Măsuri de securitate și de protecție a datelor în aplicația ULTRA

Document informativ pentru birourile notariale, practicienii în insolvență și responsabilii lor cu protecția datelor. Versiunea **1.0**, valabilă pentru aplicația ULTRA **0.26** și ulterioare, data _____ .

1. Pe scurt

ULTRA este o aplicație instalată pe calculatorul biroului, care ajută la redactarea, verificarea și organizarea actelor. Protecția datelor se sprijină pe cinci principii:

- **Documentele rămân la birou.** Actele, dosarele, indexul de căutare și istoricul conversațiilor stau pe echipamentul biroului. Infrastructura Furnizorului nu primește și nu stochează conținutul documentelor.
- **Identificatorii personali nu pleacă spre model.** Codurile numerice personale, conturile IBAN, numerele de telefon, adresele de e-mail și datele din zona de citire optică a actelor de identitate sunt înlocuite cu marcaje neutre înainte ca textul să părăsească calculatorul și sunt puse la loc, local, în răspuns.
- **Inferența are loc în Uniunea Europeană, fără păstrarea conținutului**, pe ruta configurată pentru organizație (secțiunea 4).
- **Fiecare persoană are contul ei**, cu parolă proprie, sesiuni care pot fi revocate imediat și drepturi transmise dispozitivului într-un pachet semnat criptografic.
- **Nimic nu se șterge fără aprobare.** Asistentul lucrează exclusiv în folderul dosarului, iar orice comandă care ar șterge fișiere cere confirmarea utilizatorului cu parola contului.

Sistemul de management al Furnizorului este certificat **ISO/IEC 27001:2022** (securitatea informației) și **ISO/IEC 42001:2023** (managementul inteligenței artificiale), conform secțiunii 11.

2. Unde se află datele

Categorie de date	Unde se află	Cine are acces
Actele, dosarele, șabloanele biroului	echipamentul biroului, în folderul de lucru ales la instalare	personalul biroului, conform rolurilor
Indexul de căutare și istoricul conversațiilor	echipamentul biroului, în baza de date locală a aplicației	utilizatorul echipamentului
Textul transmis pentru generare sau analiză	furnizorul de servicii de inferență, în Uniunea Europeană, pe durata solicitării	furnizorul de inferență, conform secțiunii 4
Conturi, licențe, contoare de utilizare, jurnal de audit	panoul central de administrare, Frankfurt (Germania)	administratorii Furnizorului
Cheile de acces și jetoanele ANAF	seiful sistemului de operare de pe echipamentul biroului	utilizatorul echipamentului
Date de facturare	Stripe; panoul central păstrează doar un rezumat al cardului	administratorii Furnizorului
Tichetele de asistență și atașamentele lor	panoul central, Frankfurt (Germania)	administratorii Furnizorului și autorul tichetului

Despre activitatea unui birou, panoul central primește doar valori numerice: unități de consum pe zi și pe model, număr de solicitări, versiunea aplicației și momentul ultimei conectări.

---

3. Datele rămân pe echipamentul biroului

Aplicația lucrează direct cu fișierele din folderul de lucru al biroului, în formatele lor obișnuite (Word, PDF, imagini). Fișierele sunt scrise atomic, astfel încât o întrerupere nu lasă un document pe jumătate salvat.

Indexul de căutare, inclusiv componenta semantică, și recunoașterea optică a textului din documentele scanate se calculează pe echipamentul biroului, cu modele descărcate o singură dată. Nici indexarea, nici recunoașterea optică nu transmit conținut în exterior.

Aplicația nu conține componente de telemetrie, de analiză a comportamentului sau de raportare automată a erorilor. Comunică cu infrastructura Furnizorului doar pentru autentificare, verificarea licenței, raportarea numerică a consumului, verificarea actualizărilor și tichetele de asistență.

Pentru birourile care doresc partajarea dosarelor între mai multe echipamente, organizația poate primi, la cerere, o instanță de date proprie, găzduită în Frankfurt. În lipsa ei, aplicația funcționează integral local.

---

4. Inteligența artificială: ce pleacă și ce nu

Anonimizare înainte de trimitere. Înainte ca textul unei solicitări să părăsească echipamentul, aplicația înlocuiește cu marcaje neutre următorii identificatori:

Identificator	Cum este recunoscut
Codul numeric personal	13 cifre cu structură și cifră de control valide
Contul bancar (IBAN)	format românesc și internațional, cu verificarea cifrelor de control
Numărul de telefon	formate naționale și internaționale uzuale
Adresa de e-mail	orice adresă validă
Zona de citire optică a actelor de identitate	rândurile citite de pe cărțile de identitate și pașapoarte

Modelul primește, de exemplu, `<user_1_cnp>` în locul codului numeric personal. Corespondența dintre marcaj și valoarea reală rămâne pe echipamentul biroului, separată pentru fiecare conversație, și este folosită la întoarcere pentru a repune valorile în documentul generat. Dacă anonimizarea nu poate fi finalizată, solicitarea nu pleacă. Instrumentele care trimit date în exterior (căutare web, preluare de pagini) refuză orice argument care conține marcaje.

Imaginile sunt citite înainte de a fi trimise. Nicio imagine nu ajunge la model neverificată: este citită optic local, iar tot ce seamănă cu un document este înlocuit cu textul extras, care trece apoi prin anonimizare. Doar imaginile fără conținut de tip document ajung la model ca imagine.

Rutele de inferență. Organizația folosește una dintre cele două rute; cea configurată este consemnată în procesul-verbal de predare-primire.

	Ruta Uniunea Europeană (AWS Bedrock)	Ruta standard (Anthropic API)
Unde are loc inferența	centre de date AWS din Uniunea Europeană, regiunea Frankfurt	infrastructura Anthropic, Statele Unite ale Americii
Păstrarea conținutului	retenție zero, blocată printr-o politică la nivel de organizație	maximum 30 de zile, exclusiv pentru monitorizarea abuzurilor
Utilizarea la antrenare	nu	nu
Temeiul transferului	nu are loc transfer în afara Spațiului Economic European	clauze contractuale standard

Legătura directă. Solicitările pleacă direct de la echipamentul biroului către furnizorul de inferență, criptate în tranzit. Panoul central emite doar o permisiune de acces valabilă o oră, fără să vadă conținutul.

Verificarea umană. Fiecare act generat este propus spre revizuire: cifrele apar ca propuneri, trimiterile legale sunt verificate automat și marcate, iar documentul nu produce efecte juridice până când profesionistul licențiat nu îl verifică.

5. Conturi și acces

Conturi individuale. Fiecare utilizator are cont propriu, cu parolă de minimum 10 caractere, păstrată doar ca hash scrypt cu sare individuală. Parola temporară primită la creare se schimbă la prima conectare. După 10 încercări eșuate contul se blochează 15 minute, iar numărul de încercări pe minut este limitat la nivelul serverului.

Sesiuni. Dispozitivul primește la conectare un jeton aleator de 256 de biți, păstrat pe server doar ca amprentă SHA-256. Un cont poate avea cel mult 3 dispozitive active. Sesiunile expiră după 180 de zile de inactivitate și pot fi revocate imediat

din panou, cu efect la următoarea solicitare.

Drepturi semnate criptografic. Licența, rolul, tipurile de dosare permise și politica organizației ajung la dispozitiv într-un pachet semnat Ed25519, cu cheia publică fixată în aplicație. Orice modificare a pachetului îl invalidează. Fără legătură cu serverul, aplicația funcționează cu ultimul pachet valid cel mult 14 zile.

Roluri și izolare. Fiecare organizație are administratori de organizație și utilizatori. Datele și spațiul de lucru sunt izolate pe organizație, inclusiv când același echipament este folosit de organizații diferite.

Panoul de administrare. Administratorii Furnizorului se conectează cu cont individual și cookie de sesiune protejat (HttpOnly, Secure, SameSite), valabil 7 zile. Toate acțiunile administrative sunt consemnate într-un jurnal de audit cu autor, moment și adresă.

6. Criptare

În tranzit. Comunicațiile aplicației cu panoul central, cu instanța de date și cu furnizorul de inferență sunt criptate TLS. Panoul central este publicat prin Cloudflare, iar serverul de origine acceptă conexiuni numai din rețeaua Cloudflare.

Credențiale pe echipament. Cheile de acces la serviciile de inferență, jetoanele ANAF și sesiunile de cont sunt păstrate în seiful sistemului de operare (Keychain pe macOS, DPAPI pe Windows), nu în fișiere text.

La repaus, la Furnizor. Baza de administrare, copiile ei de siguranță și atașamentele tichetelor sunt stocate în Google Cloud, regiunea Frankfurt, criptate la repaus, fără acces public.

La repaus, la birou. Documentele și baza de date locală a aplicației au nivelul de protecție al echipamentului. Furnizorul recomandă și verifică la instalare criptarea discului (FileVault pe macOS, BitLocker pe Windows) și blocarea automată a sesiunii de utilizator.

7. Siguranța asistentului pe echipament

Perimetrul dosarului. Asistentul poate citi și scrie exclusiv în folderul dosarului activ și în folderul de configurare al aplicației. Orice cale care iese din perimetru, inclusiv prin legături simbolice, este respinsă.

Ștergerea cere parola. Orice comandă care ar șterge un fișier, pe orice sistem de operare, se oprește și cere aprobarea utilizatorului cu parola contului. Comenzile distructive pentru sistem sunt refuzate.

Reguli impuse central. Administratorul organizației poate defini reguli pe care asistentul le respectă în fiecare conversație. Ele ajung la dispozitiv în pachetul semnat, așa că nu pot fi modificate de utilizator.

Izolarea interfeței. Interfața aplicației rulează izolat de sistem, sub o politică strictă de securitate a conținutului; legăturile externe se deschid în navigatorul sistemului.

8. Infrastructura Furnizorului

Panoul central rulează în Google Cloud, regiunea Frankfurt (Germania), în spatele rețelei Cloudflare. Serverul acceptă trafic web exclusiv din intervalele de adrese Cloudflare, aplicația este legată la interfața locală, iar accesul administrativ se face numai cu chei SSH.

Baza de administrare este salvată zilnic, păstrată 14 zile pe server și încărcată în stocarea Google Cloud din aceeași regiune, împreună cu cheile de semnare a pachetelor de drepturi. Nu există o cale prin care conținutul documentelor unui birou să ajungă în panou.

9. Actualizări și integritatea aplicației

Fiecare fișier de instalare este publicat împreună cu amprenta SHA-512 și dimensiunea exactă, verificate de aplicație înainte de instalare; un fișier incomplet sau modificat este refuzat. Versiunea pentru macOS este semnată și notarizată de Apple.

Furnizorul poate stabili o versiune minimă obligatorie: sub aceasta, aplicația afișează un ecran de blocare până la actualizare, astfel încât o corecție de securitate ajunge la toți utilizatorii într-un timp cunoscut.

Fiecare versiune trece, înainte de publicare, printr-o suită de teste care acoperă anonimizarea (inclusiv teste aleatorii cu identificatori generați), regulile de siguranță ale comenzilor, perimetrul de fișiere, comportamentul la întreruperi de rețea și fidelitatea documentelor generate.

---

10. Plăți și asistență

Plățile sunt procesate de Stripe, prin paginile sale securizate. Datele cardului nu ajung pe serverele Furnizorului; panoul păstrează doar tipul cardului și ultimele patru cifre.

Atașamentele tichetelor de asistență sunt verificate după conținutul real, nu după extensie, sunt limitate la 25 MB pe fișier și sunt stocate în regiunea Frankfurt. Personalul de asistență vede tichetul și atașamentele lui, nu dosarele biroului.

---

11. Certificări

Sistemul de management al Furnizorului este certificat de Certificare Conformitate Standarde SRL (IQ Cert), București, organism de certificare acreditat IMAB (International Management Accreditation Board), pentru următoarele standarde:

Standard	Certificat nr.	Valabil până la
ISO/IEC 27001:2022, securitatea informației	CS/2026-2478SI	2 septembrie 2027
ISO/IEC 42001:2023, inteligența artificială	CS/2026-2479AI	2 septembrie 2027

Certificatele au fost emise la 3 septembrie 2026 pentru realizarea de software la comandă, consultanță în tehnologia informației și gestiunea mijloacelor de calcul; se pun la dispoziția Beneficiarului la cerere.

Documente conexe și contact. Anexa privind prelucrarea datelor cu caracter personal (DPA), modelul de evaluare a impactului (DPIA) și procesul-verbal de predare-primire, care consemnează ruta de inferență configurată. Întrebările privind securitatea se adresează la office@fastforward.dev; Furnizorul confirmă în scris, la cerere, regiunea de prelucrare și regimul de retenție aplicate organizației.