KEMP IT LAW

Tech Law at the Apex

LAWTECH

What to look out for in a LawTech implementation contract: **checklist**

Richard Kemp & Eleanor Hobson

June 2023

This checklist sets out the key issues that a law firm customer should focus on when negotiating a LawTech contract to help them secure more meaningful contractual commitments than the provider may initially offer. It takes into account the Law Society LawTech and Ethics Principles which were published in July 2021.

Technology providers generally divide their standard form contracts into three parts:

1 Software (covering the platform).
2 Professional Services (covering the implementation).
3 Statement of work (covering the detail).

Software Agreement

This part is divided into three:

- general points,
- points where the software is provided on premises 'as a licence' and
- points where the software is provided in cloud 'as a service'.

Issue	What the customer needs
	General
Definition of "user"	As licence or subscription fees are generally determined by user count (alternatively, 'seats'), clarification is required on: • Who counts as a user. • Whether there are different "types" of user. • Whether use is limited to certain department(s). • Whether use is limited to certain group companies. • Whether legal team administration staff, contractors and IT team members are included. (Note if any of those are in a different department/group company than the permissions above). • Who outside the legal team is included. (Again, note if any of those are in a different department/group company than the permissions above).
Trial or pilot	Certain providers may offer free trials or pilots for customer assessment. Consider if you can renew/extend the free trial/pilot or if there are any "quid pro quo" terms permitting collateral use of trial data.
Data portability and end of life transition and data portability	Data portability during the term and end of service transition should be considered up front to ensure that changing provider does not mean starting from scratch or losing out on the customer's investment during the term. For example, for a document management system (DMS), document review, contract lifecycle management (CLM) or artificial intelligence (AI) product, where users have been labelling or structuring documents or data, or training AI models, it would be worth considering: • Portability. Ensure that you can transfer your data and/or documents to a new system (including the structure, compatibility and comprehensiveness – for example, by retaining hyperlinking, schema, metadata and labels or tags). Consider asking for an example of what the output would look like. Check if it is possible to extract data and documents throughout the term.

Issue	What the customer needs
	• AI model transition. Have a plan for how to retain the value of, or transition away from, trained AI models (for example by labelling data outside the platform, using middleware that retains training datasets, extracting training data (with labels and metadata) and retaining a copy of the model). Consider regularly extracting training datasets throughout the term (including metadata) to allow training of other AI systems. It may be worth considering if there are any standard input requirements of third party systems to which Customer would transition. See also "Use, return, deletion and anonymisation of documents, data or models"
Liability and mechanism of redress	In July 2021, the Law Society published its guidance paper, Law Society LawTech and Ethics Principles (Law Society LawTech Guidance). The Law Society LawTech Guidance is not mandatory but provides guidance as to the main ethical concerns that should be considered when procuring LawTech products. The Law Society recommends that customers should agree "a mechanism for redress" with the provider should the LawTech not be used as it was intended (page 20, Law Society LawTech Guidance). The customer should be careful to ensure that any liability exemptions or liability caps agreed with the provider do not operate to frustrate, or undermine, any mechanism of redress provided for under the contract (for example, a breach of contract claim). Similarly, it is good practice for a customer to negotiate a contractual requirement for the provider to carry sufficient insurance to cover its liability under the contract (page 24, LawTech Guidance).
Change of control or subcontracting	Customer should consider the risks associated with another entity obtaining control of the provider (including any data it may be hosting on behalf of the customer via the LawTech solution) or of providing such data to a subcontractor. If this poses data protection, client confidentiality or regulatory risks then the customer could consider requiring consent to any proposed change of control or subcontracting.
Free services	The Law Society warns that "free" services offered by providers may involve payment for extras, or generate income from processing data about the customer's firm or its clients, which can pose serious data protection, client confidentiality and information security risks (page 23, Law Society Lawtech Guidance). This should be considered, and where necessary, investigated further.
Explainability	Customer should also consider including provisions that allow it access to sufficient information to be able to explain to clients (and other relevant stakeholders) how the LawTech is being used and achieves a given outcome. In AI projects, the Law Society recommends that the customer should have access to plain English explanations of how the AI arrives at conclusions, together with the underlying data and code (page 17, LawTech Guidance). Under the UK GDPR, Customer may also have obligations to provide meaningful information about the logic, significance and consequences of the system, and allow individuals to exercise their rights to objection and human intervention.
Where the software is provided on premises "as a licence"	
Price and payment	Licence fees are generally determined by user count, etc (alternatively, 'seats'). Customers should consider the duration of the deal and watch out for increasing charges.
Payment start date	Providers generally want licence and maintenance fees to be made payable from when the software is delivered not when the customer first uses it. Customers should check whether they can arrange a retention against milestones and acceptance, including as against interoperability with other LawTech software and meeting future developments and functionalities on the roadmap. If the software involves any training of AI or other configuration, customer should assess whether to start with a smaller number of users during training or configuration before wider roll-out (together with acceptance).

Issue	What the customer needs
Licence scope	Confirmation that any use of the software is covered by the licence fee or whether "indirect use" is charged separately. For example, "talking to" other systems.
Support and maintenance	Support and maintenance is typically between 18-22% of the contact value. The customer should seek commitments on: • Availability. That maintenance will be provided throughout the project lifecycle (for example, for ten years). • Pricing. That maintenance charges will be held for several years and then subject to maximum annual increases. • Specification. That the software will conform to the specification. • KPIs and service levels. There should be a defined service credit regime that escalates to termination for multiple outages. • Updates and patching. As a minimum, there should be an obligation on the provider to provide a mechanism for downloading security updates and patches for known vulnerabilities.
Escrow, disaster recovery and business continuity	Escrow, business continuity and disaster recovery arrangements should be considered from a security and data protection perspective as well as technical and business.
Where the software is provided in cloud "as a service" (SaaS)	
Price and payment	Pricing will generally be per user (seat) and based on periodical (monthly, quarterly or annual) subscription charges (licence and maintenance rolled up). Customers should consider the duration of the deal and watch out for increasing charges. Customers should also keep an eye on hosting charges and terms. There is a trade-off between agreement term and pricing. Customers should beware that there is generally no right to terminate for convenience before the term ends, and that the provider will generally look initially for the whole balance of the price to be paid on early termination.
Service levels	The service credit and escalation regime should be defined in terms of: • Availability. • Response times. • Other KPIs.
Data Protection	Data protection is a complex area of the law, particularly following Brexit where two distinct schemes now operate in the UK and the EU, with the UK principally governed by the UK GDPR, but with the EU GDPR continuing to have extra-territorial effect in some circumstances. With respect to the UK GDPR, the customer should check: • That the data processing terms in the contract adequately reflect the mandatory requirements stipulated in the UK GDPR. • Whether the provider is (or is purporting to also be) a controller to any extent (and customers should question why and for what purposes). (Of particular concern is if any sensitive data is included – e.g. signatures, data room content relating to health or financial information). • Whether the provider requires you to obtain *consent* to any processing, whether consent is the appropriate lawful basis and, if so, how you would obtain it. (Of particular concern is if the Provider is requiring the Customer to obtain consent to the transfer of personal data to third countries). • Whether there are any sub-processors and their security arrangements. Customer may want

Issue	What the customer needs
	to consider requiring prior consent or notice to changes to the provider or location of the data centre. • The location of any data centres, "follow-the sun" support and other sub-processors, and if outside the UK, which UK GDPR data transfer mechanism is relied upon and (if applicable) whether Provider has carried out a "Transfer Impact Assessment" (TIA) or "Transfer Risk Assessment" (TRA), what supplementary measures have been implemented and if the importer produces any Transparency Reports or other documentation on how they respond to third party (and government) requests for data. • Whether Provider has carried out any impact or risk assessments (TRAs, TIAs, DPIAs or LIAs) or transparency reports (see above) and requesting copies, together with updates going forward. • Carrying out due diligence on the technical and organisational measures implemented by the provider under Art.32 UK GDPR, such as requiring the LawTech provider (or their subcontractors, or both) to complete a security questionnaire, to comply with the customer's obligations as controller. • Where Provider might use the data for their own purposes, the lawful basis for transferring the data to Provider (and whether any data can (or should) be anonymised or redacted before upload to the services). • In addition to thinking about the lifetime of the arrangement, the customer should check if any personal data contained in data or models may be retained by any other party at the end of the services. • Ensure that all relevant privacy notices are updated, how privacy information could be delivered to relevant data subjects, and noting that the Provider should be listed as a "recipient" in response to any data subject access request ("DSAR"). As well as UK GDPR, check whether EU GDPR might also apply, for example, if the business has offices, employees or clients in the EU.
Storage	Customers should assess any hosting or storage costs and consider: How affordable scaling the solution would be (for example, if it was successful or it relates to a long-term matter such as a long running dispute or long term client). How versions and in-version changes are implemented and controlled, especially where co-authoring or collaborating between departments or with third parties. (For example, if multiple fee earners are collaborating on a due diligence report or statements of case it may be important to be able to track individual changes). How data can be retired from the system, while retaining the value of any structuring (for example, retaining metadata, tags, versions, scope of access to application programming interfaces (APIs), integration with other solutions). (See also "Data portability and end of life transition" and "Use, return, deletion and anonymisation of documents, data or models".) Whether third party access can be provided (for example, client care access to bibles or real-time billing information, online collaboration, file sharing), how it can be isolated from the rest of the system and kept secure, and how permissions between third parties can be controlled (for example, different bidders accessing a data room should not be able to view others' access or notes, while a client and external counsel may want to collaborate on witness statement drafts).
Use, return, deletion and anonymisation of documents, data or models	Customers should ensure that they have certainty that: • Any independent use by the LawTech provider of documents, data or AI models does not compromise business intellectual property (IP), including checking the scope of any IP licence. • All data can be anonymised, accessed, deleted and returned at will. • Any models can be deleted or retrained at will.

Issue	What the customer needs

	• Provider is obliged to delete documents, data and models at the end of the services (or that appropriate restrictions are in place regarding any post-termination use by provider).
	• Any permissions regarding provider post-termination use of customer or matter data or models trained on such data don't cut across any other obligations the customer may have, such as:
	  ○ client confidentiality obligations whether under client terms of service, law or regulation (for example, the SRA Code of Conduct);
	  ○ privilege protections;
	  ○ retention periods in client terms of service or retention policies (including any data protection policies if any personal data might be included);
	  ○ NDAs, particularly where the relevant information might relate to a third party (for example the target company of an aborted acquisition by a client);
	  ○ other data protection obligations (for example data subject rights of deletion or access);
	  ○ IP licences;
	  ○ regulatory obligations relating to listed or regulated clients; or
	  ○ conflicts.
	In reviewing the above, if any AI models are deployed or licensing permissions include training AI, Customers should bear in mind that tests of AI models are increasingly demonstrating that AI models do not "forget" training data and can be manipulated accidentally (or deliberately) to reproduce it. In particular Customers should consider:
	• Whether to allow Providers to re-use or allow other customers or third parties to access models trained on Customer data.
	• Whether to use or permit the use of AI models trained across multiple customers' data.
	• Whether to request separate AI models or instances for different clients' data, particularly for matters requiring information barriers or that require conflict approval.
	• Whether to require all personal data, legal advice/comments or other sensitive information to be anonymised/redacted prior to any collateral use.
	• How data subjects will be informed, personal data can be deleted or how a DSAR would be responded to. If marginalia comments or other documents or communications might be privileged and how they can be separated from the remaining population.

Cloud migration in lifecycle	The customer should be paying no more for software over the lifecycle of the contract than if the software had stayed on-premises. However, this may be difficult as: • You are comparing [perpetual licence fees + upgrade fees + annual maintenance] with [annual subscription fee + maintenance rolled up]. • There will be a paid-for professional services element for the cloud migration. • There will be extra hosting (infrastructure, platform as a service) subscription charges in the cloud model that aren't comparable with the on-premises model.

Professional Services Agreement

Issue	What the customer needs
RFP responses	Provider's request for proposal (RFP) responses are warranted as true, complete and accurate.
Governance	The agreement has workable processes and procedures around Acceptance, Change control., Dispute resolution and Governance.
Acceptance	Any "deemed acceptance" and the consequences of failure to pass acceptance tests are set out. For example, the right to terminate and get money back if there is no acceptance on a '3 strikes

Issue	What the customer needs
	and you're out' basis or by a longstop date.
Customer responsibilities	The customer's duties are set out in a reasonably detailed statement. The provider can only rely on a customer breach if the customer is notified in writing and will "fix first, fight later" and try to avoid or remedy the breach.
Modifications	Confirmation whether software will be installed "out of box" or customised. If software is to be customised or modified, including if any AI models are being trained (see below), answers to the following questions should be required: • Who is authorised to make the modifications? • Will the modified software be part of standard maintenance? • Will the modified software be supported in the next version or release? • Who owns the rights to the modified software? • Are any modifications provided to other customers (particularly relevant if you have an independent iteration of an AI model or if multiple customers benefit from training, taking into account the impact on the customer's business IP)? (See also "Data portability and end of life transition" and "Use, return, deletion and anonymisation of documents, data or models" above)
Compliance	Confirmation that provider is performing duties compliantly, and that the provider's services and software comply, with all applicable laws. The provider will likely not agree that the solution will comply with any regulatory requirements that the customer (as a regulated law firm) may be subject to, so the customer should ensure these are met (for example, by ensuring the proposed services and LawTech solution are compliant with its obligations under the SRA Code of Conduct).
Conversion	Specific commitments around data conversion from the previous system and end of service data extraction to any new system. (See also "Data portability and end of life transition" and "Use, return, deletion and anonymisation of documents, data or models" above.)
Completeness	Confirmation that there is no other software (proprietary, third party or open source), hardware or services that the customer needs, except as expressly set out in the agreement.
Compatibility	Confirmation that the solution is, and will remain, compatible and integrated with other named key customer systems.
New versions	Clarity on: • Release dates for new versions of the software. • Whether new versions (as opposed to enhancements and releases) are chargeable. • Whether customer modifications are interoperable with the new version. • Provider's product upgrade or end of life policy.
Security	Duties on provider that known vulnerabilities will be regularly & promptly monitored & patched.

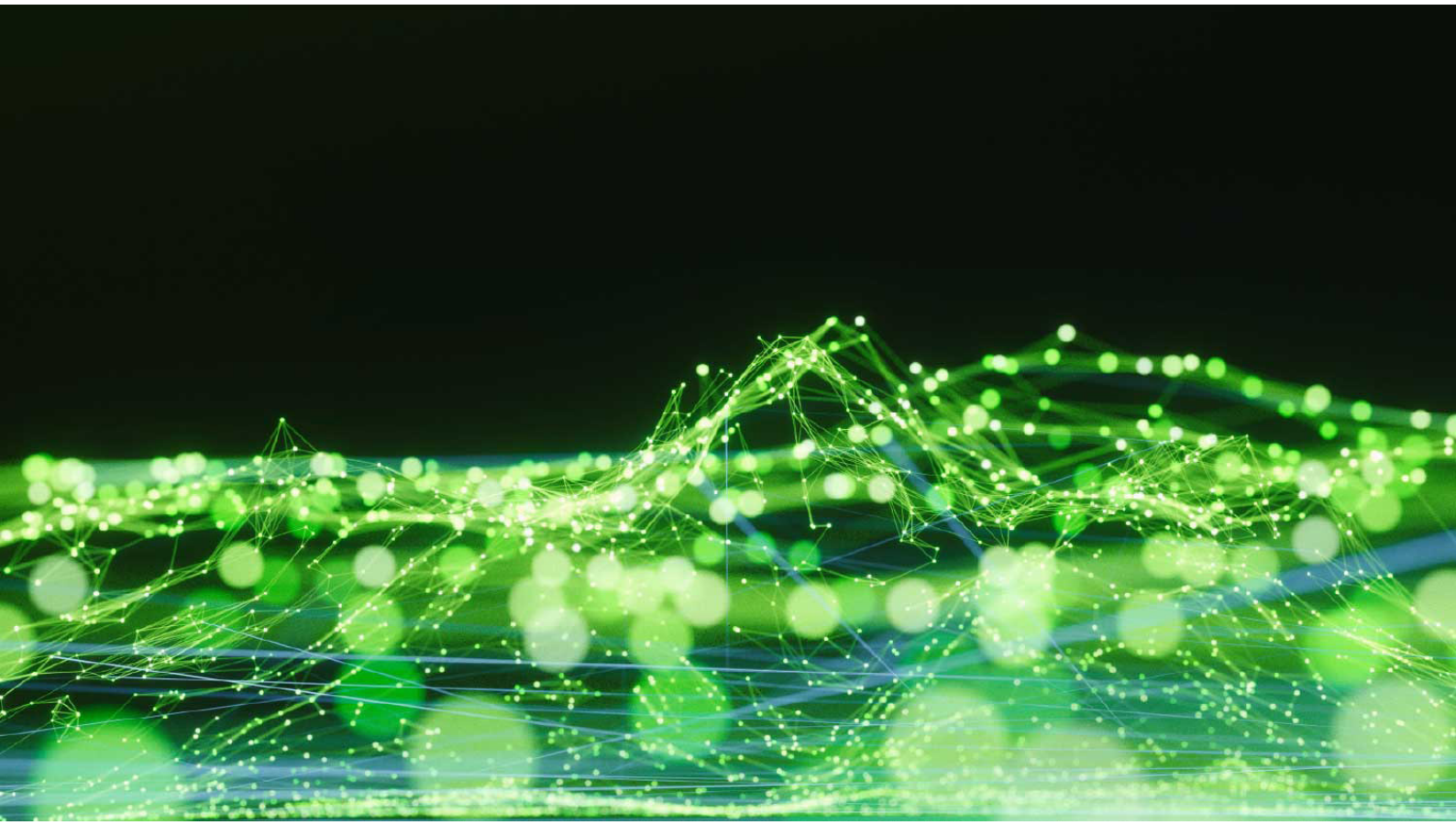
Statement of work

Issue	What the customer needs
Project management	The provider is at its weakest in a competitive tender at the moment of signature and will use its project management office (PMO) to claw back after signature what it lost before. The customer needs to run an effective PMO to manage this risk.
Training	Consider whether the provider provides any training on the system or the broader technology that may be helpful for your team or employees (for example, training on how the AI system works more broadly). The Law Society recommends that customers should maintain a record of which employees have undertaken training and training dates, and that it should obtain clear and accessible materials on

Issue	What the customer needs
	how to use the LawTech compliantly, so that it can fulfil its regulatory duty to effectively communicate its use of LawTech to its clients (page 15, Law Society LawTech Guidance). For example, as above, the customer's client should have access to plain English explanations of how any AI arrives at conclusions (page 17, Law Society LawTech Guidance).
Security assessment	The customer should carry out its normal security assessment of the provider to verify that the provider's solution aligns with the customer's data protection and information security policies.
Solicitor's regulatory assessment	The Law Society recommends the customer should carry out a risk analysis or impact assessment of the provider's proposed solution to ensure it complies with the customer's obligations as a regulated law firm, to identify and mitigate potential risks, and identify what the customer, and the provider, are accountable for. This should be documented in the contract (page 19, Law Society LawTech Guidance). As the risk assessment will be dependent on the particular solution adopted, this might be best set out in the statement of work. An example of an issue which might arise from a risk assessment is the use of AI as part of the LawTech solution. The law firm may need to seek its client consent before using AI as part of a particular matter which the LawTech will be assisting with, so an ability to turn the AI functionality on or off (for individual cases) may be necessary. Another example is that if the customer is using LawTech for document review before disclosure, its supervision process should include steps relating to quality assuring the results. (See also "Use, return, deletion and anonymisation of documents, data or models" above.)
Continuity	A contractual commitment regarding the continuity of the provider's key personnel throughout the implementation.
Resource levels	Confirmation that the provider will meet resource levels stated in the statement of work (SOW).
Resource swap out	Swap out or replacement of resources at no cost to the customer.
Price and payment	Confirmation that: • Pricing of unit resources will remain unchanged during implementation. • The price will not exceed the agreed ceiling if the scope remains unchanged. • Payment for services will be tied into project milestones and final acceptance.
Timesheets	Invoicing (whether monthly or by milestone) to be supported by timesheets with agreed data.
Project plan	Initial, then detailed, project plans (and a timeline) will be completed or signed off as stated in the SOW. Time is generally not of the essence but dates should be binding.
Project documents	Customer may freely use and disclose to other contractors or providers all project documents. All project documents should be generally understandable to a person reasonably skilled in LawTech.
Responsible officer	Where AI forms part of the LawTech solution, the Law Society recommends that the provider should appoint a responsible officer who the customer can contact with questions or concerns (page 19, Law Society LawTech Guidance). The customer should also appoint its own responsible officer who its clients and employees can contact with questions and concerns. Where relevant, this assistance should include assisting the customer with its obligations (including the one month deadline) in relation to automated decision making under Articles 13, 14 and 22 of the UK GDPR (meaningful information about the logic, significance and consequences, and the rights to objection and human intervention).
Access, authentication and oversight	The Law Society recommend that customers identify the required access, authentication and oversight level required for the LawTech solution (page 21, Law Society LawTech Guidance). In addition to provisions in the Software Agreement, the customer may prefer to have this documented as part of the Statement of Work, for the avoidance of doubt.

KEMP IT LAW

Tech Law at the Apex



Richard Kemp
Partner

T: 020 3011 1670
M: 07932 695 615
richard.kemp@kempitlaw.com

Eleanor Hobson
Associate

T: 020 3011 1671
M: 07599 109 097
eleanor.hobson@kempitlaw.com