
1. Architectuur

De Werkplaats is een digitale werkomgeving voor adviseurs en teams.

De technische infrastructuur wordt geleverd via het CAI-platform. Hosting en gegevensopslag vinden plaats via DigitalOcean op servers in Nederland.

Voor AI-functionaliteit maakt De Werkplaats gebruik van de API's van OpenAI en/of Anthropic (Claude).

2. Hosting & opslag

- Hosting en gegevensopslag vinden plaats op servers in Nederland.
- Dagelijkse versleutelde back-ups.
- Back-ups worden opgeslagen binnen de Europese Unie.
- Retentie back-ups: 30 dagen.

3. Dataverkeer & versleuteling

- Alle dataverkeer is versleuteld via TLS 1.2 of hoger
- Bestanden worden versleuteld opgeslagen (encryption at rest)
- Wachtwoorden worden gehasht opgeslagen met moderne hashing-algoritmen

4. Isolatie & toegangsbeheer

- Studios zijn technisch gescheiden van elkaar op infrastructuurniveau
- Kennisbankbestanden zijn uitsluitend toegankelijk binnen de betreffende Studio
- System prompts zijn niet zichtbaar voor eindgebruikers
- Rolgebaseerde toegang tot beheerfuncties
- Automatische sessie-time-out bij inactiviteit
- Logging van configuratiewijzigingen
- Conversatiegegevens van één Studio zijn niet toegankelijk voor andere Studio-eigenaren

5. AI-verwerking

Binnen De Werkplaats worden via API-koppelingen AI-modellen van OpenAI en Anthropic (Claude) gebruikt voor tekstanalyse en -generatie. Per AI-assistent wordt gebruikgemaakt van één van deze taalmodellen.

Daarbij geldt:

- Voor de API-verwerking worden in beginsel datacenters in Europa gebruikt. Wanneer daar onvoldoende capaciteit beschikbaar is, kan verwerking buiten de Europese Economische Ruimte (EER) plaatsvinden.
- De gegevens die via de API aan OpenAI of Anthropic worden aangeboden, worden niet door deze AI-aanbieders opgeslagen.
- Gegevens worden niet gebruikt voor het trainen van publieke AI-modellen.
- Gegevens worden verwerkt conform de afspraken die op de betreffende verwerking van toepassing zijn.
- Indien verwerking buiten de EER plaatsvindt, gebeurt dit onder toepasselijke internationale doorgiftewaarborgen.
- Er vindt geen automatische besluitvorming plaats met rechtsgevolgen.
- Er vindt geen automatische besluitvorming plaats met rechtsgevolgen.

6. Conversatiegegevens

- Conversaties worden opgeslagen binnen de Platforminfrastructuur
- Buro Mooi heeft geen toegang tot individuele conversatiegegevens van gebruikers.
- CAI kan toegang hebben tot conversatiegegevens voor technisch beheer, ondersteuning en het opsporen van technische problemen.
- Voor verbetering van het platform kunnen conversatiegegevens door CAI uitsluitend geanonimiseerd en geaggregeerd worden gebruikt.
- Conversatiegegevens worden niet gebruikt voor het trainen van AI-modellen

7. Monitoring & incidentbeheer

- Continue beschikbaarheidsmonitoring
- Detectie van afwijkend gedrag
- Incidentbeoordeling binnen 24 uur
- Notificatie binnen 72 uur bij meldingsplichtige datalekken

8. Subverwerkers

De Werkplaats maakt gebruik van subverwerkers.

Via CAI:

- DigitalOcean – hosting
- OpenAI en Anthropic – AI-verwerking
- Stripe – betalingsverwerking binnen het CAI-platform, PCI-DSS gecertificeerd

- Coddin B.V. – technisch beheer

Rechtstreeks door Buro Mooi:

- MailBlue – e-mailcommunicatie

Voor zover partijen persoonsgegevens verwerken als verwerker of subverwerker, worden passende afspraken over gegevensverwerking gemaakt. Voor de technische infrastructuur beheert CAI de relatie met haar subverwerkers.

9. Bewaartermijnen

- Werkdocumenten en conversatiegegevens: zolang het abonnement actief is. Na beëindiging van het abonnement worden deze uiterlijk binnen 30 dagen verwijderd.
- Accountgegevens: 12 maanden
- Back-ups: 30 dagen
- Financiële administratie: 7 jaar

De meest recente versie van dit document is beschikbaar via buromooi.nl.