

Ugovor o obradi podataka o ličnosti

v0.1 nacrt · jul 2026

Ugovor o obradi podataka o ličnosti — Innovatica

NACRT — JOŠ NIJE ZA UPOTREBU SA KLIJENTIMA. Struktuiran prema članu 45 Zakona o zaštiti podataka o ličnosti ("ZZPL") i članu 28 GDPR-a. **Pre prve upotrebe sa klijentom mora ga pregledati kvalifikovani advokat sa licencom u Republici Srbiji** — naročito mehanizam međunarodnog prenosa u odeljku 7 i anekse. Stavke u uglastim zagradama su mesta za popunjavanje.

1. Strane, uloge i svrha

1.1. Ovaj Ugovor o obradi podataka o ličnosti ("**DPA**") je aneks ugovora o pružanju usluga ("**Ugovor**") između **Innovatica** [puno poslovno ime, matični broj, PIB, sedište] ("**Obrađivač**") i klijenta označenog u Ponudi ("**Rukovalac**").

1.2. Za podatke o ličnosti obrađivane u pružanju Usluga, Klijent postupa kao **rukovalac**, a Innovatica kao **obrađivač**, u smislu ZZPL i, kada je primenljivo, GDPR-a. Ovaj DPA je pisani ugovor iz člana 45 ZZPL (član 28 st. 3 GDPR).

1.3. Pojmovi koji ovde nisu definisani imaju značenje iz ZZPL; "podatak o ličnosti", "obrađa", "lice na koje se podaci odnose" i "povreda podataka o ličnosti" koriste se u tamo definisanom značenju.

2. Predmet, trajanje, priroda i svrha obrade

2.1. **Predmet i priroda:** hostovanje i vođenje ugovorenih Usluga — AI asistenata i chat agenata, veb aplikacija, prikupljanja i analize javno dostupnih podataka sa interneta, izveštavanja — uključujući čuvanje, pretraživanje, analizu, evidentiranje i prenos podataka o ličnosti opisanih u Aneksu 1.

2.2. **Svrha:** isporuka Usluga po Ugovoru; nijedna druga svrha. Obrađivač ne prodaje podatke o ličnosti i ne koristi ih za treniranje sopstvenih niti tuđih modela mašinskog učenja. Treći pružaoci AI modela korišćeni u trenutku upita ugovorno su obavezani da ne treniraju na dostavljenom sadržaju (Aneks 3).

2.3. **Trajanje:** period važenja Ugovora, uvećan za period gašenja iz odeljka 8.

2.4. **Vrste podataka i kategorije lica:** prema Aneksu 1, koji se popunjava po angažmanu.

3. Instrukcije

3.1. Obrađivač obrađuje podatke o ličnosti **isključivo po dokumentovanim instrukcijama Rukovaoca** — Ugovor, ovaj DPA, njegovi aneksi i konfiguracija Usluge zajedno čine trajne instrukcije — uključujući u pogledu prenosa u druge države, osim kada je obrada obavezna po propisu koji se

primenjuje na Obradivača; u tom slučaju Obradivač obaveštava Rukovaoca pre obrade, osim ako taj propis to zabranjuje.

3.2. Obradivač bez odlaganja obaveštava Rukovaoca ako smatra da instrukcija krši ZZPL, GDPR ili drugi propis o zaštiti podataka, i može zastati sa izvršenjem te instrukcije dok se ona ne potvrdi ili izmeni.

4. Poverljivost i osoblje

Lica ovlašćena za obradu podataka o ličnosti vezana su ugovornom ili zakonskom obavezom čuvanja poverljivosti, pristup im je ograničen na ono što njihova uloga zahteva i odgovarajuće su obučena za svoje dužnosti.

5. Bezbednost obrade

5.1. Uzimajući u obzir nivo tehnoloških dostignuća, troškove primene i prirodu, obim, okolnosti i svrhe obrade, kao i rizike za lica na koja se podaci odnose, Obradivač primenjuje odgovarajuće tehničke, organizacione i kadrovske mere iz člana 50 ZZPL (član 32 GDPR). Mere na snazi pri potpisivanju opisane su u **Aneksu 2**; Obradivač ih može unapređivati pod uslovom da se ukupni nivo bezbednosti ne smanjuje.

5.2. Obradivač pomaže Rukovaocu, u meri u kojoj je to moguće i uz razumnu naknadu Rukovaoca za značajan trud, u vezi sa: odgovaranjem na zahteve lica (pristup, ispravka, brisanje, ograničenje, prenosivost, prigovor); bezbednošću obrade; obaveštavanjem o povredama; procenama uticaja na zaštitu podataka i prethodnim konsultacijama sa nadzornim organom (Poverenikom).

6. Povrede podataka o ličnosti

Obradivač obaveštava Rukovaoca **bez nepotrebnog odlaganja nakon saznanja za povredu podataka o ličnosti** koja pogađa podatke Rukovaoca, a najkasnije u roku od [48] sati od saznanja, dostavljajući informacije potrebne Rukovaocu za njegove obaveze obaveštavanja (priroda povrede, kategorije i približan broj lica i zapisa, verovatne posledice, preduzete ili predložene mere), uz dopune kako informacije postaju dostupne. Obaveštavanje nadzornog organa i lica na koja se podaci odnose obaveza je Rukovaoca, osim ako se drugačije ne ugovori.

7. Podobrađivači i međunarodni prenos

7.1. Rukovalac daje **opštu saglasnost** za angažovanje podobrađivača navedenih u **Aneksu 3**. Obradivač obaveštava Rukovaoca o nameravanim dodavanjima ili zamenama najmanje [15] dana unapred; Rukovalac može pisanim putem prigovoriti iz razumnih razloga zaštite podataka, u kom slučaju strane traže rešenje, a ako ga ne nađu, Rukovalac može raskinuti pogođenu Uslugu.

7.2. Obradivač pisanim ugovorom nameće svakom podobrađivaču obaveze zaštite podataka koje nisu manje zaštitne od ovog DPA i ostaje u potpunosti odgovoran Rukovaocu za izvršenje obaveza podobrađivača.

7.3. **Mesto obrade.** Primarna obrada i čuvanje odvijaju se u Evropskoj uniji (Microsoft Azure, EU regioni — trenutno Sweden Central). Pojedini podobrađivači obrađuju ograničene podatke izvan Srbije i EU (Aneks 3 — npr. AI inferencija u Sjedinjenim Američkim Državama).

7.4. **Mehanizam prenosa.** Prenosi iz Srbije vrše se po čl. 63–65 ZZPL: u države sa liste država sa primerenim nivoom zaštite (koja obuhvata članice EEP i potpisnice Konvencije 108) bez dodatnih mera; u ostale — uz odgovarajuće mere zaštite: standardne ugovorne klauzule koje je usvojio Poverenik i/ili, za

podatke u GDPR režimu, EU standardne ugovorne klauzule ili primenljiv okvir primerenosti (npr. EU-US Data Privacy Framework za sertifikovane američke pružaoce) — **[advokat da potvrdi mehanizam po podobrađivaču i da li je potrebno odobrenje ili obaveštenje Poverenika]**.

8. Vraćanje i brisanje

Po prestanku ili isteku Ugovora Obradivač, po izboru Rukovaoca, briše ili vraća sve podatke o ličnosti obrađivane u ime Rukovaoca u roku od [30] dana i briše preostale kopije, osim ako propis koji se primenjuje na Obradivača zahteva dalje čuvanje. Brisanje iz šifrovanih rezervnih kopija odvija se po ciklusu rotacije iz Aneksa 2. Na zahtev, Obradivač pisanim putem potvrđuje brisanje.

9. Provere i informacije

- 9.1. Obradivač stavlja na raspolaganje informacije razumno potrebne za dokazivanje usklađenosti sa članom 45 ZZPL (član 28 GDPR) — opise mera, relevantne sertifikate podobrađivača i sažetke provera (za hyperscale podobrađivače, njihovi objavljeni sertifikati i izveštaji, npr. ISO 27001 / SOC 2, zamenjuju neposredan uvid).
- 9.2. Rukovalac može proveravati usklađenost — sam ili preko ovlašćenog proverivača vezanog poverljivošću — najviše [jednom godišnje], osim kada povreda ili nadzorni organ zahtevaju češće, uz najavu od [15] dana, u radno vreme, bez pristupa podacima drugih klijenata i o svom trošku.

10. Odgovornost, pravo i završne odredbe

- 10.1. Odgovornost po ovom DPA podleže ograničenjima iz Ugovora, osim kada prinudni propisi o zaštiti podataka određuju drugačije (uključujući čl. 86 ZZPL / čl. 82 GDPR o naknadi štete licima).
- 10.2. Na ovaj DPA primenjuje se pravo Republike Srbije; nadležnost kao u Ugovoru. U slučaju sukoba ovog DPA i Ugovora o pitanjima podataka o ličnosti, merodavan je DPA.
- 10.3. Sačinjen u srpskoj i engleskoj verziji; **merodavna je srpska verzija.**

Aneks 1 — Opis obrade (popunjava se po angažmanu)

Stavka	Opis
Kategorije lica	Krajnji korisnici AI asistenta / veb aplikacije Klijenta; zaposleni Klijenta (kontakt osobe); lica koja se pojavljuju u javno dostupnom veb sadržaju čije prikupljanje Klijent naloži
Vrste podataka o ličnosti	Pitanja i odgovori u chatu kako ih unesu krajnji korisnici (slobodan tekst — sadržaj zavisi od unosa); pseudonimizovani mrežni identifikatori (IP adresa se čuva isključivo kao heš sa solju); tehnički logovi (vreme, latencija, status); kontakt podaci zaposlenih Klijenta; podaci o ličnosti u prikupljenom javnom veb sadržaju [precizirati po angažmanu]
Posebne vrste podataka	Nisu predviđene. Krajnji korisnici mogu uneti posebne vrste podataka u polja slobodnog teksta; konfiguracija asistenta to destimuliše, a obaveštenje Klijenta krajnjim korisnicima to adresira. [Prilagoditi po angažmanu]
Radnje obrade	Prikupljanje, čuvanje, pretraživanje (uključujući vektorsku pretragu), analiza, evidentiranje, prenos pružaocima AI inferencije, brisanje

Stavka	Opis
Rok čuvanja	Chat logovi: za vreme trajanja Ugovora, osim ako Rukovalac naloži kraći rok [podrazumevano: do instrukcije]; prikupljeni veb korpusi: do zamene ili prestanka Ugovora; rezervne kopije: po rotaciji iz Aneksa 2

Aneks 2 — Tehničke i organizacione mere (sažetak)

- Hosting u EU regionima (Microsoft Azure, trenutno Sweden Central) za čuvanje, bazu i vektorsku pretragu; upravljane PaaS usluge sa fizičkom bezbednošću na strani provajdera (data centri sertifikovani po ISO 27001, SOC 2).
- Šifrovanje u prenosu (TLS) za sav saobraćaj usluga i API-je provajdera; šifrovanje u mirovanju na svim uslugama čuvanja i baze.
- Kontrola pristupa: database uloge razdvojene po okruženju; tajne aplikacija u secrets manageru (GitHub Actions secrets / Azure), nikada u kodu ili logovima; deployment identiteti sa najmanjim privilegijama (OIDC federacija, bez dugotrajnih ključeva).
- Pseudonimizacija: IP adrese krajnjih korisnika čuvaju se isključivo kao heš sa solju; bez reklamnih identifikatora i kolačića za praćenje u podrazumevanoj konfiguraciji platforme.
- Mrežna ograničenja baze (firewall allow-lista); javni endpointi sa ograničenjem učestalosti (burst / kontinuirano / dnevno) i globalnim budžetskim prekidima.
- Evidentiranje i nadzor: centralna log analitika i application insights sa operativnim čuvanjem od [30] dana; upozorenja o troškovima i otkazima na nadzirano sanduče.
- Razvojna disciplina: sve izmene infrastrukture i konfiguracije preko verzionisanih pull request-ova sa automatskom validacijom; bez ručnih izmena produkcije.
- Rezervne kopije: upravljane automatske kopije baze po konfiguraciji provajdera [čuvanje: podrazumevano 7 dana — prilagoditi ako se ugovori drugačije].

Aneks 3 — Odobreni podobrađivači

Podobrađivač	Uloga	Mesto obrade	Mera zaštite prenosa
Microsoft (Azure)	Cloud hosting: veb aplikacije, PostgreSQL, storage, embeddings (Azure AI Foundry), e-mail/komunikacioni servisi, nadzor	EU (Sweden Central; pojedine usluge West Europe)	Obrada u EU; Microsoft Products and Services DPA uklj. SCC
Anthropic	Inferencija velikih jezičkih modela za AI asistente (API; bez treniranja na dostavljenom sadržaju po komercijalnim uslovima)	Sjedinjene Američke Države	[Sertifikacija EU-US Data Privacy Framework i/ili SCC + srpski SCC ekvivalent — advokat da potvrdi]
GitHub (Microsoft)	Hosting izvornog koda i CI/CD za konfigurisane usluge Klijenta; čuvanje operativnih tajni	EU / SAD	Microsoft/GitHub DPA uklj. SCC — [advokat da potvrdi]
[Hetzner Online GmbH]	[Planirano: pomoćni compute za zakazane poslove prikupljanja podataka — dodaje se pri aktivaciji po tački 7.1]	Nemačka (EU)	Obrada u EU

