AI Policy

Petit Legal – use of generative AI and AI tools

Document	Details
Version and date	0.5 – 14 October 2026
Lawyer	Sander Petit
Firm	Petit Legal

1. Purpose and scope

This policy governs how the Lawyer and the employee(s) of Petit Legal, and anyone else working temporarily for the firm, such as trainees, temporary staff, locum lawyers and engaged freelancers (together: **staff**), use AI tools. The policy is deliberately proportionate and practical, designed for a sole-practitioner firm with one employee. Its aim is for the firm to make use of the opportunities offered by AI without eroding the core values of the legal profession (independence, partisanship, confidentiality, integrity and expertise) or its statutory obligations.

The policy applies to all AI tools that process or generate text, speech or other data, including where they are built into another program (such as a summarisation or translation feature), and regardless of whether the tool runs on a firm device or a private device.

2. Principles

- **Final responsibility.** AI supports, but does not steer. The Lawyer remains ultimately responsible for every piece of advice, every document and every action, including where AI has been used.
- **Confidentiality first.** Professional secrecy and legal professional privilege take precedence over convenience. Client data is only entered into a tool that has been approved for that purpose (sections 4 and 5).
- **Human oversight.** AI output is never adopted without review (section 8).
- **Transparency.** The firm is clear, internally and towards clients, about how AI is used (section 6).
- **Careful selection and documentation.** A documented assessment is made in advance for each tool (section 7).

3. Roles and responsibilities

Role	Responsibility
Lawyer	Adopts the policy, decides on the admission of tools, carries out the vendor assessments and DPIAs, maintains the register (Annex A), decides per matter whether AI is used, obtains the client's consent and reviews the output. The Lawyer is ultimately responsible for compliance, including where the employee has used AI.
Employee	Follows this policy and the training, uses only tools approved by the Lawyer, refers any doubt about a category or tool to the Lawyer and reports incidents immediately.
Locum	In the Lawyer's absence, the Lawyer arranges for a locum. The locum is bound by this policy and by professional secrecy, and is given access only to the tools and data needed for the locum engagement.

4. Permitted tools

Only tools on the list in Annex A may be used for firm work. Each tool has one of three statuses. A tool that is not on the list may not be used for client data until the Lawyer has assessed it (section 7).

Status	Meaning	Conditions
Green	May be used with client data.	Only with a signed data processing agreement, a completed assessment and DPIA, and with the client's consent for the matter (section 6). Only via the firm's business subscription.
Yellow	Only without client data and without confidential firm data.	Suitable for general research and use with public information or case descriptions that pass the identifiability test in section 5.
Red	Not permitted for firm work.	Applies to tools without a data processing agreement, with unclear data processing or insufficient safeguards, and to consumer subscriptions.

Where a client consents to the use of an AI tool, that consent takes precedence over the status set out above.

Outcome of initial assessment

Claude (Team or Enterprise, or API with a data processing agreement): green, subject to conditions. The contract provides a DPA with SCCs, no training on customer data and an IP indemnity outside the liability cap, but processing takes place in the US and the open actions in Annex B must be completed first.

Perplexity: yellow. There is a DPA, but the processing location and the security measures have not been established, there is no right to object to third-party model providers, and there is no fixed notification period for data breaches.

Pocket and other AI note-takers: red for conversations with clients and third parties, until a data processing agreement, list of sub-processors, transfer safeguards and export arrangements are in place and have been assessed. These documents have been requested from Pocket.

Consumer versions (such as Claude Free, Pro and Max, and Perplexity Free and Pro): red.

5. Which data in which tool

The table below determines, for each type of data, the type of tool (section 4) into which it may be entered. Tools with red status are not permitted for any category and are therefore not included in the table. The restriction applies to everything the firm enters, uploads or has transcribed, and therefore also to attachments, images and screenshots, including the associated metadata.

Type of data	Green	Yellow	Explanatory note
Public information and general legal questions	Yes	Yes	Without reference to a specific client or case.
Internal know-how without confidential content (templates, models, general work instructions)	Yes	Yes	Check that no client names or case details are included.
Case descriptions that pass the identifiability test	Yes	Yes, after test	See the identifiability test below. If in doubt, the stricter category applies.
Client files, documents and correspondence, including data of opposing parties, witnesses and experts	Yes, with consent	No	Consent in accordance with section 6. Enter no more data than necessary for the question.
Special categories of personal data and criminal-law data (Art. 9 and 10 GDPR)	Only after separate assessment	No	The Lawyer decides in advance and records the decision, tested against the DPIA.
Confidential firm data without personal data (strategy, rates, financial data, security information)	Yes	No	Only in a tool that contractually does not train on the data.

Type of data	Green	Yellow	Explanatory note
Staff and applicant data	Only after separate assessment	No	Inform the data subject in advance (Art. 13 and 14 GDPR) and use only a green tool.
Recording or transcribing conversations with clients or third parties	Only with an approved tool after notifying all participants	No	See section 9.
Passwords, access keys, citizen service numbers (BSN) and other identification numbers	No	No	Never enter, not even in a green tool.

Where the client has consented to the processing of the data referred to above, or has itself entered that data into a particular AI tool, the Lawyer may also use that data or AI tool in the same or an equivalent manner and with the same data.

6. Clients: consent and information

1. The handling Lawyer obtains the client's prior consent to the use of AI in the matter, in line with the recommendations of the Netherlands Bar (NOvA). This is arranged in the quotation or engagement letter and, for ongoing matters, prior to use. An exception applies where the client itself indicates that it has used AI tools in providing information, or where this is evident from the information provided.
2. This policy (or a summary of it) is available to clients, on request and via the Lawyer's website (www.petitlegal.nl). The firm informs clients which categories of AI tools are used and who processes data in that context, including processing outside the EEA.
3. If a client refuses consent, no AI is used with client data in that matter. This is recorded on the file.
4. The firm takes account of AI-generated documents provided by clients themselves: these are a starting point, never a final product, and are reviewed.

7. Vendor assessment

Before a tool is given green status, the Lawyer carries out the assessment in Annex B and documents the considerations. The minimum requirements are:

- A signed data processing agreement that complies with Art. 28(3) GDPR, with a valid transfer mechanism (Art. 44 to 46 GDPR) where data is processed outside the EEA.
- Insight into storage and processing locations and an up-to-date list of sub-processors, including the procedure for changes and objections.
- A contractual commitment that data will not be used for training, and clear retention and deletion periods.
- Demonstrable security (Art. 32 GDPR): certifications or audit reports that the firm has actually seen, not merely mentioned on a website.
- A data breach notification period that enables the firm to meet its own notification obligation (Art. 33 GDPR, 72 hours).
- Exit arrangements: export or return of data, deletion after termination and a reasonable notice or transition period.
- An assessment of limitations of liability, unilateral amendment clauses, governing law and dispute resolution.
- A data protection impact assessment (DPIA, Art. 35 GDPR) where the processing is likely to result in a high risk, which is the starting point for large-scale processing of confidential files or recordings.
- Inclusion in the record of processing activities (Art. 30 GDPR) and in the firm's AI register.

Part of the assessment is a check of the current terms. Terms and sub-processor lists change regularly; the Lawyer reassesses green tools at least annually and upon every notification of a change.

8. Use and review of output

1. AI can make mistakes and generate fictitious information, including non-existent case law, statutory provisions and quotations. Every source, quotation and statutory reference in AI output is checked against the primary source before it is used in a document, advice or letter.
2. Be alert to tools that tend to confirm the prompt, even where it is incorrect. Ask critical and open questions and explicitly ask for counterarguments.
3. AI is never decisive in assessing a client's position, choosing a litigation strategy or weighing interests.
4. Documents intended for the court, an opposing party or a client are reviewed by the responsible lawyer personally and signed or released by them.

9. AI note-takers and recordings

1. Recording or transcribing conversations with clients, opposing parties or other third parties using an AI tool is only permitted with a green tool approved for this purpose, or with the client's consent.
2. All other participants are informed in advance that the conversation is being recorded or transcribed, for what purpose and by whom the data is processed.
3. Recordings and transcripts are linked to the matter file, not to a personal account or private device, and are deleted in accordance with the retention period of the file.
4. For conversations in which legal professional privilege or professional secrecy is particularly sensitive, such as litigation preparation and negotiations on confidentiality, the Lawyer personally decides whether a recording is justified. The employee never records such conversations on their own initiative.

10. Knowledge and training

The firm ensures an appropriate level of AI literacy among everyone who works with AI, as required by Article 4 of the AI Act. The Lawyer and the employee attend training at least annually on how generative AI works and its limitations, hallucinations and error detection, confidentiality and the GDPR, prompting, cybersecurity and this policy.

11. Oversight, register and incidents

1. The Lawyer maintains a register of approved tools, their status, the date of assessment and reassessment, the contract and the contact point at the vendor.
2. The Lawyer checks at least once a year whether the policy is being complied with, on the basis of a sample of files in which AI has been used, and briefly records the findings.
3. Incidents (inadvertent entry of client data into a non-approved tool, a suspected data breach, incorrect AI output in an outgoing document) are reported to the Lawyer immediately. In the event of a data breach, the firm assesses whether notification to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and to data subjects is required, and whether the client must be informed. The notification period under Art. 33 GDPR is 72 hours after becoming aware.
4. Where questions of professional conduct or a possible breach of professional secrecy arise, the Dean of the local Bar (deken) is consulted where necessary.

12. Compliance and evaluation

A breach of this policy may lead to employment-law measures, and may have a disciplinary or civil-law dimension. The policy is evaluated at least annually, taking into account changes in the AI Act, GDPR enforcement, the recommendations of the NOvA and the vendors' terms.

Annex A – Register of tools

Classification based on public terms as at 14 October 2026. Based on the completed assessment in Annex B, which also sets out the open actions per tool.

Tool	Status	Permitted for	Conditions and points of attention
Claude (Anthropic)	Green (conditional)	Business plans (Team/Enterprise) or API with DPA: matter-related work with consent.	Processing in the US; SCCs and DPIA required. EU processing only via Bedrock or Vertex. Consumer versions prohibited. Assess the standard cap and the right to amend the terms.
Perplexity	Yellow	General research with public information or case descriptions that pass the identifiability test (section 5).	Enterprise/API DPA exists, but no right to object to third-party model providers, no fixed data breach notification period and no intended processing of special categories of data.
Pocket (and similar AI recorders)	Red	Not for conversations with clients or third parties without consent.	No DPA or sub-processor list found publicly; processing in the US; consumer-oriented terms. Documents have been requested from Pocket; reconsider after receipt and assessment.

Annex B – Vendor assessment per tool

Position as at 14 October 2026, based on the providers' public terms and DPAs. This is an assessment of the standard terms; different terms may apply to Team or Enterprise contracts. Where a point could not be established, it is marked "Unknown": this must be requested from the vendor before the status changes.

Item	Claude (Anthropic)	Perplexity	Pocket
Data processing agreement (Art. 28 GDPR)	**Yes** DPA forms part of the Commercial Terms (SCCs modules 2 and 3). Does not apply to Claude Free, Pro and Max. The firm must take out a business plan and record this.	**Yes** DPA forms part of the Enterprise and API terms (version 13 Aug. 2026). Does not apply to Free or Pro. Perplexity Search and Embeddings API may have different product terms.	**Requested** No DPA found publicly; only a BAA (HIPAA) is mentioned. Data processing agreement has been requested from Pocket; assess upon receipt.
Transfer mechanism and TIA	**Partly** SCCs modules 2 and 3 and UK addendum. Participation in the EU-US Data Privacy Framework only from a secondary source. The firm must carry out its own transfer impact assessment.	**Partly** SCCs module 2 (and 3 for sub-processors) under Irish law, UK addendum. The firm must carry out the transfer impact assessment.	**Requested** No transfer mechanism found publicly; the Terms mention processing in jurisdictions without an equivalent level of protection. Requested from Pocket.
Storage and processing locations	**Partly** US. No EU residency for Claude Enterprise or the first-party API (inference "global" or "US only"), according to secondary sources from August 2026. EU processing only via Amazon Bedrock (incl. Frankfurt) or Google Vertex EU.	**Unknown** Not established. The SCCs indicate transfer to a third country. Request from Perplexity.	**Partly** US (own statement: transcription and summarisation on US cloud). Location is known, but outside the EEA.
Sub-processors and change procedure	**Partly** Official list (incl. Google Cloud, Cloudflare, Sentry, Stripe; all US except Cloudflare worldwide). Procedure for changes in the DPA not verified.	**Partly** List on the Trust Center (not reviewed). New sub-processors notified 10 business days in advance; objection only leads to termination. Third-party model providers: notification only, no right to object.	**Requested** No sub-processor list publicly; the privacy policy only mentions categories of vendors. Sub-processor list, including the AI provider that transcribes, has been requested.
No training on customer data	**Yes** Contractual (Commercial Terms, sec. B): Anthropic may not train on Customer Content.	**Yes** Contractual (sec. 1.3.3 and DPA art. 5): no training or fine-tuning on Customer Content and Personal Data.	**Partly** Only a commitment on the Trust page; not in the Terms of Use. Privacy policy mentions own use of aggregated or de-identified data. Await confirmation in the DPA.
Retention and deletion periods	**Partly** Destruction of Confidential Information on request, except back-ups (sec. E.4). Periods in the DPA not verified.	**Yes** Input retained until deleted by the customer or 30 days after end of service; deletion or return within 30 days (DPA art. 10).	**Requested** No retention or deletion arrangements found publicly; the Terms place back-ups with the user. Requested from Pocket.
Security (Art. 32 GDPR)	**Partly** SOC 2 Type I and II, ISO 27001:2022, ISO/IEC 42001:2023 (source: Anthropic). Reports via the Trust Portal still to be reviewed by the firm.	**Unknown** Only a reference to the Trust Center; content of measures not established. Secondary source: GDPR claim based on self-declaration.	**Requested** Own claims (encryption, least privilege, DDoS). SOC 2 is stated both as Type 1 and as Type II. The report has been requested from Pocket.
Data breach notification (Art. 33 GDPR, 72 hours)	**Unknown** Period in the DPA not verified.	**Partly** "Without undue delay" after becoming aware, without a fixed period (DPA art. 7).	**Requested** No notification arrangements found publicly. Requested via the DPA.

Item	Claude (Anthropic)	Perplexity	Pocket
Exit: export, return, notice period	**Partly** Termination for convenience by either party; Anthropic 30 days' notice. Destruction on request. No export obligation or transition period.	**Partly** No termination for convenience for the customer (only breach or account closure); Perplexity 30 days. Deletion within 30 days. No export obligation.	**No** Pocket may suspend or modify accounts and services at its discretion without notice. No export arrangements publicly; requested from Pocket.
Liability, indemnity and IP	**Partly** Cap: fees paid in the last 12 months; IP indemnity falls outside the cap. Customer indemnifies for claims relating to Inputs.	**Partly** Cap: 12 months; DPA liability under the same cap. IP indemnity with broad exclusions. Customer indemnifies broadly for Customer Content.	**No** Cap: the greater of USD 100 or 12 months paid. No IP indemnity. Broad indemnity by the user. Claims period 1 year.
Unilateral amendment and assignment	**Partly** Amendment 30 days after posting or notice; Anthropic may assign upon acquisition or to a group company.	**No** Amendment effective upon notice; list of third-party models can be changed unilaterally; Perplexity may assign without consent.	**No** Changes apply immediately upon posting; Pocket may assign upon merger or acquisition.
Governing law and disputes	**Partly** EEA customers: Irish law and arbitration in Dublin (UNCITRAL). Customer loses access to the Dutch courts.	**No** Californian law; exclusive jurisdiction of the courts of San Francisco County. DPA/SCCs under Irish law.	**No** Delaware law; binding AAA arbitration; class action waiver.
Audit rights and provision of information	**Unknown** Not fully verified in the DPA.	**Partly** Maximum once per 12 months with 30 days' notice, after agreement on scope (DPA art. 9).	**Requested** Not addressed publicly. Requested via the DPA.
DPIA (Art. 35 GDPR)	**To do** To be carried out by the firm before use with client data.	**To do** Only required if the tool were to be admitted for client data.	**To do** Only required if the tool were to be admitted for recordings.
Record of processing activities and AI register	**To do** Include after the Lawyer's decision.	**To do** Include with yellow status.	**To do** Include with red status.
Proposed status	**Partly** Green subject to conditions: only Team/Enterprise or API with DPA, after completion of the actions above.	**Partly** Yellow: only without client data. Reconsider after answers to the open questions.	**No** Red until the requested documents (DPA, sub-processors, SOC 2 report, export arrangements) have been received and assessed; reconsider thereafter.