Guide on the Adoption of LegalTech for Law Practices

Guide on the Adoption of LegalTech

FOR LAW PRACTICES

16 October 2023

The Law Society of Singapore

© The Law Society of Singapore (16 October 2023)

Acknowledgements

This Guide was developed by The Law Society of Singapore's Information Technology Committee. With special thanks to the following Committee Members who put together the early drafts and checklist:

- Dharma Sadasivan
- Heng Jun Meng
- Kao Kwok Weng Jonathan
- Lim Mingguan
- Lim Seng Siew
- Prasad s/o Karunakarn
- Smith Benjamin Yiwen
- Wong Li Ming Rachel
- Zachary Ng Cher-Ping

There are a number of useful resources published by professional bodies locally and in other jurisdictions that can aid practitioners and law practices in their LegalTech journey. The Committee is grateful and privileged in having guidance from publications on legal technology by the Singapore Academy of Law (*Legal Technology Manual*, 2019), and The Law Society of England and Wales (*Introduction to LawTech*, 2019, and *Lawtech: A Comparative Analysis of Legal Technology in the UK and in other Jurisdictions, 2019*).

Executive Summary

The aim of this Guide is to aid law practices in adopting sound practices and, together with other guides published by The Law Society of Singapore, managing technology risks as they adopt technology in various areas of their practices.

The extent and degree to which a practice implements this Guide should be commensurate with the level of risk and complexity of the practice and the LegalTech being considered. While efforts will be made to update this Guide, the rapid pace of development and change in technology may mean that specific references and terms in this Guide may become outdated from time to time but the spirit and principles are likely to remain relevant. Law practices can also look to other resources for more information such as the Legal Industry Digital Plan published by the Ministry of Law and the Infocomm Media Development Authority ("**IMDA**") that serves as a guide for law practices undertaking their digitalisation journey.

This Guide is not intended to be comprehensive nor replace or override any legislative provisions. It should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation(s) made under the relevant legislation(s), as well as written Practice Directions, Guidance Notes, notices, codes and other guidelines that The Law Society of Singapore may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

Table of Contents

Part 1: Overview

1. Introduction

1.1 The status of this document is that of a Guide from The Law Society of Singapore. This Guide sets out different criteria that a law practice may use in assessing whether a specific legal technology or legal technology service (collectively, "**LegalTech**") or Solution[1] is suitable for their practice.

1.2 This Guide will be useful for:

- Practitioners in law practices;
- Persons who supervise or work as in-house information technology professionals in law practices; and
- Outsourced legal technology vendors of law practices

1.3 In applying this Guide, law practices should take a risk-based approach in deciding whether a specific LegalTech or LegalTech provider is suitable for their practice. This is because law practices vary in terms of size, type and the nature and demands of their clients. Further, international law practices may require that all their offshore practices, including those in Singapore, adopt their LegalTech or LegalTech providers.

2. Scope and Qualifications

2.1 This Guide is not prescriptive and does not offer an exhaustive list of criteria and considerations applicable to all law practices. Certain criteria may not be relevant or may otherwise not represent an appropriate level of prudence for a law practice's specific circumstances.

2.2 Each law practice will need to examine its operations in detail and decide whether a specific LegalTech or LegalTech provider will fit the practice's specific needs. Law practices may wish to seek professional advice and services where necessary.

2.3 This Guide does not in any way detract from a law practice's or practitioner's professional and ethical obligations, nor is it intended to create additional ethical or professional obligations for a law practice or practitioner.

[1] As used in this Guide, a "**Solution**" is an implementation or packaging of legal technology/technologies or service/services, people, and/or processes, to support or meet a law practice's requirements.

Part 2: Types of Technology/Role of LegalTech

3. Types of Technology / Role of LegalTech

3.1 Scope of Software

3.1.1 Enabler Technology

3.1.1.1 Enabler technology is system-level technology that facilitates digitalisation throughout a law practice's operations. An example of this is document management systems that store, organise and manage legal documents for easy retrieval and secure sharing.

3.1.2 Back-Office Technology

3.1.2.1 Back-office technology enhances the efficiencies of back-office functions. An example of this is a practice management system. Such a system would manage records and files via a centralised database, allowing a law practice to be more efficient in administrative tasks such as tracking billable hours, generating invoices, consolidating instructions and communications, and managing deadlines.

3.1.3 Front-Office Technology

3.1.3.1 Front-office technology supports practitioners in the execution of rote legal tasks. This broadly includes four major areas:

(a) Knowledge management Solutions – software which allows lawyers to share internal knowledge, and organize and harness previous legal research and documents to be repurposed for current client matters

(b) Document assembly software – allows the transformation of frequently used documents and/or clauses into templates for quick production of customised documentation, reducing the time required to produce routine documents not requiring heavy customisation, and may also include the assembly and compilation of a suite of transaction documents

(c) Document review software – aids practitioners' review of documentation by using pattern recognition and statistical analysis to discover anomalies, locate patterns and identify clause-level differences

(d) E-discovery software – enables the process of discovery to be carried out electronically and adds value by being able to remove duplicates, identify related items and suggest the relevancy of documents

3.2 Hardware

While much of the current focus of LegalTech revolves around software Solutions, the hardware is equally important in enabling access to and delivery of the software Solutions. For larger law practices, these may be managed and monitored through a service provider including troubleshooting and replacement.

3.2.1 User Devices

3.2.1.1 These are the devices that are required to access the software portion of the LegalTech Solution. This would include:

(a) Personal computers / Laptops / Notebooks

(b) Mobile phones

(c) Tablets

(d) Other mobile or smart devices (e.g. connected televisions, displays or smart monitors)

3.2.1.2 Many LegalTech software Solutions have been designed to be accessible regardless of operating system or platform but there may still be compatibility issues.

3.2.1.3 Further, less mainstream devices and lower budget devices are less likely to have the same level of support as mainstream devices and may also be more prone to security vulnerabilities.

3.2.2 Input / Communication

3.2.2.1 Common devices include keyboards, mice, styli, touchpads and graphics/signing tablets.

3.2.2.2 With the surge in remote and flexible work arrangements following the COVID-19 pandemic, communications devices such as webcams and wired and wireless microphones and headsets/earpieces have also become part of a law practice's standard assortment of devices.

3.2.3 Network Infrastructure

3.2.3.1 This varies in complexity but at its most basic enables the user device to connect to the internet and other devices on the network.

3.2.3.2 This may be a single device functioning as a gateway, router and wireless access point, and for more complicated set-ups, this would include individual pieces of hardware performing each function (e.g. separate gateway, firewall, router, switches, wireless access point).

3.2.4 Servers

3.2.4.1 Traditionally, a server is a device on a network that provides certain services that can include authentication, email, and database and file access and management.

3.2.4.2 These days, a "server" can take the form of multiple devices, a single multi-service device, and it can be located on-site/on-premise, or off-site, whether at another of the law practice's locations, or the premises or data centres of a service provider.

3.2.5 Storage / Backup

3.2.5.1 Having only 1 copy of a law practices' files on the user's device is highly risky and may not be practicable if storage space is limited. More likely than not, users will need another physical storage media (e.g. external hard disks, SSDs or flash drives, network attached storage) or online or cloud storage Solution.

3.2.5.2 A commonly used 3-2-1 backup strategy contemplates multiple storage media and locations:

(a) 3 copies

(b) 2 forms of media

(c) 1 off-site

3.2.5.3 Each storage Solution has its own benefits and drawbacks ranging from cost, capacity, reliability, speed, ease-of-use and accessibility.

3.2.6 Productivity / Office Solutions

3.2.6.1 This can include devices or Solutions used and shared in the office.

3.2.6.2 Examples include shared office printers or multi-function devices, as well as security and monitoring and access control Solutions. It may also include meeting room and presentation Solutions especially devices that will be connected to the law practice's network.

3.3 Artifical Intelligence

3.3.1 Artificial Intelligence ("**AI**") is likely to have a major effect on law practices but the full extent of its ramifications has yet to reveal itself. Generally, AI is expected to improve administrative aspects of law practices, such as improving search capabilities (e.g. for email, document discovery, research, etc), business administration workflows (e.g. customer relationship management, financial forecasting, etc), and more.

3.3.2 Meanwhile, Generative AI ("**GenAI**") is the subject of some controversy. Some consider GenAI's potential to generate legal documents a powerful productivity enhancer, while others view it as a threat that undermines the value of legal practitioners. Still others take the view that GenAI will be counterproductive in generating legal documents because of its tendency to "create new things", whereas legal practitioners generally prefer following precedents that have been drafted with careful consideration.

3.3.3 Other concerns relating to GenAI are also emerging, such as its impact on reliability of evidence, its use in the preparation of submissions, and exploration of the use of GenAI by the Courts of various jurisdictions.

3.3.4 The adoption of AI (in all its different flavours) in the legal industry remains an open discussion and is beyond the remit of this Guide at the time of publication. However, practitioners interested in procuring LegalTech solutions in the AI space may still find current LegalTech resources and guidance relevant.

3.4 Role of LegalTech

3.4.1 Some of the important functions of LegalTech are as follows:

(a) To help the law practice remain competitive in the modern marketplace by keeping up-to-date with technological advancements in other industries and the evolving expectations of clients;

(b) To deliver legal services to clients in a more efficient (both in terms of costs and timing) and accurate manner, improve client engagement and risk management, as well as to expedite legal procedures;

(c) To improve the work-life balance of practitioners; and

(d) To automate repetitive and/or mundane tasks.

3.4.2 While certain LegalTech tools have been exclusively developed for lawyers and law practices, it may also be useful to consider whether there are technology tools developed outside of the legal industry, which can also be applied within the legal industry. This may include messaging or communication suites, accounting and invoicing software, and project or matter management tools.

Part 3: Barriers to Adoption

4. Time-Cost / Orientation / Change Management

4.1 The introduction of new technologies often requires orientation, detailed instructions, a transition period, and for larger organizations, staggered rollouts and a team to manage the process.

4.2 Practitioners are constantly under pressure to grow their practice and meet billing targets along with other obligations such as fulfilling their CPD requirements. Time spent learning or adopting new technologies is often hard to justify when the new technologies are poorly understood by decision-makers, and returns are usually intangible and often not immediately appreciable.

5. Budgeting and Margins

5.1 Apart from the non-billable time needed to be spent on identifying and adopting the new technologies, there is also the issue of cost and funding for the new technologies. Depending on the law practice's structure, this would require the buy-in of the relevant fee-earners whose profits would be used to fund the acquisition.

5.2 Technology appears to often have the greatest success in high volume, low margin industries. Anecdotally, manual processes at law practices contribute to higher margins contributing perhaps to less motivation for the introduction of new technologies to remove inefficiencies.

5.3 In a similar vein, manual processes may also need to be relied upon where the client is less advanced or in need of legal aid. Costs of adopting LegalTech may then need to be recovered in some other way including through services provided by the law practice.

6. Nascent Technologies / Early Adopters / Regulatory Hurdles

6.1 With the sheer number of products and Solutions available, law practices need to be sufficiently resourced to be aware of these products and Solutions and to be able to understand and assess them. Smaller law practices may be more focused on delivering actual services and advice and lack the capacity to manage adoption, migration and administration of new LegalTech Solutions.

6.2 At the same time, there may be products, Solutions and service providers that are so new that they are untested and have no track record for law practices to consider or, where applicable, qualify for any incentives or grants to help law practices with technology adoption.

6.3 Law practices are rightfully concerned about their professional responsibilities, client confidentiality and data protection. Law practices may be more forthcoming in adopting and exploring new technologies if an industry-wide standard that is recognized by the legal profession or a regulatory sandbox is set up for law practices to trial LegalTech Solutions.

Part 4: Drivers and Motivations

7. Client-Pressure

7.1 Need for efficiencies

7.1.1 In the B2B space, pressure has been building from clients for law practices to achieve greater efficiencies via a greater use of technology, and in some instances what and how technology is being used. There is increased pressure on fees particularly from larger client organisations with greater buying power looking for increased value for money from their legal budgets, with deliverables that can only be achieved through the use of LegalTech or in some cases, clients expressly require certain LegalTech be used.

7.2 Transparency

7.2.1 One area where client pressure is directly translating into LegalTech adoption is in the space of legal cost transparency. In-house legal departments have anecdotally found law practices opaque when it comes to legal fees, often complicated by multiple suppliers all billing with very different systems and processes. Billing is often abstract and difficult for in-house teams to decipher.

7.2.2 While high costs associated with legal services have been tolerated due to the risks associated with poor legal advice, there is now much greater attention paid to legal service providers and law practices as even legal services become subject to quantification and cost and efficiencies are valued as much as quality.

7.2.3 Transparency on cost is also beneficial for the law practices which have traditionally been unsophisticated in their use of financial metrics and management information.

7.2.4 In most other sectors, metrics like average order value and profitability per project or per client are scrutinised and optimised. Law practices have traditionally been less focused on this and more interested in other measures such as profit per partner. Better transparency on cost and fees will also therefore help law practices better understand their services, how to price them and what tech could create efficiencies.

7.2.5 Better management information on metrics such as ‘cost to acquire’, ‘cost per client’ and ‘return on investment’ of business development activity are useful by-products of greater client transparency and the cultural shift towards driving efficiencies.

8. Market Pressures

8.1.1 Competition has been intensifying in the legal services market for some time. In the corporate law sector, new market entrants with a greater variety of operating models and non-licensed or non-licensable practices offering law-adjacent services have been putting pressure on law practices. Legal Process Outsourcing companies with a focus on industrialising processes and driving efficiencies have been effective early adopters of LegalTech.

8.1.2 While larger law practices have more scope to invest in LegalTech, some vendors are gaining more traction in the mid-market – in particular younger, more nimble law practices that are more entrepreneurial and looking to differentiate their services from larger law practices.

8.1.3 Technological innovations make it easier and faster for organisations to transact and interact with one another. This has improved the speed and method of information transfer or dissemination. Many industries have shifted to an electronic model, including the shift to digital marketing and the development of electronic products and services as well as methods of online distribution of content.

8.1.4 In turn, LegalTech adoption is a potential source of differentiation for smaller law practices with ambitions to take on larger, more profitable work. An example here would be boutique law practices considering M&A work delivered primarily via technology, whereas previously they would have needed an army of associates or junior lawyers, unaffordable to them.

8.1.5 There has also been an increase in the number of law practices which are supportive of staff teams at all levels having greater flexibility of working. This cultural shift away from having to be physically present in the office is driving the need for greater mobility and agility, requiring an appropriate technology infrastructure to support it. The move away from traditional offices towards 'opening up of the law practice' is placing greater demands on technology and IT to deliver a mobile working environment.

8.1.6 The current generation of lawyers now entering the workforce is in the main 'digital native' with digital technologies engrained in their everyday life. Expectations that technology should be the same in the workplace as it is at home – as well as this higher level of tech literacy – should promote LegalTech adoption.

8.1.7 The impact of Environmental, Social and Governance investing and analysis across all industries affects law practices both as practices in and of themselves, and as service providers subject to scrutiny and review by clients. Technology and the responsible use of technology play an important role in a law practice's performance in this area.

9. Profession-Led

9.1 <u>Incentives / Cost recovery</u>

9.1.1 There may be other drivers in the industry. Stakeholders such as the judiciary and governmental agencies have been exploring and adopting digital Solutions in various forms in recent years.

9.1.2 It is not unlikely that there may be efforts to incentivise the use of LegalTech through various cost measures such as limiting the use of or recovery of costs for the use of physical documents, or allowing the recovery of part of the costs for the use of LegalTech in a particular matter.

Part 5: Funding Strategies

10. Access to Capital

10.1 The availability of capital plays an important role in spurring innovation and adoption of LegalTech. The legal profession can take cues from established funding strategies in other areas of technology – from angel investment to pre-IPO. As public and private attention on LegalTech grows, so too should the interest in adoption and opportunities for funding and investment.

10.2 For law practices looking to adopt new LegalTech, it is not uncommon for Solutions to be more affordable as an early adopter. Often, early adopters effectively enjoy "subsidised" rates to spur adoption and aid the new LegalTech in gaining traction. This comes with a degree of risk that the LegalTech may not be fully tested and may not succeed in the long-term.

10.3 With the continued push for the adoption of LegalTech throughout the profession and digitisation as a national strategy, at the time of publication, law practices can still avail themselves to grants and subsidies that incentivise productivity and innovation with eligibility criteria that generally encompass most Singapore law practices. These can help offset some of the onboarding and initial acquisition costs as well as some early recurring costs. While such grants and subsidies can be significant, law practices should be aware that these are temporary and should factor in subsequent recurring costs, if any.

10.4 Law practices will need to factor in costs for the LegalTech especially after the expiry of the grants and subsidies. Depending on the LegalTech, this may be a direct cost or disbursement chargeable to the client, or part of the law practice's operating budget. While there have been suggestions for a fixed cost or percentage chargeable to all clients, it is not clear whether such an approach is justifiable or permissible under current ethical and professional rules.

11. Incubators / Pilot Projects

11.1 Some larger law practices, local and international, now have their own or related technology incubators. Incubators provide LegalTech providers with easier access to decision-makers and end users, but that does not guarantee that the technology will go on to be adopted.

11.2 Some of the more successful incubators are allowing LegalTech providers access to real business opportunities in a safe, controlled and supported environment where Proof of Concept or pilot projects[2] can best be deployed.

[2] "**Proof of Concept**" and "**pilot project**" have similar meanings but very generally a "**Proof of Concept**" refers to the implementation of a Solution to determine if it works or is suitable and a "**pilot project**" is the initial implementation of the Solution at a smaller scale usually to identify and resolve any teething issues.

11.3 LegalTech providers that successfully progress from the incubator may then be taken on by the law practices in a scaled fashion, or even selected to form the basis for an industry-wide platform.

12. Equity Stakes / Spinouts

12.1 There are public reports that some law practices are taking equity stakes in LegalTech providers such as Luminance and LUPL. Benefits of this approach for the LegalTech provider may include potentially gaining access to live client work from which to train and develop its technology, while the investing law practice has the opportunity to gain early access, provide feedback, and to tailor and adapt the technology to its client base. When the LegalTech is generally available to other law practices, law practices with similar requirements are likely to benefit from the work already done to develop and tailor the technology. Whether as investors or users, law practices should ensure that they properly discharge their professional and ethical obligations when engaging with LegalTech providers.

12.2 There are also other examples of law practices investing in LegalTech or where an employee within a law practice has decided to set up their own LegalTech provider and it makes sense for the entrepreneur's law practice to stay close to the LegalTech provider and help it develop and grow.

Part 6: Considerations

13. Professional Responsibilities

13.1 Interactions with Practitioners' Professional and Ethical Obligations

13.1.1 Use of Cloud Computing in LegalTech

13.1.1.1 Some LegalTech service providers will utilise cloud services to offer their Solutions to law practices. This presents some issues in relation to a practitioner's professional and ethical duties. Practitioners may take guidance from *Guidance Note 3.4.1* issued by The Law Society of Singapore to offer guidance on the interaction between cloud computing and a practitioner's professional and ethical obligations and the issues that a law practice should consider when engaging cloud computing service providers.

13.1.2 Client Confidentiality

13.1.2.1 LegalTech may be used to process or host a law practice's data, that may include confidential client data. A law practice should enquire how the LegalTech service provider processes and stores such data, whether it has access to such data, and whether it retains such data.

13.1.2.2 If the law practice is not satisfied that a LegalTech service provider will be able to preserve the confidentiality of such data, the law practice should consider engaging a different LegalTech service provider.

13.1.2.3 A law practice should also ensure that it has adequate policies and practices to preserve data privacy and client confidentiality.

13.1.3 Security

13.1.3.1 Cybersecurity threats are perpetually present, placing the information technology systems of law practices at risk. Law practices must examine the security of service providers and their own internal systems.

13.1.3.2 The Law Society of Singapore has released a *Guide to Cybersecurity For Law Practices* on 30 March 2020 ("**Guide to Cybersecurity**") which may be referenced for insights into how a law practice may assess cybersecurity and the practices it may adopt to ensure good cybersecurity.

13.1.4 Testing, Quality Assurance and Records

13.1.4.1 Law practices should monitor and assess systems employing LegalTech products and services on an ongoing basis to ensure that the LegalTech products and services allow the law practice to uphold its professional and ethical duties. Such risk management and supervision should incorporate a structured quality assurance programme for the Solutions(s) the law practice buys or uses.

13.1.4.2 Records of the outcomes of all testing should be maintained as part of the law practice's quality assurance programme in order to demonstrate efforts for compliance with risk assessment and management. If testing reveals any risks, these should be added to the law practice's risk register and then reduced over time as a result of regular risk review meetings and actions. If a risk is not able to be reduced, the law practice should document the reasons for the law practice's inability to reduce such risk.

13.1.4.3 Law practices should consider organising the regular, preferably annual, penetration testing of any Solution by an external assessor with suitable technical expertise. Any penetration test should be accompanied by a written report detailing the outcome of a test and identifying any weaknesses or failures that need to be addressed. Any perceived failings should be addressed in a reasonable and proportionate manner depending on the severity of the risk identified and the reasonable resources available to manage that risk.

13.1.4.4 Law practices should also consider assessing their preparedness in responding to a cyber-attack that could lead to a data protection breach of its Solution. In this regard, law practices may reference the Guide To Cybersecurity for the good and enhanced practices in relation to security measures a law practice should consider.

13.1.4.5 All quality assurance, either internally or from external assessors, should be recorded and all recommended actions should be carried out without any undue delay.

13.1.5 Responsibility of Law Practice

13.1.5.1 A law practice is ultimately responsible for meeting its legal and professional duties. Such duties and obligations cannot be outsourced to LegalTech service providers and remain squarely on the law practice. The extent and degree to which a law practice implements this Guide should be commensurate with the nature of risks in, and materiality of, the service arrangement with the LegalTech service provider. Law practices should observe not just the text but the spirit of this Guide in their decision-making. A law practice should ensure that any LegalTech services it receives (whether provided by a service provider or its sub-contractor) is performed and managed as if the services were performed or managed by the law practice itself.

13.1.5.2 Where the Solution has the potential to affect client's money, conflict of interest or confidentiality, law practices should pay particular attention to Rule 35 of the Professional Conduct Rules that requires, *inter alia*, the management of the law practice to take reasonable steps to ensure they have in place adequate systems, policies and controls for ensuring compliance with the relevant legislation, Practice Directions, Guidance Notes, and rulings.

13.1.6 Unauthorised Person Acting as Advocate or Solicitor

13.1.6.1 Law practices should be cognizant of the risk of breaching the Legal Profession Act 1966 ("**LPA**") if legal advice is given through the use of LegalTech software, such as chatbots or a document assembly software, without the involvement of an advocate or solicitor.

13.1.7 Remote Advice

13.1.7.1 There may be situations in which law practices may not have the opportunity to meet their clients in person. In the event that a law practice chooses to provide remote advice, it is essential that the law practice take the necessary steps to verify their client's identity and legal capacity. Further, in order to comply with the standards of adequate professional service, law practices should also provide adequate information on fees, costs and the progress of the client's matter. In this regard, please see *Guidance Note 6.1.1* issued by The Law Society of Singapore.

13.1.8 E-Signatures

13.1.8.1 In client or know-your-client matters, there are many instances where wet ink signatures can and have been replaced by electronic forms such as signing with a touchscreen or stylus, affixing an image of signature onto the relevant documentation, or more secure digital signatures involving cryptographic keys, certificates and other means to verify the signature and whether the document has been altered since signing.

13.1.8.2 Greater security may also be used in conjunction with such electronic signatures where the user of the signature is verified and authenticated, and changes made after the signature is affixed or highlighted. These signatures are typically known as either secured electronic signatures or digital signatures.

13.1.8.3 Please also see the Electronic Transactions Act 2010, *the* "*Working Remotely – What Do I Need To Do?*" article published by The Law Society of Singapore on 3 April 2020 and check for any notices from regulators and government bodies to determine the enforceability of an e-signed document.

13.8.4 Please note that at the date of this Guide, certain documents, such as deeds of trust and powers of attorney, are not recognised if they are signed electronically.

13.1.9 Social Media / Marketing / Publications

13.1.9.1 Law practices should be cognizant of the media attention that may be generated from proceedings and exercise proper discretion in such circumstances. Practitioners should refrain from making inappropriate comments, improper disclosures or inaccurate statements. In this regard, law practices should implement internal policies on the use of the internet and social media at work.

13.1.9.2 Practitioners should pay particular attention to Rules 7(3), 37 and 38 of the Legal Profession (Professional Conduct) Rules 2015, as well as *Practice Direction 6.1.1: Media Comments and Internet / Social Media Posts* and *Practice Direction 6.2.1: Advertisement and Media Publicity* issued by The Law Society of Singapore.

13.1.10 Misconduct

13.1.10.1 With readily accessible technologies and the sheer volume of data and information on demand, there is growing concern over information disorder and privacy issues especially the potential for misuse and abuse including online harassment, cyberstalking and even aiding a client in the commission of technology-related offences. Practitioners may also find themselves tempted given the privilege and respect accorded to the profession, and how closely they work with their clients and peers.

13.1.10.2 Practitioners should be mindful of the responsibilities entrusted to them as lawyers and members of the Bar. Practitioners are expected to conduct themselves honourably and with integrity. Members of the Bar found guilty of misconduct unbefitting an advocate and solicitor as an officer of the Supreme Court or as a member of an honourable profession may be liable to be struck off the roll.

14. Regulatory Matters

14.1 Competition Concerns

14.1.1 As the legal industry continues to grow and change alongside LegalTech, practitioners will no doubt turn to each other to share knowledge and experiences or even collaborate on trialling or adopting new Solutions. While such exchanges are often productive and can benefit the industry, caution needs to be exercised lest such conduct becomes anti-competitive.

14.1.2 For further considerations when collaborating on or discussing Solutions among law practices and practitioners, please see the *Business Collaboration Guidance Note* issued by the Competition and Consumer Commission of Singapore.

14.2 Personal Data Protection

14.2.1 Law practices should note that the Personal Data Protection Act 2012 ("**PDPA**") applies to law practices and that law practices are subject to the full extent of regulatory obligations and requirements under the PDPA. Please see the *Data Protection Advisory* issued on 12 July 2019 by The Law Society of Singapore, and the *Guide To Cybersecurity and the Guide To Securing Personal Data In Electronic Medium* issued on 20 January 2017 by the Personal Data Protection Commission of Singapore.

Part 7: Legal Tech Checklist

15. Acquisition of Solutions

15.1 Review and Assessment of Solutions

15.1.1 Before procuring a LegalTech Solution, law practices should thoroughly review and assess the Solution in light of their needs and circumstances. Law practices can take guidance from publications by various professional bodies as well as the Legal Industry Digital Plan ("**IDP**") published by the Ministry of Law and IMDA that serves as a guide for law practices undertaking their digitalisation journey.

15.2 Strategy and Project Management

15.2.1 Law practices should clearly designate stakeholders who are responsible for the overall technology adoption or acquisition strategy for the law practice. These stakeholders should be responsible for providing direction, guidance and oversight of specific projects to ensure consistency in strategy and project management, as well as ensuring that milestones are reached, and deliverables are realised in a timely manner. Where manpower is available, specific teams can be formed under the guidance of the responsible stakeholders for the acquisition of particular Solutions.

15.2.2 Stakeholders should equip themselves with the relevant knowledge to carry out and discharge their responsibilities and shall keep abreast of developments through continuing education.

15.2.3 Law practices should be clear about their objectives and requirements when considering a particular Solution. This may include feasibility analyses, cost-benefit analyses, business case analyses and vendor assessment.

15.2.4 A risk management process should also be established, even at early stages, to identify and assess potential risks, as well as to monitor and address such risks if and when they arise during the project.

15.2.5 In adopting or acquiring a new Solution, law practices should set out a detailed plan for the project identifying the scope, milestones and deliverables, as well as responsibilities of the parties involved at each stage.

15.2.6 For smaller practices or sole practitioners, it may not be possible or practical to have a meaningful size of stakeholders to manage the strategy or project. It is nonetheless important that they identify and seek input from users in their practice who will actually use the Solution or be affected. In such circumstances, the sole practitioner or stakeholder may need to seek service providers that will be able to provide greater assistance in planning and managing the project.

15.3 Acquisition

15.3.1 Law practices should establish appropriate criteria for the evaluation and selection of vendors. These criteria may include the vendor's (i) qualifications, (ii) track record, (iii) development and support practices and processes, (iv) data security and localisation policies, (v) contingency and disaster recovery plans, (vi) onboarding and transitional services, (vii) and where appropriate peer reviews and recommendations.

15.3.2 Given the importance of a law practice's data (not limited to client data), law practices should ensure that their data remains within their control and is portable[3] – i.e. it will not be stored or exported in proprietary formats that could result in a loss of access to the data or inability to change vendors.

15.4 Design and Implementation

15.4.1 Law practices should establish a framework to manage the system development life cycle proportionate to the level of customisation of the Solution. This should take into account analyses of the law practice's requirements against the Solution's features, the design, implementation, testing and acceptance of the Solution.

15.4.2 For commercial off-the-shelf-Solutions, law practices are unlikely to have significant insight or input into the development life-cycle but it remains vital for law practices to identify, define and document its requirements, and properly manage the implementation, testing and acceptance of the Solution.

15.5 Management

15.5.1 It is important that law practices are aware of the need to monitor and manage the Solution throughout its entire lifecycle. This includes configuration management, refresh management, patch management, change management, and incident management.

15.5.2 It is not uncommon to discover that Solutions are at times misconfigured, depriving law practices of desired features or otherwise exposing systems to unnecessary risk.

15.5.3 With more Solutions moving to subscription-based models, law practices need to be familiar with how existing and further Solutions are being provided. This will be a key consideration especially if a Solution will be reaching EOSL[4] status and cease receiving support and updates, and the law practice must assess whether the Solution should be replaced by an alternative or a different consumption model.

---

[3] This is related to the data protection concept of "data portability" where data should be available across organisations in a common machine-readable format.

[4] "**EOSL**" means End-of-Service-Life or End-of-Support-Life, where the piece of technology (hardware or software) is no longer supported by the manufacturer.

15.5.4 Law practices must also be familiar with how the Solution will be kept up-to-date, taking into account patch and update schedules as well as ensuring these are implemented with minimal downtime and do not cause compatibility issues with the law practices' other Solutions.

15.5.5 Smaller law practices that are not able to have a dedicated support team should pay particular attention to business continuity planning and ensure that their records can still be retrieved and accessed in the event of a service outage or the proprietor or practitioner with access and control is incapacitated. The latter may involve safekeeping access keys in physical form.

15.6 The following checklist sets out some key considerations in exploring and adopting a Solution. Law practices and practitioners should familiarise themselves with the elements of the checklist and where appropriate seek further information independently, including referring to other resources such as the Legal IDP published by the Ministry of Law and IMDA, or from their service provider to understand the element or satisfy themselves that the element is or is not fulfilled.

15.7 For the avoidance of doubt, the checklist should be considered a starting point rather than a comprehensive checklist. Law practices can expand and add to the checklist as appropriate, as well as determine whether there are elements that may not be relevant and can be omitted in light of their specific circumstances. If any element is relevant but not satisfied or fulfilled, the law practice or practitioner should consider and take any remedial action if appropriate.

15.8 The checklist does not create new ethical or professional obligations, and completion of this checklist alone does not absolve a law practice from any existing obligations.

No.	Description	Checklist	Comments
Project management			
1	Is there an individual or team appointed to manage the project?	□ Yes □ No	
2	Are the roles and responsibilities of the individual or individuals involved in the project clearly defined and documented?	□ Yes □ No	
3	Does the responsible individual or individuals possess the relevant knowledge or capability to review the Solution or vendor?	□ Yes □ No	
4	The law practice has identified relevant criteria to assess the service provider and is satisfied that the vendor meets those criteria.	□ Yes □ No	
5	Deliverables and milestones for the Solution are clearly defined and documented.	□ Yes □ No	
6	Has the Solution been reviewed for the law practice's compliance with internal policies, statutory and regulatory requirements, and professional obligations?	□ Yes □ No	
7	Is there a plan for ongoing monitoring and management of the Solution? (e.g. review of suitability and considering alternatives, monitoring and implementing updates and patches)	□ Yes □ No	

Ensuring alignment / clarity on the Solution			
8	What sort of Solution are you assessing? Note: Some products may provide multiple Solutions.	□ Practice management □ Legal research □ Knowledge management □ Matter management □ Document management □ KYC / AML / CDD and other risk and compliance □ Document assembly / automation □ Document Review □ E-discovery □ Data analytics / business intelligence □ Core business functions (e.g. email, office suite, etc) □ Accounting and finance □ Chatbots □ Internal communications □ AI-driven Solutions □ Network infrastructure □ Hardware (User devices, input devices) □ Hardware (Productivity / office Solutions) □ Hardware (managed Solutions) □ Hardware, others (to specify) □ Others (to specify)	

Ensuring alignment / clarity on the Solution			
9	Who are the stakeholders or intended users? Note: Some products may involve multiple stakeholders.	□ Lawyers □ Legal support staff □ Law practice management □ Finance staff □ IT staff □ Business development staff □ Others	
10	Has the law practice sought input and feedback from key stakeholders and intended users on their expectations of the Solution and their experience using the Solution?	□ Yes □ No	
11	Is the Solution aligned with your broader IT strategy?	□ Yes □ No	
Security and compatibility			
12	Is the Solution compatible with your existing IT systems?	□ Yes □ No □ Partially	
13	Is the vendor's on-boarding and troubleshooting plan appropriate for your law practice?	□ Yes □ No □ Partially	
14	Does the vendor provide maintenance and support for the Solution? If so, how long will the vendor continue to support the Solution?	□ Yes □ No □ Partially Response:	
15	Are the vendor's security and data protection policies for the Solution clear and appropriate for your law practice? **OR** Are the vendor and/or Solution certified against internationally recognised standards?	□ Yes □ No	

16	Is the vendor transparent about any data security incidents it has experienced?	□ Yes □ No	
17	Is there any publicly disclosed data security incidents affecting the vendor or Solution?	□ Yes □ No	
18	If data is stored in the Solution (e.g. files, documents, images) or there is data generated from the Solution (e.g. analytics), is it capable of being migrated or exported for use by you or on third party Solutions?	□ Yes □ No □ Partially	
19	If there is data from or is stored in the Solution, does the vendor provide backups of the data? If so, (i) how frequently; and (ii) how quickly can the backups be restored?	□ Yes □ No	
20	Has the vendor provided details of its support of the Solution? • In particular: • guaranteed uptime • advance notice for scheduled downtime • remedies for unscheduled downtime (e.g. service level credits) • response times in the event of problems • hotline or other notification details	□ Yes □ No □ Partially	
21	If you are replacing or disposing any equipment or storage media, have you made arrangements to ensure confidential data is destroyed or cannot be recovered from the equipment or storage media?	□ Yes □ No	
Personal data protection			
22	Is the data in the Solution stored only in Singapore or across various countries?	□ Singapore Only □ Various countries □ Either / Both possible, at customer's option	
23	If the data is stored outside Singapore, will the vendor store/process it in line with PDPA requirements at a minimum?	□ Yes □ No	

24	Have you determined whether the vendor is a data intermediary in relation to the handling of personal data?	□ Yes □ No	
25	Have you requested and assessed information from the vendor relating to how the Solution ensures that personal data remains protected?	□ Yes □ No	
26	Have you agreed on a data breach / incident response plan with the vendor?	□ Yes □ No	
27 (a)	Has the vendor suffered a data breach in the past?	□ Yes □ No	
(b)	If "yes", are you satisfied that the vendor has taken adequate precautions to ensure such breaches do not occur again?	□ Yes □ No □ Partially	
Confidentiality			
28	Does the service agreement with the vendor contain adequate protections for confidential data?	□ Yes □ No □ Partially	
29	Have you determined how confidential data is to be returned or destroyed upon the termination or expiration of the service agreement?	□ Yes □ No □ Partially	
Financial Considerations			
30	What is the pricing structure of the Solution? Note: Pricing structure may be a combination of various methods (e.g. Initial acquisition or onboarding fee and regular subscription/licence fees).	□ Pre-paid credits □ Post-paid, consumption-based □ Subscription-based (e.g. per user, per month / year) □ One-time lump sum □ Monthly / Annual maintenance fees	
31	Have you factored in possible price changes by the vendor during the duration of your agreement for the Solution? (e.g. inflation, labour cost increases, etc.)	□ Yes □ No	

32	Is there a fixed or minimum contract term for the Solution? If "yes", are the costs of early termination clear and acceptable?	□ Yes □ No	
33	Are there any add-on services that may incur additional costs? (e.g. on-boarding, helpdesk, backups, access to backups, data migration, data export, etc.)	□ Yes □ No	
34	Are any grants available for the Solution?	□ Yes □ No	
35	Will signing a service agreement with a vendor before submitting a grant application render you ineligible for the grant?	□ Yes □ No	
Communication			
36	Do you have a plan for communicating the procurement of the Solution to your law practice and championing its adoption?	□ Yes □ No	
37	Have you fixed and announced the cut-over date / phasing in timeline for implementing the Solution?	□ Yes □ No	
38	Have you arranged / conducted training for end-users in using the Solution? Can the vendor provide this (if required)?	□ Yes □ No □ Yes □ No	
39	Do you have a plan (preferably discussed and agreed with the vendor) for addressing teething problems upon rolling out and implementing the Solution?	□ Yes □ No	
40	Have you identified and communicated the consequences that may arise if users do not use the Solution as required?	□ Yes □ No	

16. Risk Management

16.1 There are inherent risks associated with the adoption of any Solution. These risks should be taken into account during acquisition or adoption and measures should be taken to continually identify and mitigate such risks.

16.2 Practitioners can refer to the Guide to Cybersecurity for insights and practices to be adopted.