

IZJAVA O INFORMACIONOJ BEZBEDNOSTI I TEHNIČKIM MERAMA

Izjavu daje: AI ASISTENT FACTUM DOO Beograd (u daljem tekstu: Obradivač)

Proizvod: Factum (SaaS platforma)

Datum: 11.08.2026.

Platformu Factum razvija, hostuje i održava FAKTUM DOO Skopje, matično društvo Obradivača, koje Obradivač angažuje kao podobrađivača (tačka 10). Tehničke i organizacione mere opisane u ovoj Izjavi primenjuju se na platformu Factum, a odredbe koje se odnose na Obradivača shodno se primenjuju i na FAKTUM DOO Skopje kao podobrađivača.

1. Opis aplikacije

Factum je SaaS platforma za pravno istraživanje i izradu dokumenata, namenjena pravnim profesionalcima — advokatima, pravnim službama i internim legal/compliance timovima u institucijama. Platforma se koristi putem veb-pregledača, bez potrebe za instalacijom infrastrukture kod Korisnika, a dodatno i putem dodatka (add-in) za Microsoft Word.

Osnovne funkcionalnosti:

- **Pretraga i odgovori na osnovu konsolidovanog zakonodavstva:** Factum odgovara na pravna pitanja isključivo na osnovu konsolidovanih tekstova propisa, uz navođenje konkretnih izvora. Kada u bazi nema dovoljno osnova, platforma to navodi umesto da generiše odgovor.
- **Analiza i provera usklađenosti dokumenata:** Korisnik otprema dokument (uključujući obimne dokumente kao što su opšti uslovi, interni akti ili ugovori) i dobija proveru usklađenosti u odnosu na relevantne propise. Podržani su različiti formati, uključujući skenirane dokumente i slike.
- **Izrada i uređivanje dokumenata:** kreiranje novih i uređivanje postojećih dokumenata u aplikaciji i direktno u programu Microsoft Word, uz podršku za sopstvene šablone organizacije.
- **Organizovanje materijala (Folder / Agent Mode):** grupisanje otpremljenih datoteka u foldere, nad kojima Korisnik potom može da pretražuje i postavlja pitanja.

Sa aspekta obrade podataka, Korisnik unosi tekstualne zahteve i po potrebi otprema dokumente. Oni se obrađuju radi generisanja odgovora i čuvaju se u korisničkom profilu dok ih Korisnik ne izbriše.

Obim licence obuhvata pristup sa jednog korisničkog profila, sa jednog računara i sa više mobilnih ili tablet uređaja.

2. Upravljanje i sertifikacija (Governance)

Factum je posvećen najvišim standardima informacione bezbednosti. Sistem upravljanja bezbednošću informacija (ISMS) društva FAKTUM DOO Skopje, koje razvija i održava platformu, u potpunosti je implementiran i sertifikovan prema međunarodnom standardu:

- **Standard:** ISO/IEC 27001:2022
- **Broj sertifikata:** IC-IS-2511022
- **Izdavalac:** INTERCERT
- **Obim (scope):** dizajn, razvoj, podrška i održavanje digitalnih pravnih servisa.
- **Važenje:** do 03.11.2028. godine.

Ovaj sertifikat potvrđuje da FAKTUM DOO Skopje ima uspostavljene procese upravljanja rizikom, klasifikacije informacija i kontinuiranog unapređenja. Primenjuje se skup internih ISMS politika usklađenih sa standardom ISO/IEC 27001:2022, Opštom uredbom o zaštiti podataka (GDPR) i Zakonom o zaštiti podataka o ličnosti Republike Srbije (ZZPL). Svi zaposleni upoznati su sa svojim obavezama u pogledu zaštite podataka o ličnosti, potpisuju ugovore o poverljivosti (NDA) i dužni su da prijavljuju bezbednosne incidente koji uključuju podatke i sadržaj klijenata.

3. Arhitektura, fizička bezbednost i lokacija podataka

Platforma Factum koristi cloud infrastrukturu lociranu isključivo u Evropskoj uniji / Evropskom ekonomskom prostoru.

- **Hosting:** Hetzner Online GmbH (Falkenstein, Nemačka) — backend, frontend, self-hosted PostgreSQL i Elasticsearch; Google Cloud / Google Ireland Limited (EU/EEA regioni) — Firebase Authentication i Cloud Firestore, Google Cloud Storage, Google Cloud Run i Vertex AI.
- **Fizička zaštita:** data centri su zaštićeni fizičkim obezbeđenjem 24/7, biometrijskom kontrolom pristupa i video nadzorom i poseduju sopstvene ISO/IEC 27001 sertifikate.
- **Suverenitet podataka:** celokupan hosting, skladištenje i AI obrada sadržaja Korisnika odvijaju se isključivo na infrastrukturi lociranoj unutar EU/EEA. Pristup podacima imaju isključivo Obradivač (Republika Srbija) i FAKTUM DOO Skopje kao podobrađivač (Republika Severna Makedonija), u skladu sa tačkom 10.

4. Tehničke mere zaštite podataka

4.1. Enkripcija (šifrovanje)

- **Podaci u mirovanju (at-rest):** svi podaci sačuvani u bazama podataka i fajl-sistemima enkriptovani su industrijskim standardom AES-256.
- **Podaci u tranzitu (in-transit):** celokupna komunikacija između korisnika i servera odvija se enkriptovanim kanalom, uz korišćenje protokola TLS 1.3 (HTTPS). Za autentifikaciju servera koriste se digitalni sertifikati.

4.2. Kontrola pristupa i autentifikacija

- **Autentifikacija korisnika:** lozinka (čuva se isključivo u heširanom obliku, u skladu sa internom politikom lozinki) ili prijava putem Google naloga (OAuth 2.0), odnosno Microsoft Identity platforme.
- **Korporativni SSO (SAML / OIDC):** integracija sa identity provider-om Korisnika, uz centralizovano upravljanje pristupima. Dostupno u Enterprise paketu.
- **Dvofaktorska autentifikacija (2FA):** dostupna za korisničke naloge i obavezna za administrativne i infrastrukturne pristupe Obradivača. Dostupno u Enterprise paketu.
- **Minimalni pristup (least privilege):** osoblje Obradivača ima pristup samo onim podacima i funkcijama koji su strogo neophodni za obavljanje njegovih zadataka, što je regulisano internim politikama i ugovorima o poverljivosti (NDA).
- **Izolacija klijenata (tenant isolation):** logičko odvajanje između klijenata putem bezbednosnih pravila Firebase-a, tenant konteksta na nivou aplikacije pri svakom zahtevu ka bazi i izolacije objekata po tenantu uz IAM kontrole i vremenski ograničene potpisane URL adrese (signed URLs).

4.3. Mrežna izolacija

Kritični servisi (baze podataka, logovi, administrativni interfejsi) izolovani su od javnog interneta i dostupni isključivo putem privatne VPN mreže (Tailscale), uz stroga firewall pravila i segmentaciju mreže.

4.4. Monitoring i evidencija

- **Interna evidencija (svi paketi):** Obradivač održava centralizovanu evidenciju (logove) pristupa i aktivnosti u sistemu, uključujući vremensku oznaku, korisnika i tip akcije. Logovi su zaštićeni od neovlašćenog pristupa i izmena i čuvaju se standardno 6 meseci. Ovo je kontrola Obradivača u skladu sa tačkom 2.3 Aneksa br. 3 i primenjuje se nezavisno od izabranog paketa.
- **Pristup Korisnika evidenciji:** izdavanje izveštaja i izvoz logova o aktivnosti sopstvenih korisnika. Dostupno u Enterprise paketu.

5. Bezbedan razvoj i testiranje

Bezbednost aplikacije garantuje se sledećim kontrolama, koje čine deo ISO 27001 sistema:

- **Vulnerability Scanning:** redovno skeniranje biblioteka i komponenti trećih strana radi otkrivanja poznatih ranjivosti (CVE) pre svake nadogradnje.
- **Secure SDLC:** proces razvoja uključuje obavezan pregled koda (Code Review) i testiranje u izolovanom okruženju pre puštanja u produkciju.
- **Ažuriranje:** sve systemske komponente i serveri redovno se ažuriraju najnovijim bezbednosnim zakrpama (Patch Management).

6. Kontinuitet poslovanja i rezervne kopije (Backup)

- Automatski dnevni Hetzner snapshot-ovi servera koji hostuju PostgreSQL i backend.
- **Retencija rezervnih kopija:** pomični prozor od 7 dana.

7. Čuvanje i brisanje podataka

- **Dokumenti i datoteke u folderima:** čuvaju se dok ih Korisnik ne izbriše.
- **Datoteke priložene u razgovoru (chat):** automatski se brišu nakon 14 dana.
- **Istorija razgovora:** čuva se do brisanja od strane Korisnika; opciono je dostupno i lokalno čuvanje u veb-pregledaču korisnika.
- **Podaci o nalogu:** za vreme trajanja aktivnog ugovora; brišu se po prestanku usluge.
- **Operativni i bezbednosni logovi:** 6 meseci.
- **Rezervne kopije:** 7 dana, u skladu sa pravilima Firebase-a.
- Po raskidu ili isteku ugovora svi podaci o ličnosti obrađeni u ime Rukovaoca se, po njegovom izboru, brišu uz potvrdu ili mu se vraćaju, a postojeće kopije se brišu, osim ako zakonom nije predviđena obaveza njihovog čuvanja.

8. Upravljanje incidentima i kontakt tačke

Uspostavljena je procedura za detektovanje, prijavljivanje i rešavanje bezbednosnih incidenata.

- **Rok za obaveštavanje:** Obradivač će obavestiti Rukovaoca bez nepotrebnog odlaganja, a najkasnije u roku od 24 časa od saznanja o incidentu, u skladu sa ZZPL i GDPR-om.
- **Sadržaj obaveštenja:** priroda povrede, kategorije i približan broj lica na koja se podaci odnose, moguće posledice, kao i preduzete ili predložene mere za otklanjanje i ublažavanje posledica.
- **Lice za zaštitu podataka o ličnosti (DPO):** Metodij Ristomanov, dpo@factum.law
- **Kontakt osoba po Ugovoru:** Nenad Tomić, direktor, [e-mail]

9. Pomoć Rukovaocu i pravo na reviziju

- **Prava lica na koja se podaci odnose:** Obrađivač će pomoći Rukovaocu u ispunjavanju njegove obaveze da odgovori na zahteve za ostvarivanje prava lica na koja se podaci odnose (pristup, ispravka, brisanje, ograničenje, prenosivost i prigovor), bez nepotrebnog odlaganja po prijemu zahteva od Rukovaoca.
- **Procena uticaja (DPIA) i konsultacije:** Obrađivač će pomoći Rukovaocu pri izradi procene uticaja na zaštitu podataka o ličnosti i pri konsultacijama sa Poverenikom za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije. Dostupno u Enterprise paketu.
- **Dokumentacija i revizija:** Obrađivač stavlja Rukovaocu na raspolaganje sve informacije neophodne za dokazivanje usklađenosti i omogućava sprovođenje revizija i inspekcija u razumnim vremenskim intervalima, uz razumnu prethodnu najavu. Pri odlučivanju o obimu revizije Rukovalac može uzeti u obzir relevantne sertifikate Obrađivača. Dostupno u Enterprise paketu.

10. Podobrađivači

Obrađivač angažuje sledeće podobrađivače (svi infrastrukturni podobrađivači locirani su u EU/EEA):

Podobrađivač	Predmet obrade	Priroda obrade / mere	Trajanje
FAKTUM DOO Skopje (Skoplje, Severna Makedonija)	Razvoj, hosting i održavanje platforme Factum; tehnička podrška; celokupna obrada sadržaja Korisnika u ime Obrađivača	ISO/IEC 27001:2022 (sertifikat IC-IS-2511022, INTERCERT); pristup po principu najmanjih privilegija, 2FA, privatna VPN mreža, NDA; infrastruktura isključivo u EU/EEA	Period trajanja ugovora
Hetzner Online GmbH (Falkenstein, Nemačka, EU)	Hosting FastAPI backend-a i Next.js frontend-a, self-hosted PostgreSQL (folderi, vector embeddings, metapodaci), Elasticsearch (logovi), Hetzner Cloud Backup	IaaS / Cloud backend; TLS 1.3 u tranzitu, AES-256 u mirovanju; data centri sertifikovani prema standardu ISO 27001	Period trajanja ugovora
Google Cloud EMEA / Google Ireland Ltd. (EU/EEA region)	Promptovi, dokumenti i kontekst prosleđeni LLM modelu; generisani odgovori	Vertex AI (Gemini), Enterprise nivo sa eksplicitnim opt-out-om od treniranja i potvrđenim Zero Data Retention režimom (prolazna obrada, bez zadržavanja i bez logovanja za ljudski pregled); ISO 27001/27017/27018, SOC 2	Period trajanja ugovora
Google Ireland Limited (EU region)	Korisnički profil, istorija razgovora, reference izvora, sinhronizacija u realnom vremenu	Firebase Authentication + Cloud Firestore; ISO 27001/27017/27018, SOC 2	Period trajanja ugovora
Google Cloud EMEA (EU region)	Originalne datoteke otpremljene u okviru funkcije Folder/Agent Mode, kao i datoteke priložene u razgovoru (automatsko brisanje nakon 14 dana)	Google Cloud Storage; privatni bucket-i, IAM kontrole na nivou bucket-a, vremenski ograničene potpisane URL adrese (signed URLs), Object Versioning, AES-256	Period trajanja ugovora
Google Cloud EMEA (EU region)	Otpremljene datoteke pri konverziji/pretprocesiranju (Folder/Agent Mode)	Google Cloud Run — konverzija u PDF, kompresija i deljenje na stranice; privremena obrada, bez trajnog čuvanja	Period trajanja ugovora
Google Ireland Limited (EU region)	Samo informacije neophodne za autentifikaciju: e-mail adresa, ime, tehnički token	Google OAuth 2.0 — SSO „Sign in with Google“; federated identity	Period trajanja ugovora (samo pri korišćenju Google SSO)
Microsoft Ireland Operations Ltd. (EU region)	Samo informacije neophodne za autentifikaciju: e-mail adresa, ime, tehnički token	Microsoft Identity Platform — SSO autentifikacija (Sign in with Microsoft)	Period trajanja ugovora (samo pri korišćenju Microsoft SSO)

Podobrađivač	Predmet obrade	Priroda obrade / mere	Trajanje
Brevo SAS (Sendinblue) (Pariz, Francuska, EU)	Samo notifikacioni metapodaci (e-mail adresa, ime, tip notifikacije) — bez sadržaja koji unose korisnici	Transakcioni e-mail servis (potvrde registracije, sistemska obaveštenja); usklađen sa GDPR-om, ISO 27001	Period trajanja ugovora

- **Ugovori o obradi:** Obradivač ima potpisane ugovore o obradi podataka o ličnosti (DPA) sa svim navedenim podobrađivačima, kojima garantuje isti nivo zaštite kao onaj ugovoren sa Rukovaocem.
- **Promene liste:** o svakoj nameravanoj promeni dodavanjem ili zamenom podobrađivača Obradivač će pismeno obavestiti Rukovaoca najmanje 15 dana unapred, čime mu omogućava da ostvari svoje pravo na prigovor.
- **Prenos podataka:** celokupno skladištenje i obrada sadržaja Korisnika odvijaju se na infrastrukturi u EU/EEA. Pristup podacima iz Republike Severne Makedonije (FAKTUM DOO Skopje) vrši se u skladu sa ZZPL — Republika Severna Makedonija je potpisnica Konvencije 108 Saveta Evrope i nalazi se na listi država sa primerenim nivoom zaštite podataka o ličnosti utvrđenoj odlukom Vlade Republike Srbije. Drugi prenos podataka o ličnosti van EU/EEA se ne vrši.

11. AI obrada i zaštita sadržaja

- **Provajder:** jedini provajder velikog jezičkog modela je Google Cloud — Vertex AI (Gemini), u enterprise konfiguraciji, sa obradom u EU/EEA regionu.
- **Opt-out od treniranja:** Factum ima eksplicitni ugovorni opt-out od korišćenja podataka za treniranje modela.
- **Zero Data Retention (ZDR):** potvrđen ugovor o nultoj retenciji — promptovi i dokumenti obrađuju se prolazno, bez zadržavanja i bez logovanja za ljudski pregled (bez abuse monitoringa) od strane AI provajdera.
- **Bez treniranja:** ulazni i izlazni sadržaj Korisnika ne koristi se za treniranje, dodatno treniranje niti unapređenje modela Factum-a ili bilo koje treće strane.
- **Enkripcija:** celokupna komunikacija sa AI provajderom odvija se enkriptovanim kanalom (TLS 1.3).
- **Spoljni AI asistenti po izboru Korisnika:** ukoliko se Korisnik samostalno poveže sa spoljnim asistentom putem Factum MCP interfejsa (npr. Claude, ChatGPT, Microsoft Copilot), taj asistent deluje pod kontrolom i po ugovoru Korisnika i ne predstavlja podobrađivača Factum-a.

12. Dostupnost po paketima

Mere koje se odnose na infrastrukturu, enkripciju, izolaciju, rezervne kopije, podobrađivače i AI obradu primenjuju se na sve korisnike, nezavisno od izabranog paketa. Funkcionalnosti označene sa „Dostupno u Enterprise paketu“ predmet su posebnog ugovora ili aneksa.

Ugovor o obradi podataka o ličnosti: Standardne ugovorne klauzule (Prilog br. 1) sa Aneksima br. 1–3 imaju funkciju ugovora o obradi između Rukovaoca i Obradivača i čine sastavni deo Ugovora. Zaključenje posebnog samostalnog DPA sa dodatnim ili izmenjenim odredbama dostupno je u Enterprise paketu.

AI ASISTENT FACTUM DOO Beograd

Direktor,
Nenad Tomić