

ИЗЈАВА ЗА ИНФОРМАЦИСКА БЕЗБЕДНОСТ И ТЕХНИЧКИ МЕРКИ

Дадена од: Друштво за услуги ФАКТУМ ДОО Скопје

Производ: Factum (SaaS платформа)

Датум: 31.08.2026

1. Опис на апликацијата

Factum е SaaS платформа за правно истражување и изработка на документи, наменета за правни професионалци — адвокати, правни служби и internal legal / compliance тимови во институции. Платформата се користи преку веб-прелистувач, без потреба од инсталација на инфраструктура кај Корисникот, и дополнително преку додаток за Microsoft Word.

Основни функционалности:

- **Пребарување и одговори врз консолидирано законодавство:** Factum одговара на правни прашања исклучиво врз основа на консолидираните текстови на прописите, со наведување на конкретните извори. Кога нема доволна основа во базата, платформата го наведува тоа наместо да генерира одговор.
- **Анализа и проверка на усогласеност на документи:** Корисникот прикачува документ (вклучително обемни документи како општи услови, интерни акти или договори) и добива проверка на усогласеност во однос на релевантните прописи. Поддржани се различни формати, вклучително скенирани документи и слики.
- **Изработка и уредување на документи:** креирање нови и уредување на постојни документи во апликацијата и директно во Microsoft Word, со поддршка за сопствените шаблони на организацијата.
- **Организирање на материјали (Folder / Agent Mode):** групирање на прикачени датотеки во папки, врз кои Корисникот потоа може да пребарува и да поставува прашања.

Од аспект на обработката на податоци, Корисникот внесува текстуални барања и по потреба прикачува документи. Тие се обработуваат за да се генерира одговор и се чуваат во корисничкиот профил додека Корисникот не ги избрише.

Опсегот на лиценцата опфаќа пристап од еден кориснички профил, од еден компјутерски уред и повеќе мобилни или таблет уреди.

2. Управување и сертификација (Governance)

ФАКТУМ ДОО е посветена на највисоките стандарди за информациска безбедност. Системот за управување со безбедноста на информациите (ISMS) е целосно имплементиран и сертифициран според меѓународниот стандард:

- **Стандард:** ISO/IEC 27001:2022
- **Број на сертификат:** IC-IS-2511022
- **Издавач:** INTERCERT
- **Опсег:** Дизајн, развој, поддршка и одржување на дигитални правни сервиси.
- **Важност:** До 03.11.2028 година.

Овој сертификат потврдува дека Обработувачот има воспоставено процеси за управување со ризик, класификација на информации и континуирано подобрување. Обработувачот применува сет на интерни ISMS политики усогласени со ISO/IEC 27001:2022 и со Законот за заштита на личните податоци (ЗЗЛП). Сите вработени се запознаени со своите обврски во однос на заштитата на личните податоци, потпишуваат договори за доверливост (NDA) и се должни да ги пријавуваат безбедносните инциденти што ги вклучуваат податоците и содржината на клиентите.

3. Архитектура, физичка безбедност и локација на податоците

Платформата Factum користи „cloud“ инфраструктура лоцирана исклучиво во Европската Унија / Европскиот економски простор.

- **Хостирање:** Hetzner Online GmbH (Falkenstein, Германија) — бекенд, фронтенд, self-hosted PostgreSQL и Elasticsearch; Google Cloud / Google Ireland Limited (ЕУ/ЕЕА региони) — Firebase Authentication и Cloud Firestore, Google Cloud Storage, Google Cloud Run и Vertex AI.
- **Физичка заштита:** Дата центрите се заштитени со 24/7 физичко обезбедување, биометриска контрола на пристап и видео надзор, и поседуваат сопствени ISO/IEC 27001 сертификати.
- **Суверенитет на податоци:** Целото хостирање, складирање и AI обработка на содржината на Корисникот се одвиваат исклучиво на инфраструктура лоцирана во рамки на ЕУ/ЕЕА. Не се врши пренос на лични податоци во трети земји.

4. Технички мерки за заштита на податоците

4.1. Енкрипција (шифрирање)

- **Податоци во мирување (at-rest):** Сите податоци зачувани во базите на податоци и фајл-системите се енкриптирани со индустрискиот стандард AES-256.
- **Податоци во транзит (in-transit):** Целата комуникација помеѓу корисникот и серверите се одвива преку енкриптиран канал користејќи TLS 1.3 (HTTPS). За автентикација на серверите се користат дигитални сертификати.

4.2. Контрола на пристап и автентикација

- **Автентикација на корисници:** лозинка (се чува исклучиво во хеширана форма, согласно интерната Password Policy) или најава преку Google (OAuth 2.0) и Microsoft Identity Platform.
- **Корпоративен SSO (SAML / OIDC):** интеграција со identity provider на Корисникот, со централизирано управување со пристапите. Достапно во Enterprise пакетот.
- **Двофакторска автентикација (2FA):** достапна за корисничките сметки и задолжителна за административните и инфраструктурните пристапи на Обработувачот. Достапно во Enterprise пакетот.
- **Минимален пристап (least privilege):** персоналот на Обработувачот има пристап само до оние податоци и функции кои се строго неопходни за извршување на неговите задачи, регулирано преку интерни политики и договори за доверливост (NDA).
- **Изолација на клиенти (tenant isolation):** логичко одвојување меѓу клиентите преку безбедносни правила на Firebase, контекст на тенант на ниво на апликација при секое барање до базата, и изолација на објектите по тенант со IAM контроли и временски ограничени потпишани URL-адреси (signed URLs).

4.3. Мрежна изолација

Критичните сервиси (бази на податоци, логови, административни интерфејси) се изолирани од јавниот интернет и достапни исклучиво преку приватна VPN мрежа (Tailscale), со строги firewall правила и сегментација на мрежата.

4.4. Мониторинг и евиденција

- **Внатрешна евиденција (сите пакети):** Обработувачот одржува централизирана евиденција (логови) за пристапите и активностите во системот, вклучувајќи временска ознака, корисник и тип на акција. Логовите се заштитени од неовластен пристап и од модификација и се чуваат стандардно 6 месеци. Ова е контрола на Обработувачот согласно Анекс бр.3 точка 2.3 и се применува независно од избраниот пакет.
- **Пристап на Корисникот до евиденцијата:** издавање на извештаи и извоз на логови за активноста на сопствените корисници. Достапно во Enterprise пакетот.

5. Безбеден развој и тестирање

Безбедноста на апликацијата се гарантира преку следните контроли како дел од ISO 27001 системот:

- **Vulnerability Scanning:** редовно скенирање на библиотеките и компонентите од трети страни за познати ранливости (CVEs) пред секоја надградба.
- **Secure SDLC:** процесот на развој вклучува задолжителен преглед на кодот (Code Review) и тестирање во изолирана околина пред пуштање во продукција.
- **Ажурирање:** сите системски компоненти и сервери редовно се ажурираат со најновите безбедносни закрпи (Patch Management).

6. Континуитет на работењето и резервни копии (Backup)

- Автоматски дневни Hetzner server snapshots на серверите кои го хостираат PostgreSQL и бекендот.
- **Ретенција на резервните копии:** подвижен прозорец од 7 дена.

7. Чување и бришење на податоците

- **Документи и датотеки во папки:** се чуваат додека Корисникот не ги избрише.
- **Датотеки прикачени во разговор (чат):** автоматски се бришат по 14 дена.
- **Историја на разговори:** се чува до бришење од страна на Корисникот; опционално е достапно и локално чување во прелистувачот на корисникот.
- **Податоци за сметката:** за времетраењето на активниот договор; се бришат по престанокот на услугата.
- **Оперативни и безбедносни логови:** 6 месеци.
- **Резервни копии:** 7 дена, согласно правилата на Firebase.
- По раскинување или истек на договорот сите лични податоци обработени во име на Контролорот, по негов избор, се бришат со потврда или му се враќаат, а постојните копии се бришат, освен ако со закон не е утврдено нивно чување.

8. Управување со инциденти и контакт точки

Воспоставена е процедура за детектирање, пријавување и решавање на безбедносни инциденти.

- **Рок за известување:** Обработувачот ќе го извести Контролорот без непотребно одложување, а најдоцна во рок од 24 часа од сознанието за инцидентот, согласно ЗЗЛП и GDPR.
- **Содржина на известувањето:** природа на нарушувањето, категории и приближен број на засегнати субјекти на лични податоци, можни последици, како и преземени или предложени мерки за справување и ублажување.
- **Официер за заштита на лични податоци (ДПО):** Методиј Ристоманов, dpo@factum.law

- **Контакт лице по Договорот:** Димитар Чуковски, управител, info@factum.mk

9. Помош на Контролорот и право на ревизија

- **Права на субјектите:** Обработувачот ќе му помогне на Контролорот во исполнувањето на неговите обврски да одговори на барањата за остварување на правата на субјектите на лични податоци (пристап, исправка, бришење, ограничување, преносливост и приговор), без непотребно одложување по приемот на барањето од Контролорот.
- **ПВЗЛП и консултации:** Обработувачот ќе му помогне на Контролорот при изработка на проценка на влијанието врз заштитата на личните податоци и при консултации со Агенцијата за заштита на личните податоци (АЗЛП). Достапно во Enterprise пакетот.
- **Документација и ревизија:** Обработувачот му ги става на располагање на Контролорот сите информации потребни за докажување усогласеност и дозволува спроведување на ревизии и инспекции во разумни временски интервали, со разумно претходно најавување. При одлучувањето за обемот на ревизијата, Контролорот може да ги земе предвид релевантните сертификати на Обработувачот. Достапно во Enterprise пакетот.

10. Под-обработувачи

Обработувачот ги ангажира следните под-обработувачи, сите лоцирани во ЕУ/ЕЕА:

Под-обработувач	Предмет	Природа / мерки	Времетраење
Hetzner Online GmbH (Falkenstein, Германија, ЕУ)	Хостинг на FastAPI бекенд и Next.js фронтенд, self-hosted PostgreSQL (папки, vector embeddings, метаподатоци), Elasticsearch (логови), Hetzner Cloud Backup	IaaS / Cloud backend; TLS 1.3 во транзит, AES-256 во мирување; дата центри сертифицирани по ISO 27001	Период на договорот
Google Cloud EMEA / Google Ireland Ltd. (ЕУ/ЕЕА регион)	Промптови, документи и контекст препратени до LLM моделот; генерирани одговори	Vertex AI (Gemini), Enterprise tier со експлицитен opt-out од тренирање и потврден Zero Data Retention (преодна обработка, без задржување и без логирање за човечки преглед); ISO 27001/27017/27018, SOC 2	Период на договорот
Google Ireland Limited (ЕУ регион)	Кориснички профил, историја на разговори, референци на извори, real-time sync	Firebase Authentication + Cloud Firestore; ISO 27001/27017/27018, SOC 2	Период на договорот
Google Cloud EMEA (ЕУ регион)	Оригинални фајлови отпемени во функцијата Folder/Agent Mode, како и датотеки прикачени во разговор (автоматско бришење по 14 дена)	Google Cloud Storage; приватни bucket-и, IAM на bucket-ниво, временски ограничени потпишани URL-адреси (signed URLs), Object Versioning, AES-256	Период на договорот
Google Cloud EMEA (ЕУ регион)	Прикачени датотеки при конверзија/претпроцесирање (Folder/Agent Mode)	Google Cloud Run — конверзија во PDF, компресија и делење на страници; привремена обработка, без трајно чување	Период на договорот
Google Ireland Limited (ЕУ регион)	Само информации неопходни за автентикација: e-mail адреса, име, технички токен	Google OAuth 2.0 — SSO „Sign in with Google“; federated identity	Период на договорот (само при користење на Google SSO)
Microsoft Ireland Operations Ltd. (ЕУ регион)	Само информации неопходни за автентикација: e-mail адреса, име, технички токен	Microsoft Identity Platform — SSO автентикација (Sign in with Microsoft)	Период на договорот (само при користење на Microsoft SSO)

Под-обработувач	Предмет	Природа / мерки	Времетраење
Brevo SAS (Sendinblue) (Париз, Франција, ЕУ)	Само нотификациски метаподатоци (e-mail адреса, име, тип нотификација) — без содржина внесена од корисниците	Транзакциски e-mail сервис (потврди на регистрација, системски известувања); GDPR-усогласен, ISO 27001	Период на договорот

- **Договори за обработка:** Обработувачот има потпишани договори за обработка на лични податоци (DPA) со сите наведени под-обработувачи, со кои гарантира еднакво ниво на заштита како она договорено со Контролорот.
- **Промени на листата:** за секоја намерена промена преку додавање или замена на под-обработувач, Обработувачот ќе го извести Контролорот писмено најмалку 15 дена однапред, со што му се овозможува да го оствари своето право на приговор.
- **Без пренос во трети земји:** Обработувачот не врши пренос на лични податоци надвор од ЕУ/ЕЕА.

11. AI обработка и заштита на содржината

- **Провајдер:** единствен провајдер на голем јазичен модел е Google Cloud — Vertex AI (Gemini), во enterprise конфигурација, со обработка во ЕУ/ЕЕА регион.
- **Опт-аут од тренирање:** Factum има експлицитен договорен opt-out од користење на податоците за тренирање на моделите.
- **Zero Data Retention (ZDR):** потврден договор за нулта ретенција — промптовите и документите се обработуваат преодно, без задржување и без логирање за човечки преглед (без abuse monitoring) од страна на AI провајдерот.
- **Без тренирање:** влезната и излезната содржина на Корисникот не се користат за тренирање, дотренирање или подобрување на модели на Factum или на која било трета страна.
- **Енкрипција:** целата комуникација со AI провајдерот се одвива преку енкриптиран канал (TLS 1.3).
- **Надворешни AI асистенти по избор на Корисникот:** доколку Корисникот самиот се поврзе со надворешен асистент преку MCP интерфејсот на Factum (на пр. Claude, ChatGPT, Microsoft Copilot), тој асистент дејствува под контрола и договор на Корисникот и не претставува под-обработувач на Factum.

12. Достапност по пакети

Мерките што се однесуваат на инфраструктурата, енкрипцијата, изолацијата, резервните копии, под-обработувачите и AI обработката се применуваат на сите корисници, независно од избраниот пакет. Функционалностите означени со „Достапно во Enterprise пакетот“ се предмет на посебен договор или анекс.

Договор за обработка на лични податоци: Стандардните договорни клаузули (Прилог бр.1) со Анексите бр.1–3 ја имаат функцијата на договор за обработка помеѓу Контролорот и Обработувачот и се составен дел на Договорот. Склучување на посебен самостоен DPA со дополнителни или изменети одредби е достапно во Enterprise пакетот.

ФАКТУМ ДОО Скопје

Управител,
Димитар Чуковски