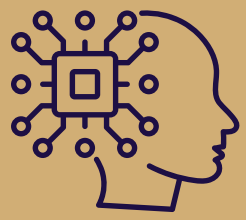
Law Society of Ireland

EVALUATING AI VENDORS



What legal practice needs from an AI supplier — and the questions to ask before you sign

Law Society of Ireland, Blackhall Place, Dublin 7

Tel: +353 1 881 5768 | Email: solicitorservices@lawsociety.ie | www.lawsociety.ie

EVALUATING AI VENDORS

The Core Problem

Many AI vendor agreements were not written with legal practice in mind. The terms offered for consumer-facing products are designed for general users rather than professional practice. Consumer agreements are generally not designed to provide the confidentiality protections, data residency commitments, or restrictions on training data use that legal practice requires.

For a solicitor, this is not a commercial inconvenience. It directly engages client confidentiality, data protection obligations under GDPR, and — where privileged material is involved — the risk of privilege waiver. The Law Society's Guidelines for the Use of Generative Artificial Intelligence by Solicitors (2025) are clear that professional obligations apply regardless of what the vendor's terms say.

> The free or low-cost tier of an AI product and the enterprise version of the same product are not the same thing. They have different terms, different data handling practices, and different contractual protections. A tool that may be appropriate under an enterprise agreement may be entirely unsuitable under consumer terms.

The Law Society's Tech Hub guidance on *Working with Technology Suppliers* covers the standard bases for any software vendor relationship: confidentiality, data security, SLAs, contract terms, scalability, and exit. That guidance remains the right starting point for general technology procurement. This resource addresses what comes next — the AI-specific layer that general vendor assessment does not cover, and that creates the most significant risk for legal practice.

Consumer Tools vs. Enterprise Agreements

This is the single most important distinction in AI vendor governance for legal practice:

Issue	Consumer tool	Enterprise agreement
Your data used to train AI models	Yes by default in most consumer products — inputs may improve the service	Contractually excludable — must be explicitly agreed
Confidentiality undertaking	None. Generic Terms of Service not designed for professional use	Data Processing Agreement required under GDPR Art. 28
Where data is processed	Vendor's discretion — may be any region or sub-processor	Specified in contract — EEA processing should be required
Privilege protection for legal material	No specific safeguards	Depends on negotiated terms — requires explicit agreement
GDPR compliance	Risk falls primarily on your firm as controller	Shared responsibility under DPA; vendor has defined processor obligations
Exit and data retrieval	Usually not guaranteed or defined	Should be specified: format, timeframe, deletion confirmation

What You Must Establish Before Signing

Any AI tool that processes client data or handles work that engages your professional obligations should meet all of the following:

- **Data residency —** Where is the data processed and stored? You should obtain a contractual commitment to EEA processing, or confirmation that Standard Contractual Clauses under GDPR Article 46 are in place where processing occurs outside the EEA. If the vendor is unable to confirm this, that is a material governance gap.
- **Training data exclusion —** Your inputs — including client data, matter information, and documents — should be contractually excluded from use in training or improving the vendor's AI models. Where a contract does not explicitly address this, the default position in many consumer agreements is that inputs may be used for model improvement.
- **Data Processing Agreement —** A DPA under GDPR Article 28 is a legal requirement where the vendor processes personal data on your behalf. This is not a negotiating preference. Where a vendor processes personal data without a DPA, your firm's compliance position under GDPR is materially weakened.
- **Exit and data retrieval —** You should be able to retrieve all client data and work product on termination — in a usable format and within a defined timeframe — and receive confirmation that your data has been deleted from the vendor's systems. Exit costs and timeframes should be agreed in the contract, not left undefined.
- **Liability for AI errors —** Standard software contracts often exclude or limit liability for inaccurate outputs. AI systems can produce plausible-sounding errors. You should understand what the vendor's contractual position is on liability for hallucinated or inaccurate content, particularly where you are relying on the tool for legal research or document drafting.

Vendor Classification

Apply a traffic-light classification to each vendor assessment:

GREEN	Vendor meets the required standards. Proceed with procurement.
AMBER	Vendor has identifiable gaps but is willing to negotiate. Proceed only subject to specific contractual amendments — list them explicitly and obtain them in writing before contracting.
RED	Vendor has material deficiencies that cannot be adequately addressed. Do not proceed without partner or board-level decision and documented risk acceptance.

Red Flags: When to Escalate or Walk Away

Each of the following should trigger a deeper investigation and, where the vendor is unwilling or unable to resolve the issue, escalate the classification toward AMBER or RED:

Red flag	What to do
Vendor cannot confirm where data is processed	Data residency is a non-negotiable requirement. Insist on a contractual commitment to EEA processing, or Standard Contractual Clauses under GDPR Article 46. If the vendor is unable to confirm this, do not proceed.
No contractual exclusion of training data use	Where a contract does not explicitly exclude your data from training, the default position in most consumer-tier agreements is that inputs may be used for model improvement. Obtain a written contractual exclusion before using the tool with client data.
Consumer terms offered for professional use	Consumer Terms of Service are not designed for legal practice. Insist on an enterprise agreement. If the vendor does not offer one, the tool is not suitable for use with client data or privileged material.
No Data Processing Agreement available	Where a vendor processes personal data on your behalf without a DPA, your firm's compliance position under GDPR is materially weakened. A DPA under Article 28 is a legal requirement, not a negotiating preference.
Unclear exit terms or data retrieval rights	The ability to retrieve client data and obtain confirmation of deletion on termination should be specified in the contract. If the vendor cannot or will not clarify exit terms, that is a governance risk in itself.

What a Sound Vendor Decision Looks Like

Before contracting with any AI vendor that will process client data or work product, you should be able to confirm:

- A Data Processing Agreement is in place that covers the specific processing being undertaken.
- Data residency is confirmed in the EEA, or adequate transfer mechanisms are in place and documented.
- Your data is contractually excluded from AI training and model improvement.
- You can retrieve and receive deletion confirmation of your data on termination, within defined terms.
- You understand what the AI system does, how it produces outputs, and what its limitations are — as required by your duty of competence.
- The decision has been approved at the appropriate level of the firm and the rationale is documented.

> **EU AI Act — Current Position**
>
> Prohibited AI practices have been banned since February 2025. General-purpose AI obligations have applied since August 2025. The main obligations for high-risk AI systems are currently set to apply from 2 August 2026. The European Commission's Digital Omnibus proposal — not yet enacted — proposes deferring these to December 2027 at the earliest. Regardless of the final timeline, firms should now be asking vendors how their system is classified under the Act and what compliance documentation they can provide.

This document does not constitute legal advice. It provides a framework for evaluating AI vendor proposals. You should seek independent legal and technical advice appropriate to your firm's circumstances.

AI Vendor Assessment – Report Template

Category 2 — Get Compliant Fast

Audience: Solicitors in private practice · In-house solicitors · Practice managers · Managing partners

Date completed: _____

This document does not constitute legal advice. It is a structured framework to support solicitors and practice managers in evaluating AI vendors against professional obligations, regulatory requirements, and the Law Society's general vendor guidance. Outputs should be reviewed against your firm's specific circumstances and obligations under the Solicitors Acts 1954–2015.

Assessment Overview

Relationship to Existing Guidance

This assessment should be completed alongside the Law Society's general guidance on *Working with technology suppliers* (available on the Law Society's Technology Hub). That guidance covers general vendor selection. This tool extends the assessment to AI-specific risks that require additional scrutiny.

Practice Name	[Enter]
Assessment Date	[Enter]
Assessed By	[Enter]
Vendor Name	[Enter]
Vendor Product/Service	[Enter]
Vendor Contact	[Enter]
Purpose of Assessment	[Enter]

1. Data Sovereignty & Residency

Where client data is processed and stored, transfer mechanisms, and sub-processor transparency.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Data processing location confirmed (EEA/non-EEA)			
Transfer mechanism documented (SCCs/Adequacy decision)			
Sub-processor chain disclosed and assessed			
Data residency contractually guaranteed			
Domain Score	**/20**		

2. Training Data & Model Governance

How the AI model was trained, data ownership, and client data usage restrictions.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Training data exclusion contractually confirmed			
Input/output data ownership position clarified			
Model versioning and change notification in place			
Opt-out of broader data sharing verified			
Domain Score	**/20**		

3. Confidentiality & Privilege Protection

How vendor protects client confidentiality and legal privilege during processing.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Enterprise agreement in place (not consumer ToS)			
Confidentiality protections adequate for client data			
Privilege risk assessed and documented			
Access controls and encryption standards confirmed			
Domain Score	**/20**		

4. Contractual Adequacy for AI

AI-specific contract terms, liability allocation, and IP ownership.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
AI-specific liability terms included in contract			
Agentic AI behaviour addressed (where applicable)			
Liability for hallucinated or inaccurate outputs allocated			
IP ownership of AI-generated work product defined			
Model change notification obligations specified			
Domain Score	**/25**		

5. Regulatory Compliance (EU AI Act & GDPR)

Vendor's compliance with GDPR, EU AI Act, and transparency obligations.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
EU AI Act risk classification confirmed by vendor			
GDPR Art. 28 Data Processing Agreement in place			
Data Protection Impact Assessment completed or planned			
Transparency obligations met (GDPR Arts. 12–14)			
Human oversight provisions adequate for legal use			
Domain Score	**/25**		

6. Professional Obligations Alignment

Compatibility with legal profession standards and meaningful human oversight.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Output verification capability confirmed			
Competence requirements met (solicitor can verify outputs)			
Supervision mechanisms allow meaningful human oversight			
Independence maintained (no conflicts of interest)			
Domain Score	**/20**		

7. Exit & Portability

Data and IP retrieval on termination, transition support, and lock-in risks.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Data retrieval mechanism documented			
IP retrieval rights confirmed on termination			
Transition timeline and support specified			
Lock-in risk assessed and acceptable			
Domain Score	**/20**		

8. Ongoing Governance & Review

Vendor transparency, review triggers, and audit rights.

Criterion	Score (1–5)	Evidence / Notes	Risk Level
Vendor notification obligations for material changes			
Review trigger mechanisms defined			
Audit or inspection rights included			
SLA monitoring provisions in place			
Domain Score	**/20**		

Summary & Classification

Overall Score Summary

Domain	Score	Max	%
1. Data Sovereignty & Residency	/20	20	
2. Training Data & Model Governance	/20	20	
3. Confidentiality & Privilege	/20	20	
4. Contractual Adequacy	/25	25	
5. Regulatory Compliance	/25	25	
6. Professional Obligations	/20	20	
7. Exit & Portability	/20	20	
8. Ongoing Governance & Review	/20	20	
TOTAL	**/170**	**170**	

Traffic-Light Classification

Classification Guidance

GREEN (≥80%): Proceed — vendor meets requirements across all domains.

AMBER (50–79%): Proceed with conditions — identified gaps must be addressed before or during engagement.

RED (<50%): Do not proceed — fundamental gaps in vendor's AI governance. Requires significant remediation before reconsideration.

Classification Result: ○ GREEN ○ AMBER ○ RED

Key Findings & Recommendation

Key Strengths

[Document vendor strengths identified during the assessment]

Key Gaps or Concerns

[Document gaps, risks, or concerns requiring attention]

Conditions for Proceeding (if AMBER)

[List specific conditions that must be met before or during engagement]

Recommendation

☐ GO ☐ GO WITH CONDITIONS ☐ NO-GO

Action Plan

#	Action Required	Domain	Owner	Deadline	Status
1					
2					
3					
4					
5					
6					
7					
8					

Sign-Off

This assessment should be reviewed at least annually, or when triggered by: material vendor changes, regulatory developments (including EU AI Act implementation), changes to the firm's use of the tool, or Law Society guidance updates.

Role	Name	Signature	Date
Assessor			
Practice Manager			
Managing Partner			

This resource was developed by Acuity AI Advisory in consultation with the Law Society of Ireland.

Acuity AI Advisory
Buttermilk Lane,
Downings North
Prosperous,
Kildare W91 K2N7
E hello@acuityai.co
W www.acuityai.co

Law Society of Ireland,
Blackhall Place,
Dublin 7,
D07 VY24

E solicitorservices@lawsociety.ie
W www.lawsociety.ie