



What You Need to Hear About AI: Legal, risk, and governance

WHAT'S SAFE TO PASTE

One prompt can be a disclosure under an NDA.

DATA TYPE	PUBLIC AI TOOL?	WHY IT TAKES
Public info, general research	YES	Low risk. No client or company identifiers involved.
Internal drafts, non-sensitive	CAUTION	Enterprise tier with a training opt-out where possible.
Client names, contracts, financials	NO	An approved enterprise tool only.
PII (employee or candidate data)	NO	A signed DPA and Legal review before any AI use.

BEFORE YOU SIGN

Seven checks for any AI supplier agreement, and what should stop the deal.

CHECK	WHAT GOOD LOOKS LIKE	RED FLAG
Data Processing Agreement	Signed before any real data touches the tool	Supplier can't produce one
Training data opt-out	Your data doesn't train their models by default	"We may use your data to improve our models"
Retention and deletion	How long it's kept, and how deletion is confirmed, in writing	No written retention or deletion terms
Sub-processors	Every third party that touches your data, named	"And our partners"
Liability and indemnification	Covers what happens if the AI causes an error or a breach	Capped at fees paid, no carve-out for a data breach
Audit rights	You can request compliance evidence	No way to verify the supplier's claims
Exit terms	Data portability and deletion timelines defined	Silent auto-renewal, terms change without notice

AI TERMS TOP 10 LIST

10 Acceptable Model Mechanics for Outputs	5 Supplier Indemnification for AI Related Claims
9 CI Includes Prompts & Outputs	4 Supplier Compliance with Law & Regulations
8 Output rights Includes Ownership & Usage	3 Sufficient Model Transparency Disclosures
7 Acceptable Model Data Retention Policy	2 Customer Data Isolation Warranty
6 Sufficient AI Product Security Standards	1 Supplier Training Data Limitation

WHO OWNS THE OUTPUT

Copyright needs a human author In the US, purely AI-generated output generally isn't protected on its own.	Editing and direction matter Substantial editing or arranging strengthens the case it's your work.	Supplier terms still apply Enterprise agreements usually assign output rights to you. Consumer tiers vary.	Training disputes are ongoing Some residual infringement risk, depending on the supplier and use case.
--	--	--	--

WHO DECIDES

Governance works when everyone knows which decisions are theirs.

Approving anew AI tool for company use IT and Legal, jointly	Signing off on a client-facing AI use case Business Owner + Legal	Reviewing a new supplier's DPA and terms Legal	Day-to-day calls on what's safe to paste You, using the Golden Rules	Escalating a suspected data or IP issue Your manager, immediately
--	---	--	--	---