

LJUDSKI NADZOR · ODGOVORNOST · RAZMJERNOST RIZIKU

UI pomaže ljudima. Odgovornost ostaje ljudska.

Načela odgovornog razvoja i korištenja umjetne inteligencije.

ID DOKUMENTA	VERZIJA	KLASIFIKACIJA	VLASNIK DOKUMENTA	CIKLUS REVIZIJE	OBJAVLJENO
ITO-TRUST-AI-001	1.0	JAVNO	Inženjering i informacijska sigurnost	Godišnje	Listopad 2026.

Odgovorno uvođenje umjetne inteligencije

Umjetna inteligencija može znatno unaprijediti način na koji organizacije obrađuju informacije, prepoznaju obrasce, automatiziraju repetitivne aktivnosti i podupiru operativno odlučivanje.

U javnom sektoru, javnoj sigurnosti i drugim okruženjima kritične važnosti te se mogućnosti moraju uvoditi odgovorno. Moguće koristi umjetne inteligencije treba razmatrati zajedno s pitanjima sigurnosti, privatnosti, odgovornosti, transparentnosti, pouzdanosti i ljudskog nadzora.

ITO umjetnoj inteligenciji pristupa kao **inženjerskoj sposobnosti** koja podupire definirane operativne ciljeve unutar odgovarajućih okvira upravljanja.

Ovaj dokument utvrđuje načela kojima se ITO vodi pri dizajnu, razvoju, integraciji ili implementaciji funkcionalnosti potpomognutih umjetnom inteligencijom.

RAZMATRA SE ZAJEDNO S KORISTIMA UMJETNE INTELIGENCIJE

- Sigurnost
- Privatnost
- Odgovornost
- Transparentnost
- Pouzdanost
- Ljudski nadzor

SADRŽAJ

01	Svrha	02
02	Naš pristup umjetnoj inteligenciji	03
03	Načela odgovorne UI	04
04	Okruženja kritične važnosti	05
05	Čovjek u petlji	06
06	UI nije automatski dokaz	07
07	Upravljanje životnim ciklusom UI	08
08	UI trećih strana	08
09	Odgovorna UI i regulativa	09
10	Naša predanost	09

KONTROLA DOKUMENTA

ID DOKUMENTA	ITO-TRUST-AI-001
VERZIJA	1.0
KLASIFIKACIJA	JAVNO
VLASNIK	Inženjering i informacijska sigurnost
CIKLUS REVIZIJE	Godišnje
OBJAVLJENO	Listopad 2026.

UI treba pomagati ljudima, a ne uklanjati odgovornost

ITO razvija tehnologiju koja ljudima i institucijama pomaže da učinkovitije obavljaju svoje odgovornosti.

Kada se funkcionalnosti potpomognute umjetnom inteligencijom koriste u radnim tokovima koji uključuju odluke sa značajnim posljedicama, odgovarajuću razinu ljudskog nadzora treba odrediti prema prirodi, riziku i pravnom kontekstu slučaja upotrebe.

TEHNOLOGIJA MOŽE POMOĆI U



AUTOMATIZACIJA I KONTROLA

Pitanje nije je li zadatak automatiziran.

Pitanje je ostaju li odluke s ozbiljnim posljedicama podložne **odgovarajućoj kontroli**.

Šest načela

01

Ljudski nadzor

Sustavi potpomognuti umjetnom inteligencijom trebaju zadržati odgovarajuću razinu ljudskog nadzora, ovisno o prirodi i mogućem utjecaju slučaja upotrebe. U radnim tokovima većeg utjecaja tehnologija treba podupirati ovlašteno osoblje, a ne prikrivati ili uklanjati institucionalnu odgovornost.

UI može podupirati prosudbu. Odgovornost ostaje ljudska i institucionalna.

02

Odgovornost

Svaka mogućnost umjetne inteligencije treba postojati unutar definiranog operativnog i upravljačkog konteksta. Institucije ostaju odgovorne za određivanje načina na koji se tehnologija odobrava i koristi u njihovim procesima, dok je ITO odgovoran za razvoj i održavanje tehnologije unutar dogovorenog opsega.

Odgovornost treba ostati prepoznatljiva čak i kada su pojedine aktivnosti automatizirane.

03

Transparentnost

Korisnici trebaju na odgovarajući način razumjeti kada funkcionalnost potpomognuta umjetnom inteligencijom sudjeluje u operativnom procesu. Gdje je to tehnički izvedivo i relevantno za slučaj upotrebe, sustavi trebaju pružiti informacije koje pomažu razumjeti rezultate umjetne inteligencije i njihovu ulogu u širem radnom toku.

04

Privatnost i upravljanje podacima

Umjetna inteligencija ne stvara novu osnovu za obradu informacija. Korištenje osobnih ili osjetljivih informacija u funkcionalnostima potpomognutima umjetnom inteligencijom mora ostati podložno mjerodavnoj pravnoj ovlasti, ograničenju svrhe, kontrolama pristupa i zahtjevima upravljanja podacima.

Tehnička mogućnost ne stvara pravnu ovlast.

05

Sigurnost i pouzdanost

Funkcionalnost umjetne inteligencije dio je ukupne sigurnosne arhitekture sustava u kojem radi. Relevantna razmatranja mogu uključivati zaštitu ulaznih i izlaznih podataka, kontrolu pristupa, cjelovitost modela i usluge, dostupnost sustava, sigurnost ovisnosti i nadzor.

Funkcionalnost potpomognutu umjetnom inteligencijom treba procjenjivati prema operativnim posljedicama netočnih, nedostupnih ili manipuliranih rezultata.

06

Razmjernost riziku

Ne stvaraju sve primjene umjetne inteligencije istu razinu rizika. Mogućnost umjetne inteligencije koja se koristi za kategorizaciju tehničkih zapisa ne zahtijeva ista razmatranja kao tehnologija koja se koristi u operativnom radnom toku javne sigurnosti.

Upravljanje, testiranje, dokumentacija i ljudski nadzor razmjerni su prirodi i mogućem utjecaju slučaja upotrebe umjetne inteligencije.

Pitanja prije uvođenja umjetne inteligencije

Korištenje umjetne inteligencije u javnom sektoru i javnoj sigurnosti zahtijeva dodatna razmatranja jer tehnologija može djelovati u procesima koji utječu na pojedince, institucionalne odluke ili operativne aktivnosti.

PRIJE UVOĐENJA FUNKCIONALNOSTI POTPOMOŽNUTE UMJETNOM INTELIGENCIJOM RELEVANTNA RAZMATRANJA MOGU UKLJUČIVATI

Svrha?

Koji problem mogućnost umjetne inteligencije treba riješiti?

Ovlast?

Je li predviđena obrada dopuštena unutar mjerodavnog institucionalnog i pravnog okvira?

Podaci?

Koje su informacije potrebne i kako se njima upravlja?

Utjecaj?

Što se može dogoditi ako je rezultat umjetne inteligencije netočan?

Nadzor?

Koja je razina ljudske provjere primjerena?

Sljedivost?

Može li se relevantna aktivnost sustava rekonstruirati kada je potrebno?

Sigurnost?

Kako se komponenta umjetne inteligencije štiti i nadzire?

Ljudski nadzor ugrađen u dizajn

Mehanizmi „čovjek u petlji” mogu biti važna zaštitna mjera kada umjetna inteligencija podupire radne tokove sa značajnim operativnim posljedicama ili posljedicama za pojedince.

OVISNO O SLUČAJU UPOTREBE, OVLAŠTENI KORISNIK MOŽE

01

Pregledati rezultat koji je generirala UI

02

Potvrditi identificirane informacije

03

Odobriti predloženu radnju

04

Odbaciti ili ispraviti rezultat

05

Donijeti konačnu operativnu odluku

Odgovarajući model ovisi o konkretnoj funkcionalnosti i riziku.

SMISLENA PROVJERA

ITO ne tretira ljudski nadzor kao kozmetički korak potvrde.

Kada je potrebna ljudska provjera, radni tok treba korisniku pružiti dovoljno informacija i ovlasti da smisleno procijeni rezultat potpomognut umjetnom inteligencijom.

Razlikovanje detekcije od utvrđivanja

Detekcije, klasifikacije, ocjene pouzdanosti ili preporuke koje generira umjetna inteligencija ne bi se automatski trebale smatrati neovisno provjerenim činjenicama.

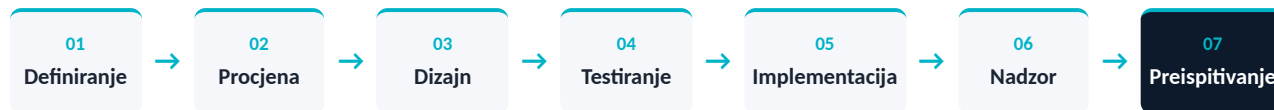
Njihov dokazni ili operativni značaj ovisi o tehnologiji, radnom toku, postupku provjere i mjerodavnom pravnom okviru.



Detekcija nije isto
što i **utvrđivanje**.

Odgovornost se nastavlja i nakon implementacije

Odgovorna umjetna inteligencija ne završava implementacijom modela ili usluge umjetne inteligencije. ITO-ov pristup uzima u obzir životni ciklus funkcionalnosti potpomognutih umjetnom inteligencijom:



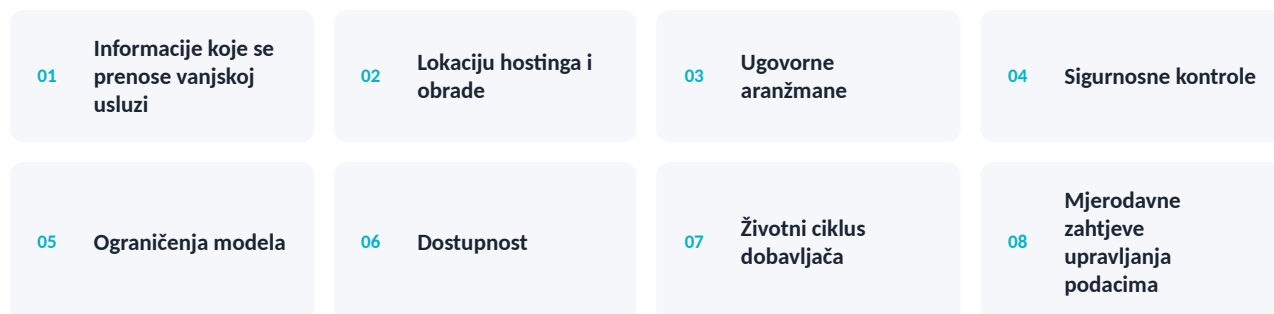
Ovisno o riziku i tehničkoj arhitekturi, aktivnosti životnog ciklusa mogu uključivati dokumentiranje predviđene svrhe, procjenu potreba za podacima, testiranje relevantnih karakteristika učinkovitosti, procjenu scenarija kvarova, kontrolu promjena pri implementaciji i preispitivanje ponašanja u radu.

08 • UI TREĆIH STRANA

Vanjski modeli i usluge umjetne inteligencije

ITO rješenja mogu uključivati ili integrirati tehnologije umjetne inteligencije koje pružaju treće strane. **Korištenje vanjske tehnologije umjetne inteligencije ne uklanja ITO-ovu odgovornost da procijeni njezinu prikladnost za predviđenu integraciju unutar opsega ITO-a.**

RELEVANTNA RAZMATRANJA MOGU UKLJUČIVATI



Posebno osjetljive institucionalne informacije ne bi se smjele prenositi vanjskim uslugama umjetne inteligencije bez odgovarajućih **tehničkih, ugovornih i upravljačkih zaštitnih mjera**.

Regulatorno okruženje koje se razvija

ITO prati razvoj upravljanja umjetnom inteligencijom, tehničkih standarda i regulatornih zahtjeva relevantnih za okruženja u kojima se njegova tehnologija koristi. Naš pristup odgovornoj umjetnoj inteligenciji može se pozivati na priznate okvire i načela, uključujući:

REFERENCIRANO

EU AI Act

Gdje je primjenjivo

NIST AI RMF

Okvir za upravljanje rizicima UI

OECD AI Principles

Međunarodna načela

ISO/IEC 42001

I srodne norme za upravljanje UI



Pozivanje na vanjske okvire ne predstavlja certifikaciju ni univerzalnu izjavu o usklađenosti. Primjenjivost ovisi o tehnologiji, slučaju upotrebe, jurisdikciji i kontekstu implementacije.

10 • NAŠA PREDANOST

Umjetna inteligencija stvara značajne prilike za unapređenje digitalne uprave i operacija kritične važnosti. Te prilike treba koristiti odgovorno. ITO je predan razvoju tehnologije potpomognute umjetnom inteligencijom uz odgovarajuće uvažavanje ljudskog nadzora, odgovornosti, privatnosti, sigurnosti, transparentnosti i rizika.

NIJE NAŠ CILJ

Automatizirati svaku odluku koju tehnologija čini mogućom.

NAŠ CILJ

Koristiti tehnologiju tamo gdje stvara **stvarnu vrijednost**, uz očuvanje **upravljanja i odgovornosti** koje zahtijeva okruženje u kojem djeluje.

Odgovorna umjetna inteligencija ne znači ograničavanje inovacija.
Znači inovacije kojima se može vjerovati.



ITO TRUST DOKUMENTI

Engineering Digital Trust.

POVEZANI DOKUMENTI

ITO-TRUST-SEC-001

ITO sigurnosni whitepaper

ITO-TRUST-PRV-001

ITO Privatnost i upravljanje podacima

ITO-TRUST-SDL-001

ITO Pregled sigurnog razvoja softvera

DOKUMENT

ITO Načela odgovorne umjetne inteligencije

ID • VERZIJA • KLASIFIKACIJA

ITO-TRUST-AI-001 • 1.0 • JAVNO

VLASNIK • REVIZIJA

Inženjering i informacijska sigurnost • Godišnje • Listopad 2026.

KONTAKT

security@ito.dev • ito.dev/en/trust-center

TVRTKA

IT Odjel Mostar d.o.o., Mostar, Bosna i Hercegovina