktiva (EU) 2022/2555 – NIS2) ter Slovenska akreditacija (SA) kot nacionalni akreditacijski organ – vsi predstavljajo pomembne temelje za nadaljnjo vzpostavitev AI-specifičnih postopkov.
- Vključevanje deležnikov: potekajo posveti in strokovna srečanja med državo, akademijo, digitalnimi inovacijskimi stičišči in industrijo, kar je dobra podlaga za poenotenje praks.

2) Možne nadaljnje aktivnosti

A. Upravni in institucionalni koraki

- Razmisliti o formalni določitvi pristojnih organov za izvajanje AI Akt (koordinator, nadzorna telesa, prekrškovni organi) in o ustanovitvi medorganskega koordinacijskega telesa (AI-koordinacijski odbor), ki bi lahko vključeval npr. ministrstva, IP-RS, URSIV, SIST, Slovensko akreditacijo in druge ključne deležnike.
- Pripraviti načrt priglašanja (notifikacije) preskuševalnih in certifikacijskih organov ter shemo akreditacije v sodelovanju s Slovensko akreditacijo, kadar bodo na ravni EU na voljo ustrezni harmonizirani standardi in tehnične specifikacije.
- Preučiti možnosti vzpostavitve nacionalnega registra za visoko-tvegane sisteme UI (z navezavo na evropske registre) in pripraviti operativne postopke za nadzor po dajanju na trg (post-market monitoring), vključno z obrazci, roki poročanja in incidentnimi protokoli.

B. Smernice, obrazci in orodja

- Razviti nacionalne predloge obrazcev in kratke smernice za oceno vplivov na temeljne pravice (Fundamental Rights Impact Assessment – FRIA) v usklajevanju z oceno učinkov na varstvo podatkov (Data Protection Impact Assessment – DPIA), za tehnično dokumentacijo

(Priloga IV AI Akt), informacije za uvajalce (Instructions for Use – IFU), vodenje evidenc (logi) ter za t. i. »artefact passport« (podatki o modelu, podatkih, testih, izvoru in licencah).
- Pripraviti kontrolne sezname, ki se sklicujejo na vodilne standarde (EN ISO/IEC 23894, EN ISO/IEC 23053, ISO/IEC 42001, ISO/IEC 5259-1/-3, ISO/IEC TS 8200, ETSI TS 104 223) in so prilagojeni MSP ter javnemu sektorju.

C. Podpora praksi in zmogljivosti

- Razmisliti o uvedbi pilotnega »AI compliance sandbox« oziroma svetovalne točke (help-desk) za mala in srednja podjetja ter javni sektor – za hitro usmerjanje, pregled dokumentacije in povezovanje na standarde.
- Vzpostaviti program usposabljanj v več stopnjah: za vodstva in pravne/službe skladnosti (obveznosti in dokazila), za tehnične ekipe (upravljanje tveganj, kakovost podatkov, robustnost in kibernetska varnost, človeški nadzor) ter za javni sektor (razpisi, pogodbeni mehanizmi, upravljanje dobaviteljev).
- Pripraviti vzorčne razpisne pogoje za javna naročila, ki vključujejo sklice na EN ISO/IEC standarde, zahteve po FRIA/DPIA, IFU, artefact-passport ter osnovne elemente PMS.

D. Meritve napredka in komunikacija

- Opredeliti nabor kazalnikov (Key Performance Indicators – KPI) pripravljenosti, npr.: število organizacij z uvedenim sistemom vodenja za umetno inteligenco (Artificial Intelligence Management System – AIMS; ISO/IEC 42001 ali ekvivalent), število izvedenih FRIA/DPIA, delež projektov z vzpostavljenim PMS, čas reševanja incidentov, delež javnih razpisov s sklici na EN ISO/IEC.
- Pripraviti komunikacijski paket (vodiči, pogosta vprašanja – FAQ, primeri dobrih praks) in jasno označiti kontaktne točke za pomoč uporabnikom.

3) Hitri koraki

- Objava osnutkov obrazcev (FRIA, IFU, artefact-passport) ter kontrolnih seznamov v odprtih formatih (DOCX/XLSX) kot delovnih pripomočkov.
- Zagon pilotnega help-deska (npr. mesečne odprte ure, standardizirana zbirka vprašanj in odgovorov).
- Izdaja vzorčnih razpisnih členov za visoko-tvegane primere uporabe in kratek praktični priročnik za post-market monitoring (PMS).
- Vzpostavitev terminološkega glosarja (sklic na SIST EN ISO/IEC 22989) in vključitev glosarja v vse predloge dokumentacije.

4) Odvisnosti in tveganja, na katera velja biti pozoren

- Možni zamiki pri evropskih smernicah in harmoniziranih standardih lahko vplivajo na dinamiko nacionalnih certifikacijskih postopkov; v takih primerih bi bilo smiselno predvideti prehodne rešitve (npr. uporaba osnutkov standardov oziroma priznanih dobrih praks).
- Kadrovske zmogljivosti (regulatorji, preskuševalni/certifikacijski organi, help-desk) so lahko omejene; priporočljivo je načrtovati postopno krepitev kapacitet.
- Neenotna terminologija in obrazci povečujejo administrativno breme in zmanjšujejo primerljivost dokazil; glosar in standardizirane predloge lahko to tveganje zmanjšajo.

Sklepno: glede na obstoječe temelje v Sloveniji bi lahko v naslednjih 12–18 mesecih korak za korakom utrdili institucionalni okvir, pripravili javno dostopne smernice in obrazce, zagnali pilotne podporne mehanizme ter poenotili razpisne in nadzorne prakse. Predlogi zgoraj so namenjeni kot izhodišče za razpravo in prilagoditev dejanskim potrebam deležnikov.

A Priloge k Poglavju 4 – FRIA/PIA predloge in vzorci »Artefact Passport«

Ta dokument dopolnjuje poglavje 4 (Klasifikacija visokotveganih sistemov) in vsebuje uporabne predloge za ocenjevanje vplivov na temeljne pravice (FRIA) in zasebnost (PIA), skupaj z vzorčnimi obrazci »Artefact Passport« za modele in podatkovne nabore. Predloge so pripravljene tako, da jih je mogoče neposredno vključiti v tehnično dokumentacijo (čl. 11 AI Akta) ter v QMS/AIMS postopke (ISO/IEC 42001) in register tveganj (EN ISO/IEC 23894).

A. FRIA – Fundamental Rights Impact Assessment (predloga)

Namen FRIA je sistematično prepoznati in ovrednotiti vplive sistema UI na temeljne pravice posameznikov in skupin. Predloga spodaj je razdeljena na identifikacijski del, kontekst uporabe, sistematično oceno tveganj in načrt ukrepov.

A.1 Identifikacija in osnovni podatki

Naziv sistema	
Klasifikacija po čl. 6–7 (pot A/B)	
Faza življenjskega cikla (razvoj/test/prod)	
Namen in opis funkcije	
Upravljavec/ponudnik (odgovorna oseba)	
Deležniki (primarni/sekundarni)	
Pravna podlaga in regulativni okvir	
Sklici na tehnično dokumentacijo (ID, verzije)	

A.2 Kontekst in primer uporabe

- Opis prizadetih skupin in potencialno ranljivih skupin.
- Operativni kontekst (npr. javni sektor, kritična infrastruktura, B2C/B2B).
- Odločilne točke in možne posledice (odklonitve, omejitve, dodelitve ugodnosti).
- Človeški nadzor: kdo, kdaj in kako poseže (sklic na ISO/IEC TS 8200).

A.3 Matrika tveganj za temeljne pravice (identifikacija–analiza–ukrepi)

ID	**Opis tveganja**	**Prizadete pravice/skupine**	**Verjetnost**	**Vpliv**	**Raven tveganja**	**Mitigacije/kontrole**	**Preostalo tveganje**
			Nizka/Srednja/Visoka	Nizek/Srednji/Visok	Nizko/Srednje/Visoko	Npr. človeški nadzor; pragovi; pojasnila; pritožbe	
			Nizka/Srednja/Visoka	Nizek/Srednji/Visok	Nizko/Srednje/Visoko	Npr. človeški nadzor;	

						pragovi; pojasnila; pritožbe	
			Nizka/Srednja/Visoka	Nizek/Srednji/Visok	Nizko/Srednje/Visoko	Npr. človeški nadzor; pragovi; pojasnila; pritožbe	
			Nizka/Srednja/Visoka	Nizek/Srednji/Visok	Nizko/Srednje/Visoko	Npr. človeški nadzor; pragovi; pojasnila; pritožbe	

A.4 Posebni vidiki in dokazila

• Testi pravičnosti in pristranskosti (IEEE 7003) – izbrani atributi, metrike, pragovi.
• Transparentnost (IEEE 7001) – profili informacij za uporabnike/operaterje/revizorje.
• Kakovost podatkov (ISO/IEC 5259-1/-3) – poročila po podskupinah.
• Robustnost in kibernetska varnost (ETSI TS 104 223) – pred-objavne baterije testov; sklici na rezultate.
• PMS (AI Act, čl. 61–68): spremljanje incidentov, drift, CAPA; frekvenca in kazalniki.

A.5 Odločitev in odobritev

Sklep (go/conditional/no-go)	
Pogoji za uvedbo (če pogojno)	
Odgovorna oseba/organ za odobritev	
Datum in veljavnost ocene	
Načrt ponovne ocene (triggerji/frekvenca)	

B. PIA – Privacy Impact Assessment (predloga)

PIA oceni tveganja za zasebnost in skladnost obdelave osebnih podatkov. Predloga sledi načelom ‘privacy by design/default’ in se lahko uskladi z IEEE 7002 ter z zahtevami člena 10 AI Akta.

B.1 Identifikacija obdelave

Opis obdelave in namen	
Vrste podatkov (posebne kategorije?)	
Subjekti podatkov in obseg	
Pravne podlage (GDPR/lex specialis)	
Prenosi/sprejemniki/tretje države	
Roki hrambe in politika brisanja	

Tehnične in organizacijske kontrole	
Dostopi, vloge, sledljivost	

B.2 Tveganja za zasebnost in ukrepi

ID	Opis tveganja	Verjetnost	Vpliv na pravice	Raven	Mitigacije	Preostalo
		N/S/V	N/S/V	N/S/V	Minimizacija; anonimizacija; TEEs; DLP; DPIA	
		N/S/V	N/S/V	N/S/V	Minimizacija; anonimizacija; TEEs; DLP; DPIA	
		N/S/V	N/S/V	N/S/V	Minimizacija; anonimizacija; TEEs; DLP; DPIA	
		N/S/V	N/S/V	N/S/V	Minimizacija; anonimizacija; TEEs; DLP; DPIA	

B.3 Transparentnost in pravice posameznikov (DSAR)

- Obvestila posameznikom (vsebina, kanali, čas).
- Mehanizmi za uveljavljanje pravic (dostop, popravek, izbris, omejitev, ugovor, prenosljivost).
- Čas odziva in operativni kazalniki (SLA).
- Beleženje zahtev in izidov (evidence).

B.4 Sklep in odobritev

Sklep (go/conditional/no-go)	
Dodatni pogoji	
Odobritev odgovorne osebe (DPO)	
Datum/veljavnost	

C. Vzorčni obrazci – »Artefact Passport«

»Artefact Passport« je standardizirana kartica identitete modela ali podatkovnega nabora. Omogoča sledljivost, primerljivost in hitro presojo skladnosti (AI Act čl. 11, 15) ter se povezuje z

arhitekturo (EN ISO/IEC 23053), kakovostjo podatkov (ISO/IEC 5259-1/-3), tveganji (EN ISO/IEC 23894), preglednostjo (IEEE 7001), pristranskostjo (IEEE 7003) in varnostjo (ETSI TS 104 223).

C.1 Model – Artefact Passport

Polje	Vnos
Model ID / naziv	
Različica modela / datum	
Tip/Arhitektura (npr. XGBoost, CNN, LLM)	
Namen uporabe (use-case) in meje	
Odgovorna oseba (owner) in stik	
Povezani podatkovni nabori (ID, verzija)	
Konfiguracije in hiperparametri (sklic)	
Trening okolje in odvisnosti (SBoM)	
Metrike uspešnosti (globalne in po podskupinah)	
Metrike pravičnosti (IEEE 7003) in pragi	
Robustnostni testi (ETSI TS 104 223) – rezultati	
Varnostne kontrole (dostopi, TEEs, šifriranje)	
Transparentnost (IEEE 7001) – profil/obvestila	
Človeški nadzor (ISO/IEC TS 8200) – mehanizmi	
PMS: drift monitorji, incidenti, CAPA	
Licenca/model cards in omejitve uporabe	
Odobritve (QA/Compliance/Legal) – datumi/podpisi	
Opombe in znane omejitve	

C.2 Podatkovni nabor – Artefact Passport

Polje	Vnos
Dataset ID / naziv	
Različica / datum	
Izvor/pravice/licenca	
Opis vsebine in namena	
Subjekti in atributi (posebne kategorije?)	
Kakovostni kazalniki (ISO/IEC 5259-1)	
Porazdelitve in neuravnoteženost	
Označevanje/ground truth (postopki/kakovost)	
Transformacije in pipeline (sledljivost)	
Anonimizacija/psevdonimizacija	
Dostopi in varovanje (šifriranje/TEEs)	
GDPR/PIA sklici in roki hrambe	
Vprašanji pravičnosti (atributi, tveganja)	

Odobritve za uporabo (pravni/etika/QA)	
Povezani modeli/eksperimenti	

C.3 Dnevnik sprememb (change log)

Datum	Artefakt	Verzija	Sprememba	Odobritev	Sklic na evidence

Opomba: vsa polja so primerna za povezave na repozitorije (CI/CD, registri modelov, DMS) in na evidence testov ter presoj.