

The Lawyer's AI Data-Safety Checklist

11 checks before your firm lets AI near a client file.

Written for EU practice — GDPR, the AI Act, and professional secrecy.

Avocado Tech · AI for law firms

Most lawyers using AI today are careful, not careless. The problem isn't recklessness — it's that the free, consumer versions of these tools are built to learn from what you type, and "anonymising" the file before you paste it strips out the very facts that would have made the answer good. You end up either leaking, or getting a weak answer.

This checklist is the middle path: how to get real help from AI without putting a client's confidence — or your practice licence — at risk. Tick each box (☐) you can honestly answer yes to.

Before you type

1. The Bar test.

☐ Is this a matter I'd be comfortable defending to the Bar if the tool's provider read it? If not, it doesn't go in a consumer tool.

2. No training on your inputs.

☐ Have I confirmed the tool does not train on what I type? Consumer and free tiers usually do, unless you opt out — that alone rules them out for client work.

3. A written firm policy.

☐ Do we have a written rule on what may and may not be pasted into AI — and does everyone on the team actually know it?

Choosing the tool & the plan

4. Enterprise-grade plan, not personal.

☐ Are we on an enterprise-grade plan rather than a personal one? No-training is the floor; the enterprise tier is where the real controls live.

5. A data processing agreement.

☐ Is there a signed data processing agreement (DPA) naming the provider as a processor under GDPR?

6. Minimal retention.

☐ Is data retention minimised — ideally zero retention beyond the request itself?

7. EU data residency.

☐ Is EU data residency available and switched on, where the provider offers it?

Where the knowledge lives

8. You own it.
- ☐ Is our firm's knowledge stored somewhere we own and control — not locked inside a vendor's product we can't export?
9. An open, portable format.
- ☐ Is it kept in an open format we could still read if the vendor disappeared tomorrow?

Who stays in charge

10. Human-in-the-loop.
- ☐ Does a qualified lawyer review and approve every AI-assisted output before it reaches a client or a court?
- Human-in-the-loop keeps you in the AI Act's lower-risk tier — and satisfies your supervision duty.
11. You can show your work.
- ☐ Could we show what the AI did, and on what basis, if privilege is ever challenged?

Score yourself

Ticks	Where you stand
8 or more	You're ahead of most firms. Tidy up the gaps and you're on solid ground.
5 to 7	Fixable in an afternoon — mostly plan settings and one page of policy.
Under 5	Pause. Stop pasting client data into AI until you've closed the gaps.

Want a walk-through for your firm?

That's what we do — independent advice, AI built in your own environment, and the training to use it well. Human-in-the-loop, confidential by design.

Avocado Tech · jan@avocado.io · +385 91 794 2703 · avocado.io/law