Tehnične smernice:

Digitalizacija kulturne dediščine z uporabo velikih jezikovnih modelov – v1.0

Veliki jezikovni modeli (VJM) postajajo pomembno orodje umetne inteligence (UI) za napredno digitalizacijo kulturne dediščine v Sloveniji. Učinkovita in varna uporaba VJM v slovenskih produkcijskih in javnih okoljih odpira vrsto tehničnih in upravljavskih izzivov. Za uspešno implementacijo VJM je med drugim potrebno zagotoviti ustrezno kakovost vhodnih podatkov, tehnično zanesljivost samih modelov in primerno infrastrukturo. Te smernice so namenjene naročnikom in razvijalcem UI-orodij, temelječih na VJM, da bodo lažje dosegali tehnične standarde za zagotavljanje kakovosti rešitev in skladnost z nacionalno ter evropsko zakonodajo.

1. VJM: tehnične smernice za razvoj in uporabo

VJM imajo velik potencial pri digitalizaciji slovenske kulturne dediščine, a hkrati prinašajo številne tehnične in upravljavske izzive. Ena glavnih omejitev je pojav t.i. *halucinacij*, pri katerem model generira na videz prepričljive, vendar dejansko nepravilne ali nepreverjene informacije, kar neposredno zmanjšuje zanesljivost in sledljivost rezultatov. Zato je treba uvajati arhitekturne in sistemske pristope za zmanjševanje tega pojava – vključiti preverjene vire znanja, deterministična pravila in vmesne plasti, ki zagotavljajo uporabo potrjenih dejstev. Dodatna omejitev je, da večina VJM ni optimizirana za slovenski jezik in kulturni kontekst, kar se kaže v slabšem razumevanju nians uporabniških zahtev ter manj konsistentnih rezultatih pri kompleksnih scenarijih uporabe.

Ključno je, da je pri uporabi VJM za potrebe slovenske kulturne dediščine tehnologija prilagojena slovenskemu jeziku in družbenemu okolju. Tuji modeli, kot sta komercialni GPT-5 ali z odprtimi utežmi Gemma so trenirani pretežno na angleških in drugih velikih jezikih, zato lahko neposredna uporaba takih modelov v slovenskem okolju brez prilagoditev vodi v slabše rezultate ali napake. Priporoča se uporaba oziroma razvoj modelov, ki so primarno učeni na slovenskih podatkih, oziroma dodatno prilagajanje (angl. *fine-tuning*) obstoječih modelov na obsežnem slovenskem in strokovno-domenskem (kulturno-dediščinskem) gradivu.

Sorazmerno s cilji in viri projekta digitalizacije je treba sprejeti odločitve glede izbire osnovnega modela, vrste in obsega njegovega prilagajanja ter uporabe dodatnih metod za izboljšanje delovanja VJM. Izziv predstavlja tudi stabilna in varna integracija VJM v operativne delovne tokove ter upravljanje morebitnih etičnih in pravnih tveganj. To zahteva prilagoditve učnih in inferenčnih postopkov, zagotavljanje preglednosti delovanja modelov ter implementacijo zaščitnih in nadzornih mehanizmov na ravni arhitekture in končne uporabe. Razvoj in uporaba VJM morata ustrezati določenim kakovostnim standardom, da se zagotovi zanesljivo delovanje, varnost in skladnost s predpisi (npr. zahteve Akta o UI).

Priporočila:

1.1. Lokalizacija modelov na slovenski jezik in kulturni kontekst

Prijavitelj mora zagotoviti, da je uporabljeni VJM prilagojen slovenskemu jeziku in kulturnemu okolju. Model mora pri generiranju izhodov delovati v slovenskem jeziku (»razmišljati« v slovenščini) ter izkazovati razumevanje slovenskega zgodovinskega in kulturnega konteksta vsaj na ravni, primerljivi z njegovim razumevanjem globalnih informacij. Ponujena rešitev mora vključevati dokazila ali opis postopka, kako je dosežena ta prilagoditev (npr. opis uporabljenih slovenskih virov za učenje in rezultati evalvacij, ki potrjujejo ustreznost modela v slovenskem okolju).

1.2. Standardiziran razvojni okvir

Za razvoj in poganjanje VJM je treba uporabljati uveljavljeno, odprtokodno programsko infrastrukturo. Prijavitelj mora zagotoviti, da bo rešitev temeljila na preizkušenih in široko podprtih ogrodjih (npr. PyTorch, HuggingFace ipd.), kar bo olajšalo dolgoročno vzdrževanje in interoperabilnost z drugimi sistemi. Vse podporne storitve za modele in, kadar je smiselno, tudi modeli sami, naj bodo kontejnerizirani (npr. z Dockerjem) in orkestrirani s platformo kot je Kubernetes, kar omogoča avtomatsko skaliranje ter visoko razpoložljivost sistema. To zagotavlja, da se modeli lahko izvajajo konsistentno v različnih okoljih (razvojno, produkcijsko) in da je nameščanje posodobitev enostavno in varno.

Prijavitelj mora v ponudbi predstaviti predvideno tehnologijo, programska ogrodja in infrastrukturne rešitve, s katerimi bodo zagotovljeni standardiziran razvoj, obratovanje in vzdrževanje VJM.

1.3. Evalvacija in testiranje modelov

Razvojni proces mora vključevati temeljito evalvacijo razvitega oziroma prilagojenega modela pred njegovo uporabo v produkciji. Prijavitelj mora preizkusiti učinkovitost modela na različnih tipih nalog (npr. razumevanje besedila, povzemanje, vprašanja in odgovori) ter v različnih vsebinskih in jezikovnih kontekstih, ki so relevantni za končno uporabo. Poseben poudarek je na varnostnem testiranju – model mora biti preizkušen z zlonamernimi ali neprimernimi pozivi (t. i. *adversarial testing* in scenariji zlorabe), da se identificirajo in odpravijo neželena vedenja modela (npr. halucinacije, pristranski ali žaljivi odgovori), še preden je model dostopen uporabnikom.
Prijavitelj mora v načrtu razvoja predvideti fazo obsežnega testiranja in v ponudbi opisati merila ter metodologijo evalvacije modela. Rezultate ključnih evalvacij (učinkovitost, varnostni testi ipd.) mora biti izvajalec zmožen predstaviti pred zaključkom projekta oziroma pred prevzemom rešitve.

1.4. Naslavljanje pristranskosti modela

Prijavitelj mora preveriti, ali izbrani osnovni model (ali prilagojeni model) vsebuje kakšne vgrajene stereotipe, pristranskosti ali netočnosti v kontekstu slovenske kulture in zgodovine. V primeru zaznanih odklonov mora predvideti ukrepe za izboljšanje modela, bodisi z dodatnim učenjem na posebej izbranih gradivih, z vnosom

korekcijskih pravil, ali s postopki poravnave z ustreznimi vsebinami (npr. s prilagoditvijo pozivov). Namen je zagotoviti, da model ne reproducira neželenih pristranskosti ali napačnih predstav, ki bi lahko vplivale na interpretacijo slovenske kulturne dediščine.

1.5. Prilagajanje izhodov različnim uporabniškim skupinam

Razvita rešitev mora zagotavljati ustrezno prilagojene izhode za različne ciljne skupine uporabnikov, kot so npr. otroci, tuji turisti, osebe s posebnimi potrebami in domenski strokovnjaki (zgodovinarji, kustosi ipd.). Sistem mora omogočati, da se nivo podrobnosti, zahtevnost jezika, oblika predstavitve vsebine in druge lastnosti odgovorov prilagodijo glede na posamezno uporabniško skupino. Izhodi morajo biti hkrati razumljivi in dostopni manj strokovnim uporabnikom ter dovolj natančni in strokovno ustrezni za zahtevnejše uporabnike.
Prijavitelj mora v ponudbi predstaviti načrt, kako bo rešitev upoštevala specifike različnih uporabniških skupin (npr. preko različnih načinov podajanja vsebin, nastavitev sistema ali ločenih modulov za posamezne tipe uporabnikov).

1.6. Dokumentacija in sledljivost modelov

Za vsak razviti ali prilagojeni VJM mora prijavitelj zagotoviti ustrezno tehnično dokumentacijo in navodila za uporabo. V dokumentaciji je treba zapisati podrobnosti razvoja modela (npr. arhitekturo, uporabljene modelne in hiperparametre, različice programske opreme), predvidene namene uporabe in omejitve modela, opis uporabljenih učnih podatkov (s povzetkom njihove vsebine in izvora) ter informacije o zmogljivosti in evalvacijskih rezultatih modela.
Takšna pregledna dokumentacija bo uporabnikom, nadaljnjim razvijalcem in nadzornim organom omogočila razumeti lastnosti modela ter preveriti njegovo skladnost z zahtevami (npr. glede avtorskih pravic, etičnih načel, varstva podatkov). Prijavitelj mora dokumentacijo pripraviti do zaključka projekta, v ponudbi pa naj predstavi njeno predvideno strukturo skladno z zahtevami (upoštevaje tudi zahteve poročanja po Aktu o UI, če je to relevantno).

1.7. Varna in učinkovita računska infrastruktura

VJM so računsko izredno zahtevni za izvajanje, zato mora prijavitelj zagotoviti ustrezno računsko infrastrukturo, na kateri bo rešitev delovala. Celotne operacije, povezane z VJM (hramba podatkov, učenje modelov, inferenca), je treba izvajati na način, skladen z nacionalnimi in evropskimi varnostnimi standardi ter s strateškimi usmeritvami (npr. Nacionalni program umetne inteligence 2030) predvideva vzpostavitev lastnih zmogljivosti na tem področju).

Praviloma to pomeni, da se infrastruktura nahaja v Sloveniji oziroma – če to ni mogoče – vsaj znotraj EU, pod pravnim okriljem, ki zagotavlja ustrezno varstvo podatkov in suverenost nad rešitvijo. Priporočljivo je, da projekti, financirani iz javnih sredstev, izkoristijo domačo računalniško infrastrukturo (bodisi javno bodisi zasebno), ki ima ustrezne varnostne certifikate. V kolikor prijavitelj izjemoma namerava gostovati rešitev izven Slovenije, mora to jasno utemeljiti in zagotoviti enakovreden nivo varnosti ter učinkovitosti, kot bi se pričakoval pri domači namestitvi. Ponudba mora

vključevati tudi storitev gostovanja rešitve za najmanj 3 leta po vzpostavitvi, razen če naročnik določi drugače.

1.8. Izbira osnovnega modela

Svetujemo sistematično ovrednotenje več možnih osnovnih VJM. Dobra izhodišča predstavljajo nacionalni odprti modeli (npr. v sklopu projekta *PoVeJMo*) ali večjezični modeli iz evropskih pobud (npr. *openEuroLLM*, *LLMs4EU*), saj so ti praviloma bolje usklajeni z evropskim jezikovnim, kulturnim in regulativnim okoljem. Končna izbira naj bo prilagojena konkretnemu primeru uporabe – npr. specializirani modeli za vprašanja in odgovore (angl. *QA*), modeli optimizirani za arhitekture z zunanjimi viri znanja (RAG) ali modeli za vektorske predstavitve besedil (angl. *embeddings*) in druge modalnosti. Pri odločitvi naj se upoštevajo ključni vidiki, kot so: večjezična podpora modela (na podlagi uveljavljenih evalvacijskih meril), licenčni pogoji in omejitve uporabe (za komercialno in javno rabo), učinkovitost izvajanja (npr. hitrost odziva, poraba pomnilnika), zrelost ekosistema orodij in skupnosti, arhitektura modela ter sestava in izvor podatkov, na katerih je bil model predhodno usposobljen.

1.9. Prilagajanje modela (*fine-tuning*)

Priporočamo prilagoditev izbranega osnovnega modela, kjer je to izvedljivo, saj s tem izboljšamo njegovo delovanje v ciljni domeni. Po izbiri osnovnega modela je treba določiti ustrezne metode prilagajanja (ki se lahko tudi kombinirajo). Med možnimi pristopi so zlasti: nadaljnje predhodno učenje modela na domenskih podatkih (dodatno učenje na obsežnem nizu kulturno-dediščinskih besedil za poglobitev znanja), nadzorovano učenje z navodili za specifično rabo (angl. *instruction tuning* na naboru vprašanj/odgovorov), domenska poravnava in vsebinska obogatitev modela, poravnava z uporabniškimi preferencami (npr. prilagoditev ustreznosti, sloga in uporabnosti odgovorov), prilagajanje za specifične naloge (angl. *downstream task fine-tuning*), ter drugi pristopi, kot so prenos znanja iz sorodnih jezikov ali domen (angl. *transfer learning*), destilacija znanja ter postopno oziroma kontinuirano učenje modela. Izbor metod naj upošteva časovne in infrastrukturne omejitve projekta ter razpoložljivost zadostnih količin kakovostnih podatkov za učenje.

1.10. Uporabniška izkušnja

Celotna uporabniška izkušnja naj bo konsistentna, sistem pa odziven. Poskrbite za kratke odzivne čase (zagotovite dovolj procesorske moči in optimizirano inferenco modela). Uporabniški vmesnik naj bo intuitiven in prilagojen različnim napravam (načela odzivnega dizajna – angl. *responsive design*). Priporočamo modularno, komponentno zasnovo uporabniškega vmesnika, da se omogoči ponovna uporaba posameznih funkcionalnosti, lažje prilagajanje sistema novim primerom uporabe ter učinkovito vzdrževanje in nadgrajevanje. Poseben poudarek naj bo na dostopnosti v skladu z vključujočim oblikovanjem – sistem naj zagotavlja podporo uporabnikom z različnimi oblikami oviranosti (npr. možnost pretvorbe besedila v govor in obratno), tako da bo rešitev dostopna najširšemu krogu uporabnikov.

1.11. Sinergije z obstoječimi pobudami

Izkoristite znanje in rezultate aktualnih nacionalnih in evropskih pobud s področja jezikovnih tehnologij. V Sloveniji poteka raziskovalni program *PoVeJMo* (Prilagodljivo obdelovanje naravnega jezika z velikimi jezikovnimi modeli), katerega cilj je razvoj odprtega VJM za slovenščino. Ta projekt sledi dobrim praksam razvoja VJM: izvaja kontroliran postopek priprave modela (popoln nadzor nad vhodnimi podatki in spoštovanje zasebnosti), model je odprto dostopen za različne namene (javne in zasebne), učenje modela pa je nadalje predhodno usmerjeno primarno na slovenski jezik za zagotovitev jezikovne avtentičnosti in boljšega razumevanja lokalnega konteksta. Na ravni EU poteka projekt *LLMs4EU* (Large Language Models for the EU), ki povezuje vodilne evropske institucije in podjetja z namenom razviti odprto dostopne modele in orodja za vse uradne jezike EU (vključno s slovenščino). Projekt *LLMs4EU* razvija rešitve za celoten proces razvoja VJM – od učenja modelov do zagotavljanja skladnosti z EU predpisi. Priporočamo, da spremljate rezultate teh pobud ter navežete stik s partnerji (Slovenija v navedenih projektih tudi sodeluje), saj boste tako imeli priložnost prvi dostopati do najsodobnejših rešitev.

1.12. Arhitektura sistema in integracija znanja

Za učinkovito uporabo VJM je poleg samega modela pomembna tudi zasnova celotnega sistema ter povezava z viri znanja s področja kulturne dediščine. Priporočamo razmislek o hibridnih arhitekturah, kot je RAG (Retrieval-Augmented Generation), ki združuje moč VJM z iskanjem po zunanjih podatkovnih zbirkah. Namenska implementacija RAG za specifični primer uporabe omogoča, da sistem ob uporabnikovem poizvedovanju poišče relevantne informacije v zbirki digitaliziranih virov (npr. muzejski opisi, arhivsko gradivo, članki) in jih posreduje modelu, ta pa nato generira odgovor na podlagi dejanskih, preverjenih podatkov. Tak pristop bistveno poveča zanesljivost in uporabnost rešitve – model ni omejen zgolj na statistično znanje iz faze učenja, temveč lahko v realnem času dostopa do točnih podatkov in navaja verodostojne vire. Poleg RAG lahko uporabo VJM nadgradite tudi z drugimi tehnikami, kot so izpopolnjeno oblikovanje vhodnih pozivov (angl. *prompt engineering*) ter multimodalni pristopi, kjer model poleg besedil obdeluje in generira tudi druge medije (slike, zvok, video ali 3D-vsebine). Katerakoli arhitekturna rešitev naj bo prilagojena temu, da se kontekst Slovenije in njene kulturne dediščine vedno upošteva pri delovanju modela.

1.13. Vzdrževanje in odgovornost

VJM sistem ni enkraten produkt, temveč zahteva stalno vzdrževanje in nadzor. Priporočamo, da že ob zasnovi sistema predvidite postopke za sprotno spremljanje delovanja modela v praksi (npr. beleženje in pregled primerov, ko model resno odpove ali uporabniki prijavijo problematične odgovore). Ponudnik oziroma razvijalec naj pripravi načrt za redno posodabljanje modela in podatkovne baze znanja. To vključuje nadgradnje modela z novimi podatki (da ostaja znanje ažurno) ter hitre popravke ob zaznanih napakah ali pristranskostih. Svetujemo, da uporabljate tehnologije in platforme, ki so odprtokodne ali široko podprte v industriji, s čimer se izognete odvisnosti od posameznega ponudnika na dolgi rok. Arhitektura rešitve naj bo zasnovana tako, da omogoča prenosljivost – v primeru zamenjave infrastrukture se

lahko sistem enostavno preseli, prav tako naj bo omogočena integracija modela v večje, nacionalne platforme v prihodnosti. Odgovorno upravljanje skozi celoten življenjski cikel modela je ključno za ohranjanje kakovosti rešitve in zaupanja uporabnikov.

1.14. Transparentnost in razložljivost

Spodbudite zaupanje uporabnikov v UI rešitev z visoko stopnjo transparentnosti in razložljivosti delovanja sistema. Uporabniki ne smejo sistema dojemati kot "črne skrinjice", temveč kot orodje, ki deluje v njihovo korist in pod nadzorom skrbnikov. Rešitev naj bo skladna z mednarodnimi etičnimi normami in zakonodajo, ki za področje UI zahteva varnost, pravičnost, preglednost in razložljivost delovanja. V praksi to pomeni, da uvedete ukrepe, kot so: jasna oznaka vseh UI-generiranih vsebin (uporabnik mora vedeti, da je odgovor pripravil model), možnost vpogleda v uporabljene vire podatkov pri posameznem odgovoru (npr. navajanje virov oziroma povezav na digitalne zbirke, od koder model črpa informacije – arhitektura RAG to že omogoča), ter priprava razumljivega opisa delovanja sistema za uporabnike. Slednji je lahko v obliki rubrike *»Kako deluje naš UI vodič?«*, kjer na poljuden način opišete, da model analizira uporabnikovo vprašanje, poišče ustrezne podatke v bazi in sestavi odgovor, pri čemer ima vgrajene varnostne filtre ipd. Varnostni vidik transparentnosti pomeni tudi, da se beleži in nadzira izhod modela – morebitne škodljive ali neprimerne odgovore je treba evidentirati in analizirati ter model naknadno prilagoditi, da se prepreči ponavljanje takih primerov (vzpostavitev povratne zanke za nenehno izboljšavo). Na ta način bo rešitev bolj varna, pravična in zaupanja vredna za uporabnike.

1.15. Varnost in stabilnost

Posvetite posebno pozornost varnosti in robustnosti sistema. Zagotovite tako kibernetsko varnost (zaščito pred vdori ali zlonamerno uporabo) kot vsebinsko varnost izhodov modela. Že med razvojem implementirajte mehanizme filtriranja in moderiranja neprimernih vsebin (vgrajeni filtri oz. modeli za zaznavo in blokado sovražnega, žaljivega ali neresničnega besedila). Posebej previdno obdelajte občutljive teme, ki bi lahko bile kontroverzne v kulturnem kontekstu (npr. narodnost, vera, zgodovinski konflikti ali politične teme), da model podaja točne in nepristranske informacije ter ne utrjuje stereotipov ali netočnih razlag. Sistem mora delovati stabilno tudi v neobičajnih ali mejnih situacijah – pred uvedbo testirajte obnašanje modela na robnih primerih in zagotovite, da v primeru, ko model odgovora ne ve, to jasno pove ali vljudno usmeri uporabnika drugam, namesto da bi si "izmislil" dejstva. Zanesljivo, varno in predvidljivo obnašanje sistema v vseh pogojih bo povečalo zaupanje uporabnikov in kakovost storitve.

2. Kakovostni podatki: tehnične smernice za zbiranje in upravljanje

Za razvoj domenskih VJM na področju kulturne dediščine, ki podpirajo slovenski jezik in so prilagojeni slovenskemu kulturnemu kontekstu, je potrebno zbrati in pripraviti zadostno količino kakovostnih, verodostojnih in raznolikih podatkov iz slovenskega okolja. Pri zbiranju večjih količin gradiva za inovativne rešitve digitalizacije kulturne

dediščine s pomočjo VJM je treba upoštevati določene standarde ter relevantno zakonodajo. V nadaljevanju so opredeljene ključne zahteve in priporočila za zbiranje in pripravo podatkov.

Priporočila:

2.1. Zanesljivost in raznolikost podatkovnih virov

Prijavitelji morajo pri izbiri virov za učenje ali prilagajanje VJM zagotoviti visoko zanesljivost, kakovost in ustrezno raznolikost podatkov. Viri morajo odražati dejansko jezikovno in vsebinsko realnost obravnavane domene.

- Prijavitelji so dolžni prednostno uporabljati avtorizirane, preverjene in strokovne vire, zlasti:
  - recenzirane znanstvene članke,
  - akademske monografije,
  - uradne publikacije,
  - muzejsko in drugo institucionalno dokumentacijo.

- Sekundarni oziroma kurirani viri, kot so:
  - publikacije brez znanstvene recenzije,
  - enciklopedije,
  - katalogi kulturne dediščine,
  - strokovni blogi uveljavljenih avtorjev,

  so dopustni le kot dopolnilni viri. Vsebine iz teh virov morajo biti ustrezno preverjene in kritično ovrednotene.

- Neuradni viri in spletna vsebina (npr. poljubni spletni blogi, forumi, vsebine na družbenih omrežjih) se štejejo za nizko zanesljive vire in se lahko vključijo le izjemoma, kadar ustreznejši viri niso na voljo. V takšnih primerih mora prijavitelj uvesti dodatne postopke preverjanja dejstev ter utemeljiti uporabo tovrstnih virov. Za presojo o kvaliteti teh vsebin je ključna navedba vira.

Prijavitelji morajo v ponudbi jasno opisati uporabljene vrste virov ter postopke za zagotavljanje njihove verodostojnosti, kakovosti in raznolikosti.

2.2. Čiščenje in standardizacija podatkov

Prijavitelj mora zagotoviti temeljito čiščenje in standardizacijo zbranih podatkov. Iz nabora je treba odstraniti morebitne napake, nedoslednosti ter podvojene ali nerelevantne vsebine (vključno z neustreznimi elementi, npr. ostanki HTML kode). Podatki morajo biti tudi uravnoteženi, da ne prevladujejo posamezni tipi virov ali stališč, ter pretvorjeni v enoten, strojno berljiv format.

Poseben poudarek je na jezikovni kakovosti – popravljanje pravopisnih, tipkarskih in tehničnih napak (npr. zaradi preloma) – ter na doslednem označevanju gradiva z ustreznimi metapodatki (npr. izvor, avtor, čas nastanka). Enotna struktura in bogati

metapodatki omogočajo boljšo sledljivost podatkov, lažje kasnejše iskanje in povezovanje gradiv ter uporabo metod, kot je npr. RAG.
Prijavitelj mora v ponudbi opisati postopek čiščenja, uravnoteženja in standardizacije podatkov ter predvideno shemo metapodatkov.

2.3. Varstvo osebnih podatkov

Prijavitelj mora zagotoviti, da zbiranje in uporaba gradiva potrebnega za VJM poteka v skladu s Splošno uredbo o varstvu podatkov (GDPR) in slovensko zakonodajo o varstvu osebnih podatkov. Pred vključitvijo kakršnih koli gradiv v učenje modela je treba iz njih odstraniti ali anonimizirati osebne in druge občutljive podatke, razen če za to obstaja izrecna pravna podlaga in pridobljena ustrezna soglasja za obdelavo teh podatkov v ta namen.

Priporočeno je avtomatizirano prečiščevanje osebnih imen, kontaktnih podatkov, naslovov in drugih potencialno občutljivih informacij v besedilnih virih, še posebej če bodo razviti modeli ali rešitve javno dostopni. Prijavitelj mora v ponudbi predložiti opis ukrepov, s katerimi bo zagotovil varstvo osebnih podatkov (npr. postopek anonimizacije gradiv).

2.4. Upravljanje pristranskosti in reprezentativnost podatkov

Prijavitelj mora analizirati zbrano gradivo za morebitne pristranskosti (angl. *bias*) in zagotoviti, da je nabor podatkov reprezentativen in uravnotežen glede na relevantne vidike obravnavane domene. V skladu s standardi upravljanja podatkov za visoko tvegane sisteme UI je treba dokumentirati predpostavke o tem, kaj podatki pokrivajo, oceniti zadostnost in pokritost nabora ter uvesti ukrepe za zaznavanje in zmanjševanje pristranskosti v podatkih (kot to predvideva Akt o UI).

Prijavitelj mora predložiti opis pristopa k odkrivanju in obravnavi pristranskosti v podatkih, vključno z morebitnimi načini za sprotno uravnoteženje nabora ter odstranjevanje ali zmanjševanje zaznanih pristranskosti.

2.5. Spoštovanje avtorskih pravic

Prijavitelj mora zagotoviti, da uporaba vseh gradiv pri razvoju VJM spoštuje avtorske pravice in pripadajoče licenčne pogoje. Za vsako uporabljeno gradivo je treba voditi evidenco vira ter njegove licence ali pravne podlage za uporabo. Kadar je le mogoče, naj se za učenje modelov uporabijo gradiva iz javne domene oziroma pod odprtimi licencami (npr. Creative Commons), ali pa gradiva, za katera ima prijavitelj ustrezna dovoljenja imetnikov pravic.

V primeru uporabe z avtorskimi pravicami zaščitenih del mora prijavitelj zagotoviti pravno podlago za njihovo obdelavo (npr. sklic na določbe 57.a in 57.b člena ZASP, ki v skladu z EU direktivo dovoljujeta besedilno in podatkovno rudarjenje zakonito dostopnih vsebin ob določenih omejitvah). V ponudbi mora prijavitelj navesti predvidene vrste gradiv in njihove licence oziroma pravne podlage, na podlagi katerih bodo podatki uporabljeni.

2.6. Dokumentacija in kakovostni nadzor

Priporočamo pripravo podatkovnega lista (angl. *datasheet*) za vsak zbrani korpus ali nabor podatkov, ki naj opisuje izvor, sestavo, obseg, licenco, postopek zbiranja/čiščenja ter znane omejitve nabora. Prav tako je smiselno redno izvajati nadzor kakovosti (ročni pregled vzorcev podatkov, avtomatizirano zbiranje statističnih kazalnikov o naboru, sprotno dodajanje novih relevantnih podatkov), da ostane podatkovna zbirka transparentna, ažurna in večkrat uporabna.

2.7. Podatkovna suverenost

Priporočamo pristop, ki ohranja slovensko kulturno in jezikovno identiteto ter digitalno suverenost. Model VJM naj bo treniran in prilagojen na način, ki daje prednost slovenskim vsebinam in znanju. Vključi naj se gradiva iz različnih regij, manjšin in zgodovinskih obdobij, da model ne bo favoriziral le najbolj znanih ali osrednjih del kulturne dediščine. S tem se zagotovi ohranjanje celovite kulturne raznolikosti v digitalnem okolju. Za nadzor nad uporabo in hrambo podatkov se priporoča uporaba nacionalne infrastrukture ali zasebnih oblačnih storitev pod slovensko jurisdikcijo.

2.8. Večkratna raba in odprtost podatkov

Priporočamo pripravo podatkov v odprtih formatih ter po načelih FAIR (Findable, Accessible, Interoperable, Reusable), da bodo nabori večkrat uporabni in deljivi med projekti. Kadar je mogoče, naj bodo zbrani podatki objavljeni javno pod ustreznimi licencami (posebej za projekte, financirane iz javnih sredstev), kar omogoča drugim ponovno uporabo gradiva za nove modele, analize ali aplikacije. Tako se izognemo podvajanju naporov, izboljšamo učinkovitost porabe javnih sredstev in spodbujamo kroženje znanja. Prav tako priporočamo upoštevanje standardov evropskih podatkovnih prostorov (»data spaces«) za kulturno dediščino (npr. priporočila iniciative *Europeana*) z namenom večje interoperabilnosti in vključitve v širše evropske okvire.

3. Infrastruktura

Zahtevana strežniška infrastruktura:

Izvajalec mora ob oddaji ponudbe razpolagati z ustreznim razvojnim in produkcijskim okoljem, ki omogoča stabilno, varno in učinkovito izvajanje UI sistemov. Obe okolji morata biti vzpostavljeni v konfiguraciji, kot je opredeljena v nadaljevanju, ter morata omogočati takojšnje testiranje, nameščanje in zanesljivo obratovanje ponujene rešitve. V kolikor izvajalec uporablja drugačno infrastrukturno rešitev od spodaj navedene, mora k ponudbi priložiti natančne tehnične specifikacije uporabljene opreme in programske podpore. Poleg tega mora z ustreznimi benchmark testi, meritvami zmogljivosti in analizo rezultatov dokazati, da je ponujena infrastruktura funkcionalno in zmogljivostno enakovredna zahtevani konfiguraciji.

Programska infrastruktura naj temelji na orkestracijski platformi Kubernetes (K8s), ki omogoča avtomatsko skaliranje, upravljanje delovnih obremenitev ter visoko razpoložljivost UI sistemov.

Za razvoj in evalvacijo modelov naj se uporablja ogrodje PyTorch, medtem ko je za učinkovito izvajanje velikih jezikovnih modelov integriran vLLM, ki omogoča optimizirano upravljanje pomnilnika na grafičnih procesorjih (GPU).

Vsi UI modeli in aplikacije naj bodo kontejnerizirani s pomočjo tehnologije Docker, kar zagotavlja dosledno delovanje v različnih okoljih. Infrastruktura naj podpira distribuirano učenje, samodejno skaliranje ter redundantne konfiguracije za zagotavljanje visoke zanesljivosti in odpornosti, kar je ključno za stabilno delovanje vladnih UI sistemov.

Priporočene specifikacije za eno UI vozlišče:

- 2× Intel Xeon ali AMD EPYC CPU (visoka frekvenca) s 32 jedri na CPU
- 512 GB RAM
- 2× NVMe SSD disk za operacijski sistem
- 1× dvovratna (dual-port) 25 GbE omrežna kartica
- 1× InfiniBand 200 GbE omrežna kartica
- Napajanje: 2× 3200 W redundantni napajalnik
- *GPU zahteve* (odvisne od potreb projekta), primeri konfiguracij:
  - 4× NVIDIA L40S (48 GB VRAM vsak) **ali** 2× NVIDIA H200 (141 GB VRAM vsak)
  - 8× NVIDIA H200 (141 GB VRAM vsak) *(4×2100 na vozlišče)*
  - 8× NVIDIA L40S (48 GB VRAM vsak) **ali** 4× NVIDIA H200 (141 GB VRAM vsak)

Priporočen strežnik za hrambo podatkov UI gruče:

- 2× Intel Xeon ali AMD EPYC CPU (32 jeder na CPU)
- 256 GB RAM
- 6× 4 TB SSD (RAID6 + 2 × rezervni disk)
- 1× dual-port 25 GbE omrežna kartica
- 1× InfiniBand 200 GbE omrežna kartica

Skupna infrastruktura

Virtualizacija

Virtualizacijska infrastruktura je pomembna za vse podporne storitve in aplikacije. Vključevati mora najmanj dva fizična strežnika (zaradi redundance), ki delujeta kot gostitelja za virtualne strežnike. Zaščita pred izpadom je obvezna.
Poleg gostiteljskih strežnikov je potreben tudi namenski strežnik za hrambo virtualnih strežnikov in podatkov, ki se na njih nahajajo. Priporočamo uporabo strežnika za blokovno shrambo.

Minimalne zahteve glede prostora za shranjevanje veljajo za osnovno delujočo konfiguracijo in se lahko prilagodijo specifičnim potrebam posameznega projekta. Poleg strojne opreme mora izvajalec zagotoviti tudi ustrezne licence za izbrano virtualizacijsko platformo.

Kubernetes (K8s) in porazdeljen sistem za objektno hrambo

Za Kubernetes (K8s) in storitve za porazdeljeno hrambo objektov (npr. MinIO, Ceph, ipd.) se uporablja skupna strežniška gruča. Zaradi redundance in osnovnih zmogljivostnih zahtev mora gruča obsegati najmanj 6 strežnikov – po 3 "master" in 3 "worker" vozlišča. Infrastruktura mora biti zasnovana modularno, z možnostjo enostavne razširitve skladno s prihodnjimi potrebami in projekcijami.
Ti strežniki poleg izvajanja storitev K8s hkrati služijo tudi kot shramba za podatke prek MinIO. Kot obvezna komponenta za upravljanje omrežja v gruči se uporablja **Calico**.

Priporočene specifikacije za eno vozlišče v gruči:

- 2× Intel Xeon ali AMD EPYC CPU (visoka frekvenca)
- 32 jeder na CPU
- 256 GB RAM
- 2× SSD za operacijski sistem
- 4× 4 TB NVMe disk (RAID6, prilagojeno predvideni potrebi po kapaciteti shrambe – D3)
- 1× dvovratna 25 GbE omrežna kartica

Omrežje

Omrežje mora biti vzpostavljeno z redundanco, kar pomeni, da morata biti zagotovljeni dve stikali, ki omogočata povezavo vsakega strežnika na obe stikali. Število vrat na stikalu mora biti usklajeno s številom strežnikov, ki bodo povezani, pri čemer se praviloma zahteva vsaj dve 16-portni stikali, ki omogočata 2× 25GbE povezljivost do vsakega strežnika.

Osnovne zahteve za podatkovni center

IT oprema mora biti nameščena v ustreznem podatkovnem centru, ki zagotavlja visoko razpoložljivost in ima v redundanci vse ključne sisteme. Podatkovni center mora izpolnjevati najmanj naslednje zahteve:

1. Podatkovni center ustrezne kapacitete (zadostna fizična in energetska zmogljivost za predvideno IT opremo in morebitne prihodnje razširitve)
2. Hlajenje v konfiguraciji N+1, z neodvisnimi hladilnimi enotami in nadzorom temperature ter vlage
3. Napajanje preko UPS naprav z redundanco 2N, ki omogoča neprekinjeno napajanje ob izpadu enega sistema
4. Rezervno napajanje z električnim agregatom, ki se samodejno vključi ob izpadu primarnega napajanja
5. Internetna povezljivost preko več (vsaj dveh) neodvisnih ponudnikov, z geografsko ločenimi optičnimi potmi

6. Implementirani sistemi za fizično varovanje, vključno z videonadzorom, elektronskim nadzorom pristopa in vodenjem dnevnikov dostopa
7. Alarmni sistem z več-conskimi senzorji gibanja, požara, izlitja vode in temperaturnih odstopanj
8. Zagotavljanje 24/7 prisotnosti dežurne ekipe za nujne intervencije v primeru izpadov ali okvar
9. Zagotavljanje SLA z najmanj 99,9 % razpoložljivosti za ključne storitve podatkovnega centra
10. Stalen (24/7) monitoring vseh IT in podpornih sistemov, z avtomatiziranim obveščanjem ob zaznanih anomalijah
11. Veljavni certifikati ISO 9001, ISO 14001 in ISO 27001 (ali enakovredni standardi)

Smernice so nastale v sklopu aktivnosti projekta LLMS4EU (https://www.alt-edic.eu/projects/llms4eu/), ki razvija vključujoče in večjezične modele generativne umetne inteligence za ključne evropske sektorje.

Za vse interesente je na voljo podporno mesto, kjer lahko postavite vprašanja: https://www.tourism4-0.org/podpora.

Objava: Januar 2026