MPL LEGAL TECH ADVISORS

Legal AI Governance Quick-Start Guide

Evaluate any AI tool or workflow in under 5 minutes, and know whether it's legally defensible or already exposing your firm.

Book a 15min AI & Data Readiness Check

1.) Governance Readiness Scan

If you can't confidently answer **"YES"** to all 10 questions below, treat your current AI use as non-compliant. This quick scan will reveal any major gaps in your AI governance. For each question, mark **Yes**, **No**, or **Unsure**:

1. Do you have a complete list of all AI tools currently being used in the firm?

If you don't even know which AI applications are in play, you can't manage their risks. An up-to-date inventory of tools is the first step to governance.

☐ **Yes** ☐ **No** ☐ **Unsure**

2. Have you formally approved which tools are permitted vs. prohibited?

Without an official "approved tools" list (and a banned tools list), staff may experiment with unvetted AI. Formal approval ensures only vetted, safe tools get used.

☐ **Yes** ☐ **No** ☐ **Unsure**

3. Do you know where each vendor stores and processes your data (geography + jurisdiction)?

Data location matters for confidentiality and compliance. You should know exactly which country or region your data resides in and under whose legal jurisdiction. If not, you might be violating data privacy or cross-border regulations.

☐ **Yes** ☐ **No** ☐ **Unsure**

© 2025 MPL Legal Tech Advisors | Legal AI Governance Guide | mpladvisors.com

4. Does the vendor delete all inputs immediately by default?

If the AI vendor stores your prompts or file uploads by default, your sensitive data could linger on their servers. Default deletion (or non-retention) of inputs is critical to protect confidentiality.

☐ **Yes** ☐ **No** ☐ **Unsure**

5. Can vendor employees or subcontractors access your data?

If humans at the vendor (or their subcontractors) can peek at your inputs or outputs, client confidentiality could be compromised. The best vendors isolate data so that no one on their end can read it.

☐ **Yes** ☐ **No** ☐ **Unsure**

6. Can you force prompt deletion or retrieval if content becomes subject to legal hold?

If your firm faces litigation, you need to preserve (and possibly obtain copies of) any data given to or generated by the AI. If the vendor cannot promptly delete data on request or provide a copy for a legal hold, that tool isn't safe for legal work.

☐ **Yes** ☐ **No** ☐ **Unsure**

8. Have all staff been trained on what is prohibited from AI prompts?

Even the best AI policy fails if employees don't know the rules. Everyone should know exactly what NOT to input into AI (client names, personal data, privileged info, etc.). If staff haven't been trained on this, assume they might inadvertently spill secrets.

☐ **Yes** ☐ **No** ☐ **Unsure**

9. Does your process require human review before AI-generated output is shared externally?

AI can fabricate facts or produce flawed work. You should never allow raw AI output to reach clients, courts, or third parties without a human check. If there's no mandatory human review step, your firm is one copy-paste away from a malpractice incident.

☐ **Yes** ☐ **No** ☐ **Unsure**

10. Is there a documented STOP-USE rule for AI when a risk threshold is hit?

Define in advance what will trigger pulling the plug. For example, "If the tool produces >5% errors or any confidentiality breach, stop using it." A clear stop-use policy prevents dangerous AI use from continuing due to inertia or ambiguity.

☐ **Yes** ☐ **No** ☐ **Unsure**

SCORING RULE:

Now, evaluate your responses:

- ➔ **All YES** - Congratulations, your basic AI governance is on track. Proceed to Section 2.
- ➔ **Any MAYBE/UNSURE** - Don't ignore it. Investigate and clarify that area *immediately* before using the AI further.
- ➔ **Any NO** - **Stop.** Your current AI use is not defensible. Treat it as non-compliant and pause deployment until you address the gap.

Book a 15min AI & Data Readiness Check

2.) Immediate Stop-Use Red Flags

If any of the following are true, suspend AI use until the issue is fixed. These are non-negotiable red flags that indicate severe risk:

☐ **Vendor retains prompts (no guaranteed deletion):** *If your queries and uploads aren't wiped from the provider's systems, sensitive data can linger indefinitely on their servers.*

☐ **Vendor uses data for model training by default:** *Your inputs are being repurposed to train the AI's models. This means client information could indirectly become part of the AI and even surface in responses to others. Major confidentiality red flag.*

☐ **Vendor under U.S. CLOUD Act jurisdiction (with no contractual override):** *If the provider is subject to U.S. law (even if data is stored in-region elsewhere) and your contract doesn't prevent disclosure, U.S. law enforcement can demand your data under the CLOUD Act. Client data could be accessed without your knowledge.*

☐ **No audit logs of AI activity:** *The tool doesn't record who is using it or what they've generated. Without audit logs, you can't trace which user prompted what or who viewed which output. This makes oversight and incident investigation impossible.*

☐ **Tool cannot comply with legal hold requirements:** *The AI system can't preserve or export past prompts and outputs on demand. If you get a litigation hold, you might be unable to retrieve (or ensure deletion of) relevant AI records, risking spoliation of evidence.*

☐ **Gen AI output auto-saves to unmanaged locations (email drafts, clipboard, browser cache):** *The tool's outputs or chat history might be automatically saved in places outside your secure systems. Unmanaged copies of AI output can leak or be accessed by unauthorized parties.*

☐ **Staff using personal accounts or unapproved devices:** *Employees are accessing the AI tool with personal logins or on phones/laptops outside the firm's control. Firm data could be going to personal email or unencrypted devices, destroying your ability to maintain confidentiality.*

Rule: If you cannot trace or delete data, you cannot claim confidentiality. In any scenario where the firm loses track of where data went or can't pull it back, that AI usage violates basic legal duties. Shut it down.

Book a 15min AI & Data Readiness Check

3.) Data Retention + Training Risk Decoder

How to read between the lines of vendor privacy policies: AI vendors often sugar-coat their data usage terms. Here's how to decode some common phrases you'll encounter:

VENDOR LANGUAGE SAYS...	WHAT IT ACTUALLY MEANS...
"We may use your data to improve our services."	Your inputs are being **stored and used to train future models**.
"We restrict employee access."	Employees **can access your data if 'needed'.** (It's not a zero-access policy).
"We anonymize your data where possible."	**De-anonymization via pattern matching is still possible.** In practice, unique details in your data can still be pieced together.
"Data stored in-region, but service controlled globally."	**CLOUD Act still applies: U.S. law enforcement can request access.** Geographic storage doesn't matter if the parent company is under U.S. jurisdiction.

Takeaway: Don't be lulled by reassuring lingo. If a vendor's policy is vague or has loopholes, assume your data isn't fully safe.

Book a 15min AI & Data Readiness Check

4.) Litigation Hold + Escalation Protocol

If an AI tool has touched any document, prompt, or communication that becomes subject to a legal hold and you must act fast to preserve integrity. Follow these steps immediately:

1.) Freeze further AI interaction with that matter. *Cease all use of the AI tool on the case in question at once.*

2.) Submit a deletion or data retrieval request to the AI vendor, citing your legal hold obligations. *Formally require that no data related to this matter be deleted (legal hold) or ask for an export if needed for review.*

3.) Log the vendor's response - document whether they confirmed compliance or refused. *Keep a record of their reply for your audit trail.*

4.) If the vendor cannot comply, escalate to the supervising partner and ethics counsel. *Leadership needs to know immediately if the tool or vendor might cause a breach of legal duties.*

If you cannot retrieve or wipe data under hold, the tool is incompatible with legal practice. In other words, any AI that won't let you honor a litigation hold has no place in your firm.

Book a 15min AI & Data Readiness Check

5.) AI Risk Tier Matrix

Not all AI tools carry equal risk. Use the matrix below to categorize any AI tool by risk tier and apply the corresponding policy:

RISK TIER	TOOL TYPE EXAMPLE	PERMITTED USE POLICY
Tier 1: Low Exposure	Local/offline tools (e.g. on-prem summarizers) that **do not retain** data.	Allowed without restriction. Low-risk utilities that keep data in-house can be used freely.
Tier 2: Moderate Exposure	Cloud or SaaS tools with strong deletion controls and security (e.g. transcription or drafting assistants with a proper contract).	Allowed with caution: Use under supervision and log all usage. Review outputs and keep audit trails.
Tier 3: High Exposure	Public or unvetted AI services (e.g. free chatbots, third-party tools lacking agreements).	Not allowed until **contractually constrained**. These high-risk tools should be blocked or sandboxed unless you have ironclad contracts and controls in place.

When in doubt, default to a higher risk tier. It's easier to relax controls on a safe tool than to explain a data breach from a "high exposure" tool that slipped through.

This Quick-Start Guide is a starting point. If you want your firm's real AI usage mapped, risk-ranked, and converted into a defensible policy →

Book a 15min AI & Data Readiness Check

Watch the full breakdown