

# Zásady ochrany osobních údajů (GDPR)

**MetaHub** — Platforma pro správu a automatizované zpracování obchodních dokumentů  
Provozovatel: **Everquest.io s.r.o.**, IČO: 57387273, DIČ: 2122690053, IČ DPH: SK2122690053, se sídlem  
Hodžova 4791/3, Záturčie, 036 01 Martin

Kontakt DPO: [dpo@metahub.cz](mailto:dpo@metahub.cz)

Platnost od: 1. 3. 2026

## 1. Jaké osobní údaje zpracováváme

### 1.1 Údaje uživatelů (zaměstnanců / členů týmu)

- Jméno, příjmení, e-mailová adresa
- Hashované heslo nebo OAuth token (Google)
- Role a oprávnění v rámci firmy
- Datum registrace a poslední přihlášení
- IP adresa při přihlášení (logy)

### 1.2 Údaje z nahraných dokumentů

Dokumenty nahrané do systému (faktury, účtenky, timesheety) mohou obsahovat:

- Obchodní jména dodavatelů a odběratelů
- IČO, DIČ, bankovní spojení, IBAN
- Částky, data, čísla dokladů
- Jména fyzických osob (pokud jsou na dokladech uvedena — např. u OSVČ)

### 1.3 Technické a provozní údaje

- Záznamy o použití AI (počet tokenů, odhadované náklady) — neobsahují obsah dokumentů
- Záznamy přístupu k API (IP adresa, časové razítko, endpoint)
- Chybové logy

## 2. Účely a právní základ zpracování

Účel zpracování	Právní základ (čl. 6 GDPR)
Poskytování služby (správa dokumentů, schvalování)	Plnění smlouvy (6/1/b)
Automatická extrakce dat z dokumentů pomocí AI	Plnění smlouvy (6/1/b)

Účel zpracování	Právní základ (čl. 6 GDPR)
Zasílání transakčních e-mailů (schválení, upozornění)	Plnění smlouvy (6/1/b)
Bezpečnost, prevence zneužití, logy přístupu	Oprávněný zájem (6/1/f)
Fakturace a vedení účetních záznamů	Právní povinnost (6/1/c)

---

## 3. Zpracování dokumentů pomocí AI — podrobnosti

---

### 3.1 Jak zpracování funguje

Po nahrání dokumentu je jeho obsah odeslán do API Anthropic (model Claude) pro automatickou extrakci strukturovaných dat (dodavatel, částky, data splatnosti, bankovní údaje). Dokument je odeslán jako:

- obrázek v kódování base64 (PNG, JPEG), nebo
- extrahovaný text (digitální PDF)

### 3.2 Třetí strana — Anthropic, PBC

Obsah dokumentů je zpracováván službou **Anthropic, PBC** (San Francisco, CA, USA) prostřednictvím jejich Messages API.

#### Klíčové záruky ze strany Anthropic:

- Data odeslaná přes API **nejsou používána k trénování modelů**
- Anthropic může data krátkodobě uchovávat za účelem bezpečnostního monitoringu (typicky max. 30 dní)
- Anthropic je certifikován dle SOC 2 Type II
- Předávání dat do USA je kryto standardními smluvními doložkami (SCC) dle čl. 46 GDPR

### 3.3 Co se neodesílá do AI

- Identita uživatele ani název společnosti
- Interní ID záznamu
- Konfigurace pravidel ani nastavení schvalování

### 3.4 Minimalizace dat

Systém odesílá do AI pouze obsah nezbytný pro extrakci. Pro digitální PDF je upřednostňován prostý text před odesláním obrazové přílohy.

---

## 4. Ukládání dokumentů

---

Dokumenty jsou ukládány na serveru provozovatele (MinIO / S3-kompatibilní úložiště) provozovaném na území EU.

Každá firma si může v nastavení zvolit:

- **INTERNAL** — soubory jsou uchovávány v šifrovaném úložišti
- **NONE** — soubory jsou po zpracování AI okamžitě smazány (uchovávají se pouze extrahovaná strukturovaná data)
- **GOOGLE\_DRIVE / DROPBOX / ONEDRIVE / CUSTOM\_S3** — soubory jsou ukládány ve vámi zvolené cloudové službě

## 5. Doba uchovávání dat

Kategorie dat	Doba uchovávání
Uživatelské účty	Po dobu trvání smluvního vztahu + 90 dní po ukončení
Nahrané dokumenty (soubory)	Dle volby firmy; při nastavení NONE ihned po zpracování
Extrahovaná data (databáze)	Po dobu trvání smluvního vztahu
Logy AI použití (tokeny, náklady)	2 roky
Přístupové logy	1 rok
Zálohy databáze	30 dní

## 6. Přenos dat do třetích zemí

Příjemce	Země	Právní základ přenosu
Anthropic, PBC (AI zpracování)	USA	Standardní smluvní doložky (SCC)
Mailgun (transakční e-maily)	EU (api.eu.mailgun.net)	Zpracování v EU
Google (OAuth přihlášení)	USA	SCC + adekvátní ochrana

## 7. Práva subjektů údajů

Máte právo kdykoliv:

- **Přístupu** — získat kopii svých osobních údajů
- **Opravy** — opravit nesprávné údaje
- **Výmazu** — požádat o smazání (právo být zapomenut)
- **Omezení zpracování** — omezit způsob zpracování
- **Přenositelnosti** — obdržet data ve strojově čitelném formátu
- **Námítky** — vznést námitku proti zpracování na základě oprávněného zájmu

- **Odvolání souhlasu** — pokud je zpracování založeno na souhlasu

Žádosti zasílejte na: [dpo@metahub.cz](mailto:dpo@metahub.cz)

Lhůta pro odpověď: **30 dní** (může být prodloužena o dalších 60 dní v složitých případech).

Máte také právo podat stížnost u dozorového úřadu:

**Úřad pro ochranu osobních údajů (ÚOOÚ)**, Pplk. Sochora 27, 170 00 Praha 7 <https://www.uoou.cz>

---

## 8. Postup při výmazu dat (při ukončení smlouvy nebo na žádost)

---

- Deaktivace uživatelského účtu a zrušení přístupu
  - Smazání nahraných souborů z úložiště MinIO
  - Anonymizace nebo výmaz extrahovaných dat z databáze
  - Smazání záznamů v AI usage logu přiřazených ke společnosti
  - Písemné potvrzení dokončení výmazu do 30 dní
- 

## 9. Bezpečnost zpracování

---

Přijatá technická a organizační opatření:

- Šifrování přenosu dat (HTTPS/TLS) pro veškerou komunikaci
  - Hashování hesel (bcrypt)
  - JWT tokeny s krátkou dobou platnosti (60 minut) + refresh tokeny
  - Řízení přístupu na základě rolí (ADMIN, APPROVER)
  - Dočasné soubory při zpracování AI jsou mazány ihned po dokončení
  - Presigned URL pro přístup k dokumentům s platností 1 hodina
  - Přístup k produkčnímu prostředí je omezen a monitorován
- 

## 10. Cookies a analytika

---

Webová aplikace MetaHub používá pouze technicky nezbytné cookies (session token, CSRF ochrana). Analytické ani marketingové cookies nejsou nasazeny.

---

## 11. Změny tohoto dokumentu

---

O podstatných změnách budeme uživatele informovat e-mailem nebo prostřednictvím oznámení v aplikaci nejméně 14 dní před jejich účinností.

---

