



Strasbourg, 25 Siječnja 2019.

T-PD(2019)01

**KONZULTATIVNI ODBOR  
KONVENCIJE ZA ZAŠTITU POJEDINACA  
S OBZIROM NA AUTOMATSKU OBRADU OSOBNIH PODATAKA  
(Konvencija 108)**

**SMJERNICE ZA UMJETNU INTELIGENCIJU I ZAŠTITU PODATAKA**

Directorate General of Human Rights and Rule of Law

Sustavi, softveri i uređaji temeljeni na umjetnoj inteligenciji ("AI") (u daljnjem tekstu AI aplikacije)<sup>1</sup> pružaju nova i vrijedna rješenja za rješavanje potreba i rješavanje izazova u raznim poljima, poput pametnih domova, pametnih gradova, industrijskog sektora, zdravstva i prevencije kriminala. AI aplikacije mogu predstavljati koristan alat pri donošenju odluka, posebno za potporu politikama utemeljenim na dokazima i inkluzivnoj politici. Kao što može biti slučaj s drugim tehnološkim inovacijama, ove primjene mogu imati negativne posljedice za pojedince i društvo. Kako bi to spriječile, stranke Konvencije 108 osigurat će i omogućiti razvoj i uporabu umjetne inteligencije poštujući prava na privatnost i zaštitu podataka (članak 8. Europske konvencije o ljudskim pravima), jačajući time ljudska prava i temeljne slobode.

Ove smjernice pružaju niz osnovnih mjera koje bi vlade, programeri umjetne inteligencije, proizvođači i pružatelji usluga trebali slijediti kako bi osigurali da aplikacije umjetne inteligencije ne narušavaju ljudsko dostojanstvo i ljudska prava i temeljne slobode svakog pojedinca, posebno u pogledu prava na zaštitu podataka.<sup>2</sup>

Ništa se u ovim Smjernicama neće tumačiti kao isključivanje ili ograničavanje odredbi Europske konvencije o ljudskim pravima i Konvencije 108. Ove smjernice također uzimaju u obzir nove zaštitne mjere modernizirane Konvencije 108 (češće se naziva „Konvencija 108+“).<sup>3</sup>

## I. Opće smjernice

1. Zaštita ljudskog dostojanstva i zaštita ljudskih prava i temeljnih sloboda, posebno pravo na zaštitu osobnih podataka, ključni su pri razvoju i usvajanju AI aplikacija koje mogu imati posljedice na pojedince i društvo. To je posebno važno kada se aplikacije AI koriste u procesima donošenja odluka.
2. Razvoj AI koji se oslanja na obradu osobnih podataka trebao bi se temeljiti na načelima Konvencije 108+. Ključni elementi ovog pristupa su: zakonitost, pravičnost, specifikacija svrhe, proporcionalnost obrade podataka, privatnost prema dizajnu i prema zadanim postavkama, odgovornost i dokazivanje poštivanja (odgovornosti), transparentnost, sigurnost podataka i upravljanje rizikom.
3. Pristup usmjeren na izbjegavanje i ublažavanje potencijalnih rizika obrade osobnih podataka nužan je element odgovorne inovacije na području AI.
4. U skladu sa smjernicama za procjenu rizika koje su date u Smjernicama o velikim podacima koje je Odbor za konvenciju 108 usvojio 2017.<sup>4</sup> godine, trebalo bi usvojiti širi pogled na moguće ishode obrade podataka. Ovo bi stajalište trebalo uzeti u obzir ne samo ljudska prava i temeljne slobode, već i funkcioniranje demokracija i socijalnih i etičkih vrijednosti.
5. AI prijave moraju u svakom trenutku u potpunosti poštivati prava subjekata podataka, posebno u svjetlu članka 9. Konvencije 108+.
6. AI aplikacije trebale bi omogućiti značajnu kontrolu subjekata podataka nad obradom podataka i povezanim učincima na pojedince i na društvo.

---

1. Sljedeća definicija umjetne inteligencije trenutno je dostupna na web stranici Vijeća Europe "<https://www.coe.int/en/web/human-rights-rule-of-law/artificial-intelligence/glossary>": „Skup znanosti, teorije i tehnike čija je svrha strojno reproducirati kognitivne sposobnosti ljudskog bića. Trenutni razvoj cilja, na primjer, na mogućnost da se stroju povjere složeni zadaci koji su prethodno dodijeljeni čovjeku.“

2. Ove smjernice slijede i nadovezuju se na Izvešće o umjetnoj inteligenciji („Umjetna inteligencija i zaštita podataka: izazovi i mogući lijekovi“) dostupno na: <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>

3. Izmjene i dopune Protokola CETS br. 223 uz Konvenciju o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka.

4. <https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0>

## II. Smjernice za programere, proizvođače i pružateljima usluga

1. Programeri umjetne inteligencije, proizvođači i pružatelji usluga trebali bi usvojiti vrijednosno orijentirani pristup u dizajniranju svojih proizvoda i usluga, u skladu s Konvencijom 108+, posebno s člankom 10.2, i drugim relevantnim instrumentima Vijeća Europe.
2. Programeri umjetne inteligencije, proizvođači i pružatelji usluga trebali bi procijeniti moguće negativne posljedice aplikacija umjetne inteligencije na ljudska prava i temeljne slobode i, uzimajući u obzir te posljedice, usvojiti pristup predostrožnosti na temelju odgovarajućih mjera za sprečavanje i ublažavanje rizika.
3. U svim fazama obrade, uključujući prikupljanje podataka, programeri umjetne inteligencije, proizvođači i pružatelji usluga trebali bi usvojiti pristup dizajna ljudskih prava i izbjegavati sve potencijalne pristranosti, uključujući nenamjerne ili skrivene, te rizik od diskriminacije ili drugih štetnih utjecaja na ljudska prava i temeljne slobode subjekata podataka.
4. Programeri umjetne inteligencije trebali bi kritički procijeniti kvalitetu, prirodu, podrijetlo i količinu korištenih osobnih podataka, smanjujući nepotrebne, suvišne ili marginalne podatke tijekom razvoja i faze osposobljavanja, a zatim nadzirati točnost modela dok se opskrbljuje novim podacima. Upotreba sintetičkih podataka<sup>5</sup> može se smatrati jednim od mogućih rješenja za smanjivanje količine osobnih podataka koje obrađuju AI aplikacije.
5. Rizik štetnih utjecaja na pojedince i društvo zbog dekontekstualiziranih podataka<sup>6</sup> i dekontekstualiziranih algoritamskih modela<sup>7</sup> treba na odgovarajući način razmotriti u razvoju i korištenju AI aplikacija.
6. Programeri, proizvođači i pružatelji usluga umjetne inteligencije potiču se na uspostavljanje i savjetovanje s neovisnim odborima stručnjaka iz različitih područja, kao i na suradnju s neovisnim akademskim institucijama, koje mogu doprinijeti dizajniranju temeljenih na ljudskim pravima i etički i socijalno orijentirane AI aplikacije i otkrivanje potencijalnih pristranosti. Takvi odbori mogu igrati posebno važnu ulogu u područjima u kojima transparentnost i angažman dionika mogu biti teži zbog konkurentskih interesa i prava, kao što je na području prediktivne pravde, prevencije i otkrivanja kriminala.
7. Treba poticati participativne oblike procjene rizika, temeljene na aktivnom angažmanu pojedinaca i skupina na koje potencijalno utječu prijave za umjetnu inteligenciju.
8. Svi proizvodi i usluge trebali bi biti dizajnirani na način koji osigurava pravo pojedinaca da ne podliježu odluci koja na njih značajno utječe, a temelji se samo na automatiziranoj obradi, bez uzimanja u obzir njihovih stavova.
9. Kako bi se povećalo povjerenje korisnika, programeri, proizvođači i pružatelji usluga umjetne inteligencije potiču se da dizajniraju svoje proizvode i usluge na način koji štiti slobodu izbora korisnika u vezi s korištenjem umjetne inteligencije, pružajući izvedive alternative aplikacijama za umjetnu inteligenciju.
10. Programeri umjetne inteligencije, proizvođači i pružatelji usluga trebali bi usvojiti oblike nadzora algoritma koji promiču odgovornost svih relevantnih dionika tijekom cijelog životnog ciklusa tih aplikacija, kako bi osigurali poštivanje zakona i načela o zaštiti podataka i ljudskih prava.
11. Subjekti podataka trebaju biti informirani ako komuniciraju s aplikacijom AI i imaju pravo dobiti informacije o obrazloženju temeljem operacija obrade podataka AI koje se na njih primjenjuju. To bi trebalo uključivati posljedice takvog obrazloženja.
12. Pravo na prigovor treba osigurati u vezi s obradom koja se temelji na tehnologijama koje utječu na mišljenja i osobni razvoj pojedinaca.

---

5. Sintetički podaci generiraju se iz podatkovnog modela izgrađenog na stvarnim podacima. Oni bi trebali predstavljati izvorne stvarne podatke. Pogledajte definiciju sintetičkih podataka u OECD. 'Glossary of Statistical Terms'. 2007. [http://ec.europa.eu/eurostat/ramon/coded\\_files/OECD\\_glossary\\_stat\\_terms.pdf](http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf) ("Pristup povjerljivosti gdje se umjesto širenja stvarnih podataka objavljuju sintetički podaci generirani iz jednog ili više populacijskih modela").

6. To je rizik zanemarivanja kontekstualnih informacija koje karakteriziraju specifične situacije u kojima se trebaju koristiti predložena rješenja temeljena na AI (umjetnoj inteligenciji)

7. To se događa kada se AI modeli, izvorno dizajnirani za određenu aplikaciju, koriste u drugom kontekstu ili u različite svrhe.

### III. Smjernice za zakonodavce i tvoraca politika

1. Poštivanje načela odgovornosti, usvajanje postupaka procjene rizika i primjena drugih prikladnih mjera, poput kodeksa ponašanja i mehanizama certificiranja, mogu povećati povjerenje u proizvode i usluge AI.
2. Ne dovodeći u pitanje povjerljivost zaštićenu zakonom, postupci javne nabave trebaju nametnuti programerima umjetnih inteligencija, proizvođačima i pružateljima usluga posebne dužnosti transparentnosti, prethodne procjene utjecaja obrade podataka na ljudska prava i temeljne slobode i oprez na potencijalne nepovoljne učinke i posljedice AI aplikacija (u daljnjem tekstu: praćenje algoritma).<sup>8</sup>
3. Nadzornim tijelima treba osigurati dovoljno resursa za potporu i nadgledanje programa praćenja algoritama programera AI, proizvođača i pružatelja usluga.
4. Pretjerano oslanjanje na rješenja koja pružaju aplikacije za umjetnu inteligenciju i strah od osporavanja odluka koje su predložene putem aplikacija za inteligenciju riskiraju promjenu autonomije ljudske intervencije u procesima donošenja odluka. Stoga treba očuvati ulogu ljudske intervencije u procesima donošenja odluka i slobodu donositelja ljudskih odluka da se ne oslanjaju na rezultat preporuka danih pomoću AI.
5. Programeri umjetne inteligencije, proizvođači i davatelji usluga trebali bi se obratiti nadzornim tijelima kada aplikacije AI mogu značajno utjecati na ljudska prava i temeljne slobode subjekata podataka.
6. Treba poticati suradnju između nadzornih tijela za zaštitu podataka i drugih tijela koja su nadležna za AI, kao što su: zaštita potrošača; konkurencija; antidiskriminacija; regulatorni organi i medijska regulatorna tijela.
7. Treba uspostaviti odgovarajuće mehanizme kako bi se osigurala neovisnost povjerenstava stručnjaka spomenutih u odjeljku II.6.
8. Pojedinci, skupine i drugi dionici trebali bi biti informirani i aktivno uključeni u raspravu o tome koju bi ulogu AI trebao igrati u oblikovanju društvene dinamike i u procesima donošenja odluka koji na njih utječu.
9. Donositelji politika trebali bi ulagati resurse u digitalnu pismenost i obrazovanje kako bi povećali svijest i razumijevanje subjekata podataka o aplikacijama AI i njihovim učincima. Oni bi također trebali poticati profesionalno osposobljavanje programera za umjetnu inteligenciju kako bi podigli svijest i razumijevanje potencijalnih učinaka umjetne inteligencije na pojedince i društvo. Trebali bi podržati istraživanje o umjetnoj umjetnosti usmjerenoj na ljudska prava.

---

8. O pojmu algoritamske budnosti, kao usvajanju odgovornosti, svijesti i praksi upravljanja rizicima koji se odnose na potencijalne štetne učinke i posljedice tijekom cijelog životnog ciklusa ovih aplikacija, vidi također 40. međunarodnu konferenciju povjerenika za zaštitu podataka i privatnosti, Izjavu o etici i zaštiti podataka u umjetnoj inteligenciji, vodeće načelo br. 2. Vidi također Izvještaj o umjetnoj inteligenciji (fusnota 2), odjeljak II.4