

UVOD

Dobrodošli na kurs **Privatnost u AI eri: Kako zaštititi svoje podatke?**

Veštačka inteligencija je deo našeg svakodnevnog života – koristimo je u poslu, obrazovanju, kreativnim procesima i donošenju odluka. Svaki put kada koristimo AI, razmenjujemo informacije. Ali koliko znamo o tome **gde ti podaci završavaju?**

- ♦ Da li AI alati skladište informacije koje unosimo?
- ♦ Da li ih dele sa trećim stranama?
- ♦ Kako možemo koristiti AI bez ugrožavanja privatnosti?

Ovo nisu hipotetička pitanja – **sve češće AI postaje deo kritičnih sistema, od poslovnih analiza do lične komunikacije.**

Zašto je ovo važno?

AI može značajno unaprediti efikasnost i produktivnost. Ali, ako ne razumemo **kako AI rukuje našim podacima**, možemo se suočiti sa ozbiljnim posledicama, kao što su:

- ⚠ **Curenje poverljivih informacija** – AI može skladištiti ili koristiti podatke bez naše kontrole.
- ⚠ **Pravni problemi** – Korišćenje AI alata u poslovne svrhe može biti suprotno regulativama poput GDPR-a.
- ⚠ **Manipulacija i zloupotreba** – AI može koristiti naše podatke za personalizovane reklame, pa čak i za kreiranje profila bez naše saglasnosti.

U ovom kursu naučićemo **kako da prepoznamo rizične AI alate, kako da zaštitimo podatke i kako da koristimo AI bezbedno.**

1. PRIVATNOST I ZAŠTITA PODATAKA U AI ALATIMA

Gde završavaju naši podaci?

Kada koristimo AI alate, retko postavljamo ključno pitanje:

👉 **Ko ima pristup informacijama koje unosimo?**

Zamislimo sledeću situaciju:

Pravni tim jedne kompanije koristi generativni AI za analizu ugovora. Oni unose interne podatke o klijentima, traže rezime ključnih stavki i predloge za izmene. Nekoliko meseci kasnije, slične formulacije pojavljuju se u drugom AI modelu. **Kako se to dogodilo?**

➡ Zato što nisu proverili **da li AI alat skladišti unete informacije i koristi ih za dalji razvoj modela.**

Sličan problem se dešava i sa pojedincima:

- 🔴 **Student** koristi AI za pisanje seminarskog rada, ne znajući da alat može zadržati njegov tekst i koristiti ga u budućnosti.
- 🔴 **Zaposleni** u banci koristi AI da napiše izveštaj, ali podaci o klijentima ostaju u sistemu alata i postaju dostupni drugim korisnicima.
- 🔴 **Kreativac** generiše sliku pomoću AI, ali kasnije saznaje da je AI model treniran na njegovim radovima **bez njegovog znanja.**

Dakle, **AI ne samo da koristi podatke koje unosimo – ponekad ih i zadržava.**

Kako AI prikuplja i obrađuje podatke?

AI sistemi koriste različite metode za učenje, a neki mogu **čuvati i obrađivati podatke** koje unosite.

Postoje **dve glavne vrste AI modela**:

✓ **Lokalni AI modeli** – Pokreću se **na vašem uređaju** i ne dele podatke sa eksternim serverima.

👉 Primer: privatno trenirani AI asistenti koji rade unutar zatvorene mreže.

⚠️ **Cloud AI modeli** – Obrada podataka se odvija **na udaljenim serverima**, što znači da podaci mogu biti **skladišteni, analizirani i korišćeni za dalji razvoj modela**.

👉 Primeri: **ChatGPT, Google Gemini, Microsoft Copilot.**

🔥 **Ključno pitanje:**

Da li alat eksplicitno navodi da NE skladišti vaše podatke?

Ako ne, **pretpostavite da ih može sačuvati.**

Koje informacije nikada ne bi trebalo unositi u AI alate?

Postoje podaci koje nikada ne biste smeli deliti sa AI alatima koji rade u **cloud-u**:

- ❌ **Lični podaci** (ime, prezime, adresa, JMBG, brojevi računa)
- ❌ **Osetljive poslovne informacije** (poverljive strategije, ugovori, intelektualna svojina)
- ❌ **Podaci za autentifikaciju** (lozinke, PIN kodovi, dvofaktorske verifikacije)
- ❌ **Informacije koje nisu vaša svojina** (poverljivi podaci o trećim stranama)

📌 **Primer iz prakse:**

Zaposleni u velikoj kompaniji koristili su ChatGPT za pisanje internih izveštaja. **Nisu znali da su neki uneti podaci korišćeni za unapređenje modela** – što znači da su potencijalno **mogli postati dostupni i drugim korisnicima**. Ovaj incident doveo je do toga da mnoge firme **zabrane korišćenje javnih AI sistema**.

♦ **Kako se zaštititi?**

- ✓ Koristite **AI alate koji imaju jasan data privacy policy**.
- ✓ Proverite da li alat **nudi opciju isključivanja čuvanja unetih podataka**.
- ✓ Kada je moguće, koristite **on-premise ili self-hosted AI rešenja**.
- ✓ Izbegavajte unos bilo kakvih **poverljivih podataka** u AI sisteme.

📌 **Zlatno pravilo:**

Pre nego što pitate AI za pomoć, zapitajte se – da li bih ovu informaciju podelio sa nepoznatom osobom na internetu?

2. KAKO AI ALATI KORISTE PODATKE – I KAKO SE ZAŠTITITI?

Kada koristimo AI alat, često unosimo informacije ne razmišljajući **šta se s njima dalje dešava**. Da li se podaci brišu nakon što AI odgovori? Da li ostaju u sistemu? Da li mogu završiti kod treće strane?

Kratak odgovor je: **Zависи od AI alata koji koristite.**

2.1. Kako AI modeli prikupljaju i obrađuju podatke?

RAZUMEVANJE LOKALNIH VS. CLOUD AI SISTEMA

Lokalni AI sistemi funkcionišu drugačije od cloud rešenja, i ta razlika je ključna za privatnost:

📌 Lokalni (on-device) AI:

✅ Kako radi?

- Ceo AI model se nalazi na vašem uređaju
- Podaci nikada ne napuštaju vaš sistem
- Procesiranje se vrši lokalno, koristeći vaše računarske resurse

✅ Prednosti za privatnost:

- Potpuna kontrola nad podacima
- Nema rizika od cloud curenja
- Radi čak i bez internet konekcije

⚠️ Ograničenja:

- Manji modeli zbog ograničenja uređaja
- Može biti sporiji od cloud rešenja
- Zahteva više resursa vašeg uređaja

📌 Cloud AI sistemi:

✅ Kako radi?

- AI model se nalazi na udaljenim serverima
- Vaši podaci se šalju na obradu
- Rezultati se vraćaju vašem uređaju

✅ Prednosti:

- Pristup moćnijim modelima
- Brža obrada
- Manje opterećenje vašeg uređaja

⚠️ Rizici za privatnost:

- Podaci putuju internetom
- Moguće skladištenje na serverima
- Potencijalni pristup trećih strana

♦ Kako izabrati pravo rešenje?

Za svakodnevne zadatke gde privatnost nije kritična:

✅ Cloud AI je prihvatljiv izbor

Za rad sa poverljivim podacima:

✅ Uvek birajte lokalna rešenja

Postoje **tri glavna načina** na koja AI alati koriste podatke:

1) AI alat ne čuva vaše podatke – Obrada je lokalna

- ✓ **Sigurna opcija** – podaci se obrađuju **samo na vašem uređaju** i ne dele se sa serverima.
- 👉 **Primeri:** Lokalni AI alati, offline prepoznavanje govora, self-hosted rešenja.

2 AI alat čuva podatke za interne analize

- ⚠️ **Umeren rizik** – podaci se koriste za poboljšanje modela, ali **nisu javno dostupni**.
- 👉 **Primeri:** Mnogi cloud AI alati tvrde da anonimizuju podatke, ali ih ipak koriste za unapređenje modela.

3 AI alat koristi vaše podatke za treniranje modela

- 🔴 **Najveći rizik** – Uneti podaci mogu postati deo budućih odgovora koje dobijaju i drugi korisnici.
 - 👉 **Primer:** Ako koristite besplatnu verziju ChatGPT-a, vaši podaci mogu biti korišćeni za poboljšanje modela.
 - 📌 **Kako da saznate šta se dešava s vašim podacima?**
 - 🔍 **Pogledajte politiku privatnosti AI alata.**
 - 🔍 **Ako alat ne navodi kako obrađuje podatke – pretpostavite da ih skladišti.**
 - 🔍 **Testirajte alat unosom lažnih informacija i proverite da li ih "pamti".**
-

2.2. Šta se dešava sa vašim podacima kada koristite AI?

Svaki put kada koristite AI alat, postoji mogućnost da se vaši podaci:

- ✓ **Skladište privremeno** – AI ih zadržava tokom sesije, ali ih briše nakon zatvaranja.
- ✓ **Skladište dugoročno** – AI ih koristi za unapređenje modela.
- ✓ **Prosleđuju trećim stranama** – Neki AI alati mogu deliti podatke sa partnerima ili oglašivačima.

📌 **Primer iz prakse:**

Zaposleni u jednoj banci koristili su AI chatbot za kreiranje izveštaja. Kasnije su otkrili da su se **njihovi podaci pojavili u AI odgovorima drugim korisnicima** jer alat nije imao zaštitu privatnosti.

- ✓ **Kako se zaštititi?**
 - ✓ **Ne unosite osetljive podatke** ako niste sigurni kako alat funkcioniše.
 - ✓ **Koristite AI alate sa opcijom "disable chat history".**
 - ✓ **Proverite da li AI alat omogućava brisanje podataka** na zahtev korisnika.
-

2.3. Kako proveriti koliko je AI alat siguran?

Ako koristite AI alat, postavite sebi ova pitanja:

- ✓ **Ko je razvio AI alat?**
- ✓ Ako alat dolazi od **poznate kompanije (Google, OpenAI, Microsoft, Meta, Apple)**, veća je verovatnoća da postoje jasne politike privatnosti.
- ⚠️ Ako alat dolazi od **nepoznatog izvora**, vaši podaci mogu biti zloupotrebljeni.

✓ **Da li alat ima opciju privatnog režima?**

✓ AI alati sa privatnim režimom ne skladište vaše podatke.

⚠ Ako alat ne nudi ovu opciju, podaci mogu biti zadržani.

✓ **Kako se alat finansira?**

✓ Ako je alat **besplatan**, postavite pitanje – **od čega zarađuje?**

⚠ Besplatni alati često koriste podatke korisnika za monetizaciju.

2.4. Kako koristiti AI alate bezbedno?

✓ **Šta možete da uradite odmah da zaštitite privatnost?**

✓ Proverite politiku privatnosti alata – ako je nejasna, **ne unosite osetljive podatke**.

✓ Ne koristite AI za poverljive informacije – pravne, medicinske, poslovne.

✓ Izbegavajte AI alate koji zahtevaju previše ličnih podataka.

✓ Koristite open-source AI alate kada je moguće – oni su transparentniji.

✓ Ako alat nudi privatni režim, uključite ga.

🔴 **Zlatno pravilo:**

Ako alat **ne nudi jasan uvid u to kako koristi podatke**, nemojte unositi informacije koje ne biste želeli da budu javno dostupne.

🔴 **Zaključak ovog segmenta:**

AI alati mogu biti korisni, ali vaša privatnost zavisi od vas.

- ♦ Ako ne znate gde završavaju vaši podaci, pretpostavite da nisu sigurni.
- ♦ Koristite alate koji omogućavaju brisanje podataka i imaju opciju privatnog režima.
- ♦ Ako AI alat ne navodi kako koristi podatke – budite oprezniji!

3. KAKO KOMBINOVATI AI I PRIVATNOST U SVAKODNEVNOM RADU?

Sada kada znamo **kako AI alati koriste podatke i kako se zaštititi**, vreme je da vidimo **kako AI možemo koristiti na bezbedan način u različitim oblastima**.

AI može biti veoma koristan, ali samo ako znamo kako da ga koristimo **bez ugrožavanja privatnosti**.

U ovom segmentu pokrivamo:

1 **AI u poslovnom okruženju** – Kako koristiti AI bez kompromitovanja poverljivih podataka.

2 **AI u svakodnevnom životu** – Kako zaštititi lične podatke prilikom korišćenja AI servisa (društvene mreže, pretraga, AI asistenti).

3 **Sigurna upotreba AI na mobilnim uređajima i aplikacijama** – Kako smanjiti rizik od praćenja i zloupotrebe podataka.

3.1. AI U POSLOVNOM OKRUŽENJU: KAKO KORISTITI AI BEZ RIZIKA?

Sve više kompanija koristi AI za analizu podataka, automatizaciju zadataka i komunikaciju sa klijentima. Ali, **nepažljivo korišćenje AI-a može dovesti do curenja poverljivih informacija.**

Primer rizika:

Zaposleni u jednoj IT firmi koristili su AI alat za pisanje izveštaja o klijentima, ne znajući da alat skladišti unete informacije. Nekoliko meseci kasnije, podaci iz tih izveštaja pojavili su se u drugim AI generisanim odgovorima.

Kako izbeći ovaj problem?

- ✓ **Nikada ne unosite osetljive poslovne podatke u AI alatke koje rade u cloud-u.**
- ✓ **Koristite on-premise AI rešenja** (AI koji se pokreće unutar firme).
- ✓ **Proverite politiku privatnosti AI alata pre korišćenja.**
- ✓ **Ukoliko koristite cloud AI, aktivirajte opciju "disable chat history".**

✓ **Sigurna upotreba AI u poslovanju:**

- ♦ Koristite AI za opšte zadatke (analiza tržišta, sumiranje tekstova), ali ne za poverljive informacije.
- ♦ Ako AI generiše izveštaje, uvek ih **ručno proverite** pre slanja klijentima.
- ♦ **Obučite zaposlene kako da koriste AI bezbedno** i definišite pravila unosa podataka.

3.2. AI U SVAKODNEVNOM ŽIVOTU: KAKO ŠTITITI LIČNE PODATKE?

AI koristimo svakodnevno – od društvenih mreža do virtuelnih asistenata. Ali, da li znamo **šta AI radi sa našim podacima?**

Gde sve AI može prikupiti podatke o nama?

- ♦ **Pretraga na internetu** – AI analizira šta tražimo i koristi to za personalizovane reklame.
- ♦ **Društvene mreže** – AI prati naše interakcije i kreira profile naših interesovanja.
- ♦ **Pametni asistenti (Alexa, Siri, Google Assistant)** – AI beleži naše glasovne komande i može ih skladištiti.
- ♦ **AI generisani preporučeni sadržaj** – AI odlučuje koje vesti i postove vidimo, što može oblikovati naše mišljenje.

Kako se zaštititi?

- ✓ **Koristite pretraživače sa zaštitom privatnosti.**
- ✓ **Isključite personalizovane reklame u podešavanjima Google i Facebook naloga.**
- ✓ **Pazite šta delite sa AI chatbotovima i digitalnim asistentima.**
- ✓ **Ako koristite AI u aplikacijama – proverite da li čuvaju vaše podatke.**

✓ **Pametna AI upotreba u svakodnevnom životu:**

- ♦ Koristite AI kao alat za poboljšanje produktivnosti, ali **ne delite previše informacija.**
- ♦ Ako koristite AI za pretragu – **pratite više izvora kako biste izbegli filter balon** (AI koji vam prikazuje samo ono sa čim se već slažete).
- ♦ **Koristite privatni režim ili alternative koje ne prate korisnike.**

3.3. SIGURNA UPOTREBA AI NA MOBILNIM UREĐAJIMA I APLIKACIJAMA

Mobilni telefoni su **glavna meta AI alata koji prate korisnike.** Mnoge aplikacije koriste AI za poboljšanje korisničkog iskustva, ali i za **prikupljanje podataka.**

📌 Kako AI aplikacije mogu ugroziti privatnost?

- ⚠️ Aplikacije koriste AI za **analizu glasovnih komandi i lokacije**.
- ⚠️ AI može pratiti **naše navike i pretrage** kako bi nam prikazao personalizovane reklame.
- ⚠️ Besplatne AI aplikacije često **koriste naše podatke kao izvor prihoda**.

🔥 Kako zaštititi privatnost na mobilnim uređajima?

- ✓ Proverite dozvole aplikacija – Da li aplikacija traži pristup mikrofONU, kameri ili lokaciji?
- ✓ Koristite VPN kada pretražujete osetljive informacije.
- ✓ Ako koristite AI aplikaciju, proverite da li omogućava isključivanje praćenja.
- ✓ Birajte AI aplikacije koje ne dele podatke sa trećim stranama.

✓ Sigurna AI upotreba na telefonima:

- ♦ Koristite AI samo kada je to neophodno i **izbegavajte AI asistente koji stalno slušaju**.
- ♦ Ako AI aplikacija traži previše dozvola – **verovatno koristi vaše podatke za analizu**.
- ♦ Redovno brišite istoriju pretrage i AI interakcija na svom telefonu.

📌 Zaključak ovog segmenta:

- ♦ AI može biti izuzetno koristan, ali samo ako ga koristimo odgovorno.
- ♦ Ne unosite privatne informacije u AI alatke bez jasnih pravila privatnosti.
- ♦ Ako alat nudi opciju privatnog režima – **uključite ga!**
- ♦ Koristite AI u obrazovanju i poslu, ali ne kao zamenu za sopstveno razmišljanje.

4. AI REGULATIVE I ZAŠTITA PRIVATNOSTI: GDPR, CCPA I DRUGI STANDARDI

Sada kada smo prošli kroz praktične savete za sigurnu upotrebu AI u svakodnevnom životu, vreme je da se pozabavimo **pravnim okvirima koji štite privatnost korisnika AI sistema**.

📌 Zašto su regulative važne?

- ✓ AI alati mogu biti moćni, ali ako nisu regulisani, mogu ugroziti prava korisnika.
- ✓ Mnoge zemlje su već usvojile zakone koji štite podatke od zloupotrebe.
- ✓ Razumevanje pravnih okvira pomaže korisnicima i kompanijama da koriste AI **na usklađen način**.

U ovom segmentu pokrivamo:

- 1) **Koji zakoni štite privatnost korisnika?**
- 2) **Šta AI alati moraju da rade da bi bili u skladu sa zakonom?**
- 3) **Kako da prepoznate da li AI alat krši vaša prava?**
- 4) **Primeri AI kršenja regulativa i pravne posledice.**

4.1. KOJI ZAKONI ŠTITE PRIVATNOST KORISNIKA?

📌 U zavisnosti od vaše lokacije, AI alati moraju poštovati različite regulative.

✓ GDPR (Evropska unija) – Najstrožiji zakon o zaštiti podataka u svetu

- ✓ AI alati moraju da **obaveste korisnike kako koriste njihove podatke**.
- ✓ Korisnici imaju pravo da **traže brisanje svojih podataka iz AI sistema** („pravo na zaborav“).
- ✓ Ako AI alat koristi podatke korisnika bez dozvole, može biti **kažnjen sa do 20 miliona evra ili 4% godišnjeg prihoda firme**.

- ✓ **CCPA (Kalifornija, SAD) – Pravo korisnika da znaju kako se njihovi podaci koriste**
 - ✓ AI alati moraju jasno navesti **kakve podatke prikupljaju i sa kim ih dele.**
 - ✓ Korisnici mogu tražiti **brisanje svojih podataka** iz AI sistema.
 - ✓ Ako AI alat prekrši zakon, kompanija može biti **tužena i kažnjena.**

 - ✓ **AI Act (Evropska unija) – Prvi zakon u svetu koji direktno reguliše AI**
 - ✓ Definiše, između ostalih, **visokorizične AI sisteme** koji moraju imati implementirane mehanizme **transparentnosti i bezbednosne mere.**
 - ✓ Zabranjuje AI sisteme koji narušavaju osnovna ljudska prava (npr. **masovni nadzor i manipulativni algoritmi**).
 - ✓ Uvodi **stroge kazne** za kompanije koje ne poštuju pravila.

 - ✓ **ISO 27001 – Standard za informacionu bezbednost**
 - ✓ AI alati koji imaju ISO 27001 sertifikat koriste **napredne mere zaštite podataka.**

 - 📌 **Šta ovo znači za korisnike?**
 - ♦ Ako koristite AI alat u EU, on mora biti u skladu sa GDPR-om.
 - ♦ Ako živite u Kaliforniji, imate pravo da znate **kako AI koristi vaše podatke.**
 - ♦ Ako AI alat nije usklađen sa ovim regulativama, **vaši podaci mogu biti ugroženi.**
-

4.2. ŠTA AI ALATI MORAJU DA RADE DA BI BILI U SKLADU SA ZAKONOM?

Ako kompanija razvija AI alat koji obrađuje podatke korisnika, **mora da ispuni određene zahteve.**

- 📌 **Ključni zahtevi regulativa:**
 - ✓ **Obaveštenje korisnika** – AI alati moraju **jasno navesti kako koriste podatke.**
 - ✓ **Pristanak korisnika** – AI alat ne sme koristiti podatke bez **izričite dozvole korisnika.**
 - ✓ **Mogućnost brisanja podataka** – Korisnici moraju imati opciju da **zatraže brisanje svojih podataka** („pravo na zaborav“).
 - ✓ **Sigurnosne mere** – AI alat mora imati **mere zaštite podataka od curenja ili zloupotrebe.**

 - 📌 **Kako prepoznati da li AI alat poštuje zakon?**
 - ✓ Ako alat jasno navodi **politiku privatnosti** i način korišćenja podataka – to je dobar znak.
 - ⚠️ Ako AI alat **ne pruža opciju brisanja podataka**, verovatno nije usklađen sa regulativama.
 - ⚠️ Ako alat koristi podatke **bez vašeg pristanka**, to je potencijalno kršenje zakona.

 - ✓ **Kako možete proveriti AI alat?**
 - ♦ Pročitajte **politiku privatnosti** – Ako nije jasno navedeno kako alat koristi podatke, budite oprezni.
 - ♦ Potražite **opcije privatnosti** – Da li alat nudi „disable chat history“ ili „delete my data“?
 - ♦ Ako sumnjate da AI alat krši vaše pravo na privatnost, možete se obratiti **regulatornim telima.**
-

4.3. KAKO DA PREPOZNATE DA LI AI ALAT KRŠI VAŠA PRAVA?

- 🔥 **Ako AI alat radi bilo šta od sledećeg, moguće je da krši vaša prava:**
- ✗ **Ne navodi kako koristi vaše podatke.**
- ✗ **Ne pruža opciju da obrišete svoje podatke.**
- ✗ **Prosleđuje vaše podatke trećim stranama bez vašeg znanja.**
- ✗ **Prikuplja više podataka nego što je neophodno.**
- ✗ **Ne omogućava da vidite koje podatke je prikupio o vama.**

Šta možete da uradite ako sumnjate da AI alat krši zakon?

- ◆ Proverite da li je AI alat u skladu sa GDPR-om, CCPA-om ili AI Act-om.
- ◆ Ako alat ne nudi opciju privatnog režima – ne unosite osetljive podatke.
- ◆ Ako AI alat ne odgovori na vaš zahtev za brisanje podataka, možete prijaviti kompaniju nadzornom organu u vašoj zemlji.

4.4. PRIMERI AI KRŠENJA REGULATIVA I PRAVNE POSLEDICE

Amazon Ring i masovni nadzor

Amazonove sigurnosne kamere **Ring** su tajno delile snimke sa policijom, bez saglasnosti korisnika. To je izazvalo debatu o **AI nadzoru i privatnosti**.

Zoom i AI transkripcija

Zoom je u svojoj politici privatnosti naveo da može koristiti **sadržaj video poziva za treniranje AI modela**, bez saglasnosti korisnika. Nakon javne reakcije, morali su da **izmene pravila**.

ChatGPT i problem sa privatnošću

OpenAI je morao da uvede opciju „disable chat history“ nakon što su korisnici **zahtevali veću kontrolu nad podacima**.

Zaključak:

- ◆ Ako AI alat ne poštuje regulative, vaši podaci mogu biti ugroženi.
- ◆ Velike kompanije su već bile sankcionisane zbog zloupotrebe AI podataka.
- ◆ Korisnici moraju biti informisani i zaštititi svoja prava pri korišćenju AI alata.

Zaključak ovog segmenta:

- ✓ AI regulative su ključne za zaštitu korisnika.
- ✓ Ako AI alat ne pruža opciju privatnog režima i brisanja podataka, verovatno krši standarde privatnosti.
- ✓ Uvek proverite AI alat pre nego što unesete lične ili poslovne podatke.

5. ZAKLJUČAK I KLJUČNE PREPORUKE

Sada kada smo prošli kroz sve ključne teme koje vam pomažu da **AI koristite na siguran i odgovoran način**, vreme je da sumiramo najvažnije tačke i pružimo **konkretno preporuke** koje možete primeniti odmah.

U ovom segmentu pokrivamo:

- 1 **Sažetak ključnih tačaka kursa**
- 2 **Zlatna pravila privatnosti u AI eri**
- 3 **Kako ostati informisan i koristiti AI odgovorno**

5.1. SAŽETAK KLJUČNIH TAČAKA

- ✓ AI alati prikupljaju podatke – znajte koje podatke delite i kako ih koristite.
- ✓ Ne unosite poverljive informacije u AI servise koji nemaju jasan režim privatnosti.

- ✓ Obratite pažnju na regulative – AI alati moraju biti u skladu sa GDPR-om, CCPA-om i AI Act-om.
- ✓ Koristite AI kao pomoćni alat, ali ne oslanjajte se slepo na njegove odgovore.
- ✓ Ako AI alat ne pruža opciju brisanja podataka, budite oprezni.
- ✓ AI u poslu, obrazovanju i svakodnevnom životu može biti koristan, ali samo uz pametnu upotrebu.



Ako niste sigurni u AI alat koji koristite – postavite sebi pitanje:

- ♦ Da li bih ove podatke podelio sa nepoznatom osobom na internetu?
- ♦ Ako ne znam gde moji podaci završavaju – da li bi trebalo da ih unesem?

5.2. ZLATNA PRAVILA PRIVATNOSTI U AI ERI



Pravila kojih se treba pridržavati svaki put kada koristite AI:

- ✓ Proverite politiku privatnosti pre korišćenja bilo kog AI alata.
- ✓ Ne unosite lične i poverljive podatke u AI chatbotove.
- ✓ Koristite AI alate koji nude opciju privatnog režima i ne skladište podatke.
- ✓ Ako koristite AI u poslu – koristite rešenja koja omogućavaju lokalnu upotrebu.
- ✓ Redovno ažurirajte podešavanja privatnosti na svojim nalozima i uređajima.
- ✓ Koristite pretraživače i AI alate sa ugrađenim opcijama zaštite privatnosti.
- ✓ Budite svesni AI regulativa i svojih prava kao korisnika.



Najvažnije: AI je moćan alat, ali vi ste ti koji kontrolišete kako ga koristite.

5.3. KAKO OSTATI INFORMISAN I KORISTITI AI ODGOVORNO?



Kako ostati u toku sa AI regulativama i bezbednosnim praksama?

- ♦ Pratite **promene u zakonodavstvu** (npr. GDPR, AI Act, CCPA).
- ♦ Pročitajte **politike privatnosti AI alata** koje koristite – one se stalno menjaju.
- ♦ Pratite istraživanja i članke o **AI bezbednosti i etici**.
- ♦ Proveravajte da li AI alati koje koristite imaju **sigurnosne sertifikate** (npr. ISO 27001).



Kako koristiti AI odgovorno u budućnosti?

- ♦ Postavljajte AI-u pametna pitanja – budite precizni i ne unosite osetljive podatke.
- ♦ AI neka vam pomaže, ali vi donosite odluke.
- ♦ Ne verujte slepo AI preporukama – proverite informacije pre nego što ih primenite.
- ♦ Ako AI alat ne pruža transparentne informacije o privatnosti – ne koristite ga za važne zadatke.

5.4. ZAVRŠNA MISAO



Veštačka inteligencija nije budućnost – ona je sadašnjost.

- ♦ Kako koristimo AI, zavisi isključivo od nas.
- ♦ Pametna i odgovorna upotreba AI alata znači da štitimo i sebe i druge.
- ♦ Prava privatnosti su važna – informišite se i koristite AI na siguran način.

 **Glavno pravilo:** AI može biti moćan saveznik, ali **vi ste oni koji kontrolišu kako će ga koristiti.**

 **Hvala vam što ste prošli kroz ovaj kurs! Nadam se da vam je bio koristan i da ćete sada AI koristiti sigurnije, pametnije i odgovornije.**