

# **Politika prihvatljive uporabe LLM sustava temeljenih na umjetnoj inteligenciji (AI) u školama**

**Varaždin, kolovoz 2026.**

## Sadržaj

|     |                                                                            |    |
|-----|----------------------------------------------------------------------------|----|
| 1.  | Uvod .....                                                                 | 3  |
| 2.  | Provjera informacija i činjenica .....                                     | 4  |
| 3.  | Zaštita poslovne tajne .....                                               | 5  |
| 4.  | Zaštita osobnih podataka .....                                             | 5  |
| 5.  | Zaštita poslovnih tajni, intelektualnog vlasništva i autorskih prava ..... | 7  |
| 6.  | Poštivanje ugovornih obveza povjerljivosti .....                           | 8  |
| 7.  | Generiranje ili provjera koda .....                                        | 8  |
| 8.  | Postupci selekcije i zapošljavanja .....                                   | 9  |
| 9.  | Opća pravila korištenja LLM modela .....                                   | 9  |
| 10. | Prihvatljiva rješenja za pravne subjekte kao korisnike .....               | 10 |
| 11. | Završne odredbe .....                                                      | 10 |

# Politika prihvatljive uporabe LLM sustava i usporedivih alata temeljenih na umjetnoj inteligenciji (AI) u školama

## 1. Uvod

Kao alat koji koristi jezični model umjetne inteligencije, LLM (eng: Large Language Model) sustav može predstavljati značajne izazove za škole u pogledu pravilne uporabe od strane zaposlenika i vanjskih suradnika u svrhu obavljanja radnih zadataka.

Kada zaposlenici i vanjski suradnici koriste LLM sustave za obradu informacija povezanih s poslovnim zadaćama, bez obzira jesu li samostalni (poput ChatGPT-a) ili integrirani u poslovne alate (poput Microsoft 365), **postoji rizik od netočnosti i pristranosti, kao i kršenja važećih propisa u području zaštite osobnih podataka, zaštite intelektualnog vlasništva i autorskog prava, kršenja ugovornih obveza s trećim stranama (primjerice čuvanja povjerljivosti) te otkrivanja poslovnih tajni škole i trećih strana.**

Kvaliteta informacija koje LLM sustavi pružaju jednaka je kvaliteti podataka na kojima su modeli trenirani. Unatoč tome što su LLM modeli trenirani na izrazito velikim količinama informacija dostupnih na internetu ili raznim repozitorijima (npr. GitHub, knjige, književnost, tehničke dokumentacije, jezične biblioteke, priručnici, baze znanja i sl.) kao i temeljem i informacija prikupljenih od strane svojih korisnika, postoje **neizbježne praznine u njihovim „bazama znanja“** zbog prirode umjetne inteligencije i ograničenosti skupova podataka na kojima su obučeni.

Pri tome svaki zaposlenik i vanjski suradnik mora biti upoznat da javno dostupni LLM sustavi u svojim politikama privatnosti ili u uvjetima korištenja u pravilu naglašavaju da prikupljaju cjelokupan sadržaj komunikacije i interakcije s korisnicima, sadržaj podijeljenih datoteka, uključujući i osobne podatke svih osoba podijeljenih u komunikaciji i u datotekama.

Sa svrhom upravljanja i minimiziranja prepoznatih rizika, škola donosi i redovito unaprjeđuje ovu Politiku prihvatljive uporabe LLM sustava i usporedivih alata temeljenih na umjetnoj inteligenciji (AI), koja utvrđuje pravila kada i u kojoj mjeri se takvi alati smiju koristiti za izvršavanje poslovnih zadataka zaposlenika i vanjskih suradnika.

Tekst ove politike na jednak se način primjenjuje na sve usporedive samostalne alate temeljene na umjetnoj inteligenciji (AI), od kojih su trenutno najzastupljeniji npr. OpenAI ChatGPT, Perplexity, Claude, Microsoft Copilot, X-ov Grok ili Google Gemini, kao što se primjenjuje i u slučajevima kada su isti integrirani u poslovne sustave (npr. Microsoft 365, chatbotovi, korisnička sučelja i sl.).

Ova se politika odnosi na sve zaposlenike i vanjske suradnike škola, a njene odredbe primjenjuju se na cjelokupni proces interakcije (prompting) s LLM sustavima, a ne isključivo na njihove krajnje rezultate.

Cilj je osigurati da se LLM sustavi koriste kao potpora ljudskom radu, uz strogo pridržavanje sigurnosnih pravila i pravnog okvira EU.

## 2. Provjera informacija i činjenica

Važno je imati na umu da nisu sve informacije na internetu točne, istinite i cjelovite, što može dovesti do problema i s točnošću, istinitošću, cjelovitošću i pravilnom primjenom informacija koje LLM sustavi pružaju. LLM sustavi generiraju rezultate na temelju statističke vjerojatnosti, što može dovesti do tzv. "halucinacija", odnosno, generiranja uvjerljivih, ali potpuno netočnih informacija.

Iz tog razloga postoji mogućnost da LLM sustavi generiraju netočne odgovore ako se oslanjaju na nepouz dane izvore, kao i na pogrešno koncipirane upite, činjenice ili temeljne pretpostavke koje unesu, odnosno, zadaju sami korisnici.

Rezultate koje generira LLM sustav potrebno je kritički provjeriti prije daljnje uporabe.

Ako se rezultat koristi u kontekstu koji se odnosi na pojedince, primjerice u radnim odnosima, financijskim uslugama, obrazovanju, zdravstvu, javnoj upravi ili drugim osjetljivim područjima, neprovjeren rezultat može dovesti do nepoštenog postupanja, diskriminacije ili druge štete za pojedinca.

Istovremeno, važno je istaknuti da se odgovori LLM sustava mogu mijenjati ovisno o povratnim informacijama korisnika pa i o samom ponavljanju upita ili prompta od strane istog korisnika.

Stoga, zbog prepoznatih pravnih i reputacijskih rizika, kada koriste LLM sustave za prikupljanje informacija u okviru poslovnih zadataka, zaposlenici i vanjski suradnici su obvezni pridržavati se sljedećih pravila:

- 1. Neovisna provjera činjenica:** Svaki podatak, tvrdnja ili izračun generiran putem LLM sustava mora se podvrgnuti neovisnoj provjeri putem službenih i pouzdanih izvora.
- 2. Provjera prije donošenja odluka:** Strogo je zabranjeno donošenje poslovnih, pravnih ili financijskih odluka isključivo na temelju neprovjerenih informacija iz LLM sustava.
- 3. Obavješćavanje nadređenih o netočnostima:** U slučaju uočavanja sustavnih pogrešaka, pristranosti ili necjelovitosti u odgovorima, zaposlenik je dužan odmah izvijestiti nadređenu osobu radi zaštite reputacije organizacije.
- 4. Transparentnost prema trećim stranama:** Pri distribuciji materijala izrađenih uz pomoć LLM sustava, zaposlenici moraju osigurati transparentnost i jasno navesti da je sadržaj generiran ili sukreiran od strane umjetne inteligencije i naznačiti izvor tako izrađenog teksta.

### 3. Zaštita poslovne tajne

Zaštita poslovne tajne ključan je element za poslovnu sigurnost i reputaciju. Zaposlenici i vanjski suradnici često su nositelji takvih informacija te mogu svjesno ili nehotice podijeliti vlasničke, povjerljive i/ili poslovne tajne tijekom komunikacije s LLM sustavom.

Potrebno je naglasiti da LLM sustavi mogu koristiti razgovore u svrhu treniranja vlastitog modela i poboljšanja svojih sustava te da "uče" iz svakog razgovora, što znači da podaci uneseni u upit postaju dio baze LLM sustava.

Zaposlenici i vanjski suradnici obvezni su sukladno zakonskim odredbama i školskim internim aktima štiti poslovne tajne i povjerljive poslovne informacije i **strogo se zabranjuje otkrivanje ili unošenje povjerljivih i strateških informacija i poslovnih tajni u LLM chatbotove.**

**Neovlašteno otkrivanje poslovne tajne i povjerljivih poslovnih informacija u bilo kojem obliku predstavlja povredu radne obveze.**

### 4. Zaštita osobnih podataka

LLM sustavi mogu biti korisni za izradu nacrtu tekstova, sažimanje općih informacija, prevođenje, jezično uređivanje, učenje ili generiranje ideja.

**Strogo je zabranjeno dijeljenje osobnih podataka zaposlenika organizacije i trećih osoba putem LLM sustava bez osiguranog valjanog pravnog temelja iz Opće uredbe o zaštiti podataka (GDPR), odgovarajućih informacija za ispitanike, sigurnosnih mjera, ugovorno uređenih odnosa i prethodne procjene rizika jer bi takvo postupanje moglo ozbiljno narušiti pravnu sigurnost i reputaciju škole.**

Stoga je prvi obvezni korak organizacije i svakog korisnika LLM sustava prije početka njegovog korištenja u poslovne svrhe provjera i prilagodba postavki privatnosti alata, osobito aktiviranja opcija:

- **isključenja korištenja unesenih podataka za treniranje ili poboljšanje AI modela,**
- **brisanja povijesti razgovora s LLM sustavom,**
- **korištenja privremenih razgovora i**
- **ograničavanja pohrane unesenog sadržaja tijekom razgovora s LLM sustavom.**

Osobni podaci uključuju sve informacije temeljem kojih se pojedinac može identificirati na izravan ili neizravan način, uključujući, ali ne ograničavajući se na fizičke, fiziološke, genetske, mentalne, ekonomske, kulturne ili socijalne značajke te identifikatore, mrežne identifikatore i podatke o lokaciji.

Posebno se mora voditi briga da se u LLM sustave ne unose podaci kao što su ime i prezime, OIB, adresa, broj telefona, adresa elektroničke pošte, identifikacijski brojevi, podaci o zdravlju, podaci o djeci, financijski podaci, podaci o zaposlenicima, klijentima, korisnicima, građanima ili poslovnim partnerima, kao ni druge informacije koje same za sebe ili u kombinaciji s drugim podacima mogu dovesti do identifikacije pojedinca.

Prije učitavanja dokumenata u LLM sustav potrebno je provjeriti sadržava li dokument osobne podatke, metapodatke, komentare, povijest izmjena, potpise, kontakt podatke, identifikacijske brojeve ili podatke trećih osoba. Ako takvi podaci nisu nužni za svrhu upita, potrebno ih je ukloniti ili koristiti anonimiziranu odnosno primjereno prilagođenu verziju dokumenta.

Pri tome nije dovoljno samo ukloniti ime, prezime ili adresu. Osoba se može identificirati i iz konteksta, primjerice kombinacijom radnog mjesta, datuma, lokacije, opisa događaja, broja predmeta, specifičnih okolnosti slučaja ili drugih detalja. Zato i opis stvarne pritužbe, radno-pravnog odnosa, zdravstvenog slučaja, korisničkog zahtjeva ili postupka pred tijelom javne vlasti može predstavljati osobni podatak ako se iz njega može zaključiti o kojoj je osobi riječ.

Ako je za postavljanje upita potrebno opisati određenu situaciju, treba koristiti općenite i neidentificirajuće opise. Umjesto stvarnih imena, adresa, datuma, brojeva predmeta ili drugih identifikatora trebaju se koristiti izrazi poput „osoba A”, „zaposlenik”, „korisnik”, „klijent”, „podnositelj zahtjeva” ili drugi neutralni opisi, pod uvjetom da se iz konteksta ipak ne može utvrditi o kojoj je osobi riječ.

**U radnom okruženju zaposlenici ne smiju samostalno unositi ničije osobne podatke u javno dostupne LLM sustave ako organizacija prethodno nije procijenila i odobrila uporabu takvog alata, a posebno je važno slijediti slijedeća pravila:**

- **Provjera metapodataka:** Prije učitavanja bilo kojeg dokumenta u LLM sustav, zaposlenik je dužan osigurati uklanjanje metapodataka, skrivenih komentara, potpisa i povijesti izmjena koji bi mogli otkriti identitet osoba ili interne procese.
- **Zabrana učitavanja baza:** Strogo je zabranjeno učitavanje tablica, baza podataka ili izvještaja koji sadrže podatke zaposlenika, klijenata ili poslovnih partnera.
- **Rizik kontekstualne identifikacije:** Uklanjanje imena i prezimena nije dovoljna mjera anonimizacije. Osoba se može identificirati iz konteksta (npr. spoj radnog mjesta, lokacije i opisa događaja). Za postavljanje upita moraju se koristiti isključivo neutralni opisi poput „osoba A” ili „korisnik”.

**Posebno rizičnom praksom smatra se učitavanje ili kopiranje tablica, baza podataka, izvještaja ili drugih strukturiranih dokumenata koji sadržavaju osobne podatke zaposlenika, klijenata, korisnika, građana, kandidata za posao ili drugih osoba u javno dostupne LLM sustave radi analize, sažimanja, izrade zaključaka, rangiranja, segmentacije ili donošenja preporuka.**

Takve tablice često sadržavaju veći broj osobnih podataka i omogućuju povezivanje različitih informacija o istoj osobi, primjerice imena i prezimena, kontakt podataka, radnog mjesta, plaće, ocjene rada, bolovanja, rezultata testiranja, financijskih pokazatelja, pritužbi, povijesti kupnje, korisničkih navika ili drugih podataka.

U određenim slučajevima takvi skupovi informacija mogu sadržavati i posebne kategorije osobnih podataka ili podatke koji omogućuju zaključivanje o zdravstvenom stanju, financijskoj situaciji, radnoj uspješnosti, ponašanju ili drugim obilježjima pojedinca.

Učitavanjem takvih tablica u LLM sustav može doći do neovlaštenog otkrivanja osobnih podataka, gubitka kontrole nad podacima, obrade za svrhe koje nisu bile predviđene, mogućeg prijenosa podataka izvan Europskog gospodarskog prostora, nejasnih rokova čuvanja te otežanog ostvarivanja prava ispitanika.

**Ako se LLM sustav koristi za “donošenje zaključaka” o osobama, primjerice o radnoj uspješnosti zaposlenika, ponašanju klijenata, riziku, pouzdanosti, prioritetima ili budućim odlukama, dodatno se otvaraju pitanja profiliranja, točnosti, poštenosti, transparentnosti i mogućih diskriminatornih učinaka te i samoj procjeni spada li tada LLM sustav u kategoriju visokorizičnog sustava prema Uredbi (EU) 2024/1689, odnosno Aktu o umjetnoj inteligenciji.**

**Stoga je zabranjeno unošenje tablica i baza podataka koje sadržavaju osobne podatke u javno dostupne LLM alate, osim ako je takva uporaba prethodno odobrena, pravno utemeljena, ugovorno uređena i tehnički zaštićena.**

**U slučaju sumnje na neovlašteno otkrivanje osobnih podataka ili bilo kakav sigurnosni incident povezan s AI sustavima u kojem su involvirani osobni podaci, zaposlenik je dužan odmah kontaktirati Službenika za zaštitu podataka (DPO) na email adresu: [bi@biconsult.hr](mailto:bi@biconsult.hr).**

Škola će poduzeti sve potrebne mjere kako bi se osiguralo da se sadržaj takve komunikacije u LLM sustavu i otkriveni osobni podaci nepovratno izbrišu kako bi se spriječila daljnja neovlaštena obrada osobnih podataka.

## **5. Zaštita poslovnih tajni, intelektualnog vlasništva i autorskih prava**

S obzirom na činjenicu da su LLM sustavi trenirani na velikim količinama informacija dostupnih na internetu i informacija prikupljenih od strane svojih korisnika, otvorena je mogućnost da bi zaposlenici ili vanjski suradnici tijekom komunikacije s LLM modelima mogli primati i koristiti informacije koje su zaštićene autorskim pravima i/ili predstavljaju intelektualno vlasništvo treće strane ili njihove poslovne tajne, čime se stvara pravni rizik za školu zbog neovlaštenog korištenja takvih zaštićenih informacija.

Zaposlenici i vanjski suradnici obvezni su sukladno zakonskim odredbama i internim aktima organizacije štiti intelektualno vlasništvo i autorska prava trećih strana te je strogo zabranjeno koristiti takve informacije dobivene od LLM modela na neovlašten način.

**U slučaju da zaposlenik ili vanjski suradnik sazna ili sumnja u neovlaštenu upotrebu zaštićenih dijela ili autorskih prava, trebao bi o tome odmah izvijestiti nadređene, koji poduzimaju odgovarajuće korake kako bi se zaštitila prava nositelja intelektualnog vlasništva.**

## 6. Poštivanje ugovornih obveza povjerljivosti

Tijekom korištenja LLM sustava zaposlenici i vanjski suradnici obvezni su voditi brigu da unutar komunikacije s LLM sustavima i postavljanja upita ili zahtjeva ni na koji način **ne otkrivaju niti dijele povjerljive informacije iz ugovora s trećim stranama, o njihovim klijentima ili ostalim stranama koje su predmetom ugovora s trećim stranama**. Zabranjeno je i svako dijeljenje informacija o tim stranama.

Zaposlenik ili vanjski suradnik koji unosi povjerljive informacije unutar komunikacije s LLM sustavima treba pažljivo razmotriti izvor tih informacija i provjeriti zabranjuje li ugovor s trećom stranom korištenje ili dijeljenje tih informacija.

**Otkrivanje povjerljivih informacija iz ugovora s trećim stranama predstavljalo bi kršenje povjerljivosti iz sklopljenih ugovora i škola je, kao ugovorna strana, odgovorna za povredu ugovornih obveza, dok je zaposlenik ili vanjski suradnik odgovoran zbog kršenja radne obveze i obveze očuvanja poslovne tajne i povjerljivosti.**

## 7. Generiranje ili provjera koda

LLM sustavi u izdvojenim se slučajevima koriste za generiranje jednostavnih kodnih isječaka i automatizaciju ponavljajućih zadataka u kodiranju, što povećava produktivnost programera.

**Zbog zaštite poslovnih tajni i intelektualnog vlasništva strogo je zabranjeno prenošenje bilo kojeg dijela koda u vlasništvu ili čijih je škola nositelj autorskih prava u LLM sustave bez prethodne suglasnosti ravnatelja.**

Kršenje ove obveze predstavlja kršenje radne obveze i obveze povjerljivosti.

Zaposlenici ili vanjski suradnici pri korištenju LLM sustava za generiranje softverskog koda ili drugog sadržaja moraju u cijelosti biti svjesni da taj sadržaj možda neće moći biti zaštićen autorskim pravom u pojedinim jurisdikcijama u svijetu, s obzirom na činjenicu da ga je stvorila umjetna inteligencija, a ne ljudsko biće. Također, zaposlenici ili vanjski suradnici moraju u cijelosti biti svjesni rizika da kod koji LLM sustav generira može naknadno biti zaštićen autorskim pravima trećih osoba.

Ako softver koji se dijeli s LLM modelom sadrži otvoreni kod, neophodno je prije dijeljenja provjeriti hoće li takvo dijeljenje biti smatrano distribucijom otvorenog koda, što može stvoriti pravne rizike.



## 8. Postupci selekcije i zapošljavanja

Selekcija i zapošljavanje su ključni procesi za škole i stoga je vrlo važno da se provode na transparentan i objektivan način. Uvođenjem umjetne inteligencije (AI) u ove procese dolazi do izričitih izazova koji bi mogli utjecati na konačni ishod procesa selekcije.

AI alati poput LLM sustava načelno mogu biti vrlo korisni u pomoći ljudskim resursima da učinkovitije obavljaju svoje poslove, ali u procesima selekcije i zapošljavanja donose visoke rizike za pojedince zbog rizika pristranosti, netransparentnosti, diskriminacije i kršenja načela jednakosti, posebice s obzirom da su AI alati skloni pristranosti ako nisu pravilno konfigurirani ili ako su trenirani na nepouzdanim podacima.

Uredba (EU) 2024/1689, odnosno, Akt o umjetnoj inteligenciji, u svom Prilogu III. takve sustave kategorizira kao visokorizične sustave umjetne inteligencije i utvrđuje niz zahtjevnih obveza usklađivanja prije početka njihove nabave i primjene.

**Zabranjuje se korištenje LLM sustava u postupcima selekcije i zapošljavanja, a u iznimnim slučajevima dozvolu za njegovo korištenje donosi ravnatelj uz obvezno prethodno savjetovanje sa Službenikom za zaštitu podataka.**

## 9. Opća pravila korištenja LLM modela

Zaposlenici i vanjski suradnici trebaju pravodobno obavijestiti školu o upotrebi LLM sustava u bilo kojoj poslovnoj svrhi uporabe.

Obveza uključuje jasno **označavanje sadržaja koji je generiran od strane LLM modela kako bi primatelji bili svjesni da su informacije generirane od strane umjetne inteligencije i da ih treba pažljivo provjeriti**. Obvezno je jasno identificiranje sadržaja koji je kreirao LLM model kada se dijeli s drugim osobama ili organizacijama, korisnicima, poslovnim suradnicima, javno ili unutar škole.

Dodatno, zaposlenici i vanjski suradnici su odgovorni za vođenje evidencije svih poslovnih svrha ili programskih alata ili korisničkih sučelja za koje su koristili LLM sustave sa svrhom izbjegavanja ili umanjivanja prepoznatih potencijalnih rizika, kako za školu, tako i za same zaposlenike i vanjske suradnike.

**Ovlašteni zaposlenici i vanjski suradnici smiju koristiti LLM sustave samo putem otvorenih službenih računa škola, isključivo za poslovne svrhe i za izvršavanje poslovnih zadaća s uključenim opcijama onemogućavanja zadržavanja povijesti razgovora s LLM sustavom i onemogućavanja treniranja LLM sustava na sadržaju korisnika.**

**Ovo se provodi radi omogućavanja prava na brisanje od strane škola i zabranu zadržavanja podijeljenih informacija unutar LLM sustava u skladu s njihovim politikama privatnosti i uvjetima korištenja.**

## 10. Prihvatljiva rješenja za pravne subjekte kao korisnike

Osim javno dostupnih tzv. potrošačkih verzija LLM sustava u kojima se zadržavanje sadržaja komunikacije jednostrano utvrđeno pravilima tih modela, pravnim subjektima na raspolaganju su posebna rješenja i verzije LLM sustava kojima se osigurava tražena zaštita podijeljenog sadržaja, osobnih podataka, poslovnih tajni i intelektualnog vlasništva i kojima se na ispravan način ispunjavaju zahtjevi iz članka 28. GDPR-a.

S obzirom na činjenicu da se škola nalazi u ulozi voditelja obrade osobnih podataka, a tvrtka koja upravlja LLM sustavom izvršiteljem obrade, ugovorni odnos mora uključivati i strože sigurnosne mjere zaštite, ograničavanje treniranja modela na sadržaju korisnika, mogućnost lokalne pohrane unutar EU/EGP i primjenu enkripcije u prijenosu i mirovanju.

Dodatno, ukoliko se radi o prijenosu osobnih podataka izvan EU/EGP u treće zemlje, takvi posebni LLM sustavi moraju jamčiti usklađenost s GDPR obvezama i u tom području primjenom Standardnih ugovornih klauzula Europske komisije iz 2021. godine.

## 11. Završne odredbe

Ova politika se redovito revidira prema novim tehnološkim i regulatornim promjenama.

Škola je dužna osigurati edukaciju zaposlenika, dokumentaciju i podršku za sigurno korištenje LLM sustava u okviru obveze osiguranja dostatne razine pismenosti sukladno članku 4. Akta o umjetnoj inteligenciji.

Kršenje ove politike može dovesti do disciplinskih mjera, uključujući raskid ugovora o radu ili suradnji.

Tekst ove Politike javno je dostupan i na stranicama:

<https://www.biconsult.hr/gdprcroatia/2639-politika-prihvatljive-uporabe-llm-sustava-temeljenih-na-umjetnoj-inteligenciji-ai-u-skolama>

Varaždin, 20. kolovoza 2026.

**Igor Barlek**

**Službenik za zaštitu podataka**



**IGOR BARLEK, CIPP/E**

Certified Information Privacy Professional  
Professional Data Protection Officer  
Profesionalni Službenik za zaštitu podataka  
IAPP member | EADPP member



**BI CONSULT d.o.o.**

Direktor  
Zagrebačka ulica 17, HR-42000 Varaždin  
F: +385 42 200 012 W: [www.biconsult.hr](http://www.biconsult.hr)  
M: +385 91 469 1122 E: [bi@biconsult.hr](mailto:bi@biconsult.hr)



**BI CONSULT d.o.o.**  
Zagrebačka ulica 17  
HR-42000 Varaždin

F: +385 42 200 012 W: [www.biconsult.hr](http://www.biconsult.hr)  
M: +385 91 469 1122 E: [bi@biconsult.hr](mailto:bi@biconsult.hr)  
GDPR Croatia Pages on LinkedIn & Facebook

