

Before client data reaches an AI

For law firms, accountants and medical practices in the US and Europe. Checked on 15 October 2026. Not legal advice.

1. The contract with the provider

1. US law firm: read the terms; input kept confidential and out of training (ABA Formal Opinion 512, July 2024)
2. US medical practice: a business associate agreement before any patient data (HIPAA, 45 CFR 164.502(e))
3. UK law firm: contractual, technical and organisational safeguards; no training without authorisation (SRA, 17 Aug 2026)
4. EU: a processing agreement under GDPR Art. 28; health data: Art. 9
5. Germany: plus a secrecy commitment in text form, with a warning about criminal consequences (§203 StGB, §43e BRAO, §62a StBerG)
6. Data abroad: ask where it is stored; Germany requires comparable protection; US tax preparers need consent (26 CFR 301.7216-2)

2. Consent and anonymisation

1. US lawyers: informed consent before client confidences go into an AI tool; boilerplate in the engagement letter is not enough (ABA 512)
2. Germany: consent for mandate-specific use (§43e(5) BRAO, §62a(5) StBerG)
3. Without the right contract or consent: abstract, anonymised prompts only
4. Removing names is often not enough: generalise details and check every page (GDPR Recital 26; BRAK, Dec 2024)

3. Firm policy

1. Approve the tools and the account type for each
2. File the contract terms per tool: processing agreement, BAA or secrecy commitment
3. Write down what may be entered
4. Decide when to ask for consent; keep a specific template
5. A professional reviews every AI output used in client work; train staff

Free accounts often train on input; business accounts can exclude training by agreement (BStBK FAQ, 27 Jan 2026). Free and paid tools may both pose risks (SRA, Aug 2026). Responsibility for the output stays with the professional.