THE LAW SOCIETY OF SINGAPORE

GUIDANCE NOTE 3.4.1

CLOUD COMPUTING

1. This Guidance Note takes effect on 10 March 2017.

A. Introduction

2. Cloud computing can be described generally as IT services provided by a cloud service provider ("**service provider**") which users can access on demand through the Internet.

3. Cloud computing is most commonly used for storing and transferring files across several devices. Common cloud services include Microsoft Office 365, Google Drive, Dropbox and Amazon Web Services.

4. Cloud computing has its benefits, including:

   (a) Enabling lawyers to work remotely from anywhere with an internet connection.

   (b) Reducing the costs of document management. This could potentially level the playing field for smaller law practices by helping them handle voluminous documents despite having fewer support staff and limited office space.

   (c) Enabling lawyers to spread out their costs, as many cloud services are subscription-based and billed monthly.

   (d) Providing a level of IT security that meets or exceeds that which is available from on-premises solutions within law practices.

5. While it has its benefits, a cloud computing arrangement, like any technology project, may give rise to certain issues. You must understand what these issues are and whether, as a result of these issues, there is a risk that your ethical and professional obligations may be compromised.

6. Your ethical and professional obligations include obligations under:

   (a) the Legal Profession Act (Cap 161, Rev Ed 2009) ("LPA");

   (b) the Legal Profession (Professional Conduct) Rules 2015 ("PCR");

   (c) the Personal Data Protection Act (Act 26 of 2012) ("PDPA");

   (d) the Personal Data Protection Regulations 2014 ("PDPR").

7. Provided that the issues outlined in this Guidance Note are properly addressed, the Law Society has no objection to the use of cloud services. The common service models and deployment models can be found in **Annex A**.

B. Scope of this Guidance Note

8. This Guidance Note is not prescriptive and is only a guide. It sets out generally the factors you should take into account in deciding whether to use cloud computing services, the issues that may arise and possible steps to address them. You can modify our suggested

steps in this Guidance Note. Depending on the circumstances, steps other than those suggested in this Guidance Note may also be appropriate.

9. This Guidance Note does not in any way detract from your professional and ethical obligations.

10. The Law Society does not endorse or prohibit you from using any particular service provider.

11. The following is a summary of the issues that may arise, your relevant professional and ethical duties, and our guidance on addressing these issues:

Part	Issues	Relevant duties (non-exhaustive)	Guidance
C	General issues	Ensuring adequate systems to maintain client confidentiality (rule 35(4) PCR)	The management of the law practice must take reasonable steps to ensure that the law practice has adequate systems, policies and controls in place to maintain client confidentiality
D	Your data is stored in servers overseas	Obligation to protect personal data (section 24 PDPA) Obligation not to transfer personal data out of Singapore without ensuring a standard of protection comparable to that required under PDPA (section 26 PDPA, regulation 9 PDPR)	Understand where your data is stored In relation to personal data, seek clients' consent if data is stored overseas or ensure that the transfer complies with the other exceptions under section 26 of the PDPA In relation to personal data, where client consent and other exceptions under the PDPA are not available, ensure that the data is stored in Singapore only
E	Your service provider has access to your data, or accesses your data to respond to a foreign authority's request	Duty of confidentiality (rule 6 PCR)	Ensure contractual terms state that your provider will not access your data for any secondary purpose (i.e. any purpose other than for providing the service to you – such as advertising) Consider if the service provider has a policy on government and law enforcement data access
F	Business continuity and access to your documents	Duty of competence and diligence (rule 5 PCR) Duty to retain documents for prescribed periods of time – e.g. section	Ensure contract provides for a minimum service availability and compensates you if this standard is not met Ensure service provider has continuity plans and procedures in place and that these are regularly

Part	Issues	Relevant duties (non-exhaustive)	Guidance
		70E LPA	tested and updated to minimize risk of service disruption Require service provider to return data to you in a non-proprietary format if the provider becomes insolvent Back up key documents so you can access them during service disruption
G	Security measures by service provider	Obligation to protect personal data (section 24 PDPA) Duty of confidentiality (rule 6 PCR)	Select a service provider with appropriate security measures in place (e.g.accreditation, encryption technology that meets or exceeds international standards) Take reasonable steps to negotiate for contractual remedies if your provider is hacked Ensure your law practice has good internal security practices
H	Service provider could retain data after client retainer ends	Obligation to retain personal data only as long as necessary (section 25 PDPA) Obligation to return documents when retainer ends	Ensure contract provides for permanent deletion of data, including backup copies

C. General Issues Arising from a Cloud Computing Service Arrangement

12. If you consider that your law practice will benefit from using cloud computing services, you must decide on an appropriate service provider to engage.

13. In selecting a service provider, you could consider the provider's experience (including specific experience in the legal services sector) and reputation, and its registered address and location.

14. You must understand the issues that may arise from a cloud computing service arrangement and whether there is a potential risk that your professional and ethical obligations will be compromised as a result of these issues. The management of the law practice must take reasonable steps to ensure that the law practice has adequate systems, policies and controls in place to maintain client confidentiality (rule 35(4) PCR).

15. You must also understand the issues that may arise if the service provider uses sub-contractors, is acquired by another entity, or if the contract is otherwise assigned or novated.

16. You should, where possible, sign negotiated agreements with service providers, instead of 'take-it-or-leave-it' contracts.

D. Your Data is Stored in Servers Overseas

17. Service providers offer services from data centres in different locations across the world. Backing up data to multiple locations safeguards data in case servers in one location are damaged or destroyed.

18. You should be aware of where your data is stored. The laws in some jurisdictions may not offer comparable levels of protection to the laws here, and may permit foreign authorities to access your client's data without following appropriate legal processes.

19. You must protect personal data your law practice has. Under the PDPA:

    (a) Section 24 requires that your law practice make reasonable security arrangements to protect personal data in its possession or under its control.

    (b) The law practice has the same obligation regarding personal data processed by a data intermediary for its purposes as if the personal data was processed by the law practice itself (section 4(3)). Service providers may be data intermediaries for the purposes of the PDPA.

20. You must not transfer personal data out of Singapore unless you take appropriate steps to ensure that the recipient of the personal data is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA (section 26(1) PDPA and regulation 9(1)(b) PDPR). This requirement is satisfied if:

    (a) The legally enforceable obligations are imposed in accordance with regulation 10 of the PDPR. Legally enforceable obligations include obligations imposed on the recipient under any law, or under any contract. A contract must:

        (i) require the recipient to provide to the personal data a standard of protection that is at least comparable to the protection under the PDPA, and

        (ii) specify the countries and territories to which the personal data may be transferred under the contract;

    (b) Your client consents to the transfer. In order to rely on consent, you have to provide to your client a reasonable summary in writing of the extent to which the personal data in that country or territory will be protected to a standard comparable to the protection under the PDPA (regulations 9(3)(a) and 9(4) PDPR); or

    (c) The other exceptions in regulation 9(3) of the PDPR apply – including where the transfer is necessary for the conclusion or performance of a contract between the law practice and third party which is entered into at your client's request (e.g. if a law practice engages local counsel in another jurisdiction, at the client's request); or which a reasonable person would consider to be in your client's interest.

21. We recommend that law practices insert in their engagement letters a clause informing clients:

    (a) That the law practice makes use of cloud services and clients' data may be stored overseas; and

(b) That the law practice will disclose details of their service providers at the clients' request.

22. The Personal Data Protection Commission provides a number of examples of how to comply with the PDPA when transferring data.

23. While you are not prohibited from storing data overseas, if you cannot obtain client consent or meet any exceptions in the PDPA, you should consider whether to use cloud providers that store data exclusively in Singapore.

24. The personal data may include the data of your law practice's staff and third parties. If so, your law practice must also ensure compliance with the PDPA in relation to such data stored in servers overseas.

E. Your Service Provider has Access to your Data, or Accesses your Data to Respond to a Foreign Authority's Request

25. You must maintain the confidentiality of any information which you acquire in the course of your professional work (rule 6(1) PCR). You may disclose confidential information if the client authorizes the disclosure (rule 6(3) PCR).

26. The use of cloud computing services may result in the disclosure of information that is confidential to your client. You should consider inserting clauses in your engagement letters to obtain the necessary consent from your client.

27. It may be that no information that is confidential to the client is stored on a cloud storage service. However, if there is confidential information stored on a cloud storage service, you should consider the following:

(a) Whether the service provider can access stored documents and, if so, whether the service provider commits not to use the data for any purpose other than providing the service (such as advertising).

(b) Whether the documents can be encrypted by the user before it is stored or whether your service provider uses encryption technology that meets or exceeds international standards. (You must exercise proper supervision over your staff in accordance with rule 32 PCR. If documents are to be encrypted before uploading to the cloud, steps must be taken to educate staff and workflows designed to ensure that this takes place.)

(c) Whether the service provider recognises your obligations to maintain client confidentiality.

(d) Whether the service provider uses sub-contractors to deliver its services and whether it accepts liability for any breach of confidentiality they commit.

28. In relation to sub-contracting, you must understand if the sub-contracting is for the whole or part of the subject matter of the contract, whether you can withhold consent to the sub-contracting, or if you have the right to review the terms of the sub-contract. You should take reasonable steps, where possible, to negotiate that the service provider is fully liable for the performance of the sub-contract.

29. In relation to a foreign government accessing your documents, consider whether the service provider has a policy on government and law enforcement data access including a commitment:

(a) not to hand over data to a third party unless required to do so by law;

(b) to redirect the request to you unless prohibited by law; and

(c) not to hand over encryption keys to third parties.

F. Business Continuity and Access to your Documents

30. You owe your client a duty of competence and diligence (rule 5 PCR). You may not be able to discharge this duty if, due to service disruption, you cannot access key documents stored on the cloud.

1. Availability of cloud services

31. You should consider whether the service provider will provide guarantees on when the cloud will be available.

32. Service providers commonly guarantee a minimum amount of “uptime”, e.g. guaranteeing their servers will be available 99.9% of the time. You should understand how your provider defines “service availability”:

(a) Point of measurement: availability of service provision or availability at the point of user consumption. This is normally a percentage figure.

(b) Service measurement period: even if a service boasts high availability, this could translate into relatively high downtime during normal working hours. Some providers may exclude scheduled maintenance from their availability measurements.

(c) Application availability: availability of particular applications may be just as important to you as general availability of a service.

2. Compensation if service is unavailable

33. You should also understand what compensation will be provided in case of service unavailability. Your provider may exclude or limit liability for your direct or indirect losses if their service is unavailable.

34. Service providers commonly offer service credit if they fail to meet their service level agreement, e.g. offering a period of free usage should a disruption of a certain threshold happen.

35. You should weigh up the relative merits of this regime against damages at common law. Accepting service credits as your sole and exclusive remedy may limit your right to sue for damages at large or to terminate the contract.

36. In general, if you keep hardcopies or other backups of documents, service credit regimes are likely to be adequate as they offer certainty and keep risk to identifiable and manageable levels.

3. Service provider should have continuity plans

37. You should ensure the service provider has continuity plans and procedures which are regularly tested and updated to minimize the risk of service disruption. Such plans could include:

(a) Redundancy arrangements to ensure that it can continue to operate if its IT infrastructure fails, or the cloud becomes unavailable.

(b) Whether the service provider backs up data, and if so, how often are backups done. You should be allowed access to a copy of the back-up data if there are cloud outages or if the service provider's IT infrastructure fails.

4. Other business continuity considerations

38. You should consider ensuring that if your service provider becomes insolvent or is restructured, you should be able to recover the data and transfer it back to your own IT infrastructure or to another service provider. The data should be returned in an industry standard, non-proprietary format.

39. You should consider backing up key documents so you can access them during service disruptions.

40. You should consider the risks associated with another entity obtaining control of your service provider. You should take reasonable steps, where possible, to negotiate appropriate terms to ensure that your interests are protected in such an event, e.g. negotiating:

(a) that you are given advance notice of any proposed change in the control of the service provider;

(b) that you have the right to terminate the contract; and

(c) that your prior written consent is required for any assignment or novation of the rights and obligations of the service provider.

41. You should also take reasonable steps, where possible, to negotiate that your service provider does not have the right to suspend services at its discretion. Alternatively, you should take reasonable steps, where possible, to negotiate appropriate terms to ensure your interests are protected, e.g. to permit suspension only for material breach or non-payment, and with prior notice.

42. You should consider how to properly store and protect your documents even if you do not use cloud computing. One should be careful not to overestimate the risk of unfamiliar technologies and underestimate the risk of existing methods of work. Physical documents or documents stored on internal servers may be lost through theft or fire, and having cloud backups could be a lifesaver in such situations.

5. Ensuring documents are stored for the requisite period of time

43. You must maintain documents and records for a prescribed period – e.g. for at least 5 years as part of the prevention of money laundering and financing of terrorism requirements (section 70E LPA). Documents include documents in electronic form.

44. You must also ensure authorities can gain access to your documents if necessary. Under the LPA, the Law Society or the Legal Services Regulatory Authority may request a law practice to produce documents or information:

(a) If required to produce any document or information as required by Council of the Law Society for purposes of prevention of money laundering and financing of terrorism inspection (section 70F LPA).

(b) If required by the Director of Legal Services to produce any documents or information (section 2C LPA).

45. You should ensure that the service provider does not delete any documents stored on cloud service storage without your consent.

G. Security Measures by Service Provider

46. Most major service providers invest significant resources in security. Depending on your law practice's current practices, storing documents on the cloud could be more secure than storing them on internal servers or as hardcopies.

47. You should find out from the service provider the security measures it has to protect data stored on the cloud. You may wish to ask:

(a) If your service provider uses encryption technology that meets or exceeds international standards; and

(b) if your service provider has any recognized accreditations.

A list of accreditations and further resources can be found in **Annex B**.

48. You should also take reasonable steps, where possible, to negotiate that your service provider will compensate you if it is hacked.

49. Although the service provider has security measures in place, your law practice should still ensure that it has its own IT security measures in place. Proper practice management is not the focus of this Guidance Note. However, we have included some illustrations to show how poor security practices or poor understanding of technology – as opposed to technology per se – can result in breaching your ethical obligations.

50. You should understand how to use technology.

Illustration: You run a sole proprietorship with support from your secretary. Both of you have global administration rights over all your documents stored on the cloud. You and your secretary have a dispute and she leaves your law practice. You find out that she has revoked your access rights entirely so you can no longer access your documents.

Guidance: Here the difficulties resulted because the lawyer did not understand or properly allocate administrator rights. You, and not your client or support staff, should retain administrator rights to your documents.

51. You should explain and enforce your security policies.

Illustration: After extensive negotiation, you have signed a contract with a reputable cloud services provider. The IT department sends an email announcing that all staff should use the new cloud platform from now on. The reason for the switch is not clear and other free cloud websites are not blocked on the law practice's computers. Your staff continue to transfer files via their personal cloud accounts or by sending emails to themselves.

Guidance: "Free" cloud services may generate income from processing data about you. They can pose serious data protection, client confidentiality and information security risks. Everyone in your practice should be alerted to these risks, and be

made aware of the need to use only approved service providers.

52. You may wish to refer to the Law Society's Practice Management Manual for a more comprehensive guide to best practices. We encourage all members to adopt a holistic approach to security.

H. Service Provider could Retain Data after Client Retainer ends

53. When you delete data from your cloud services account, it may not necessarily be deleted from all of your service provider's servers. For example, your service provider may temporarily retain deleted documents in case users deleted them by accident.

54. You have professional duties when your retainer ends (see rule 26 PCR). You should retain personal data only as long as necessary (section 25 PDPA) and return all documents which belong to your client when your retainer ends. Hence, you should be aware of your service provider's data retention policies, and ensure you can permanently delete or remove copies of the document stored with a service provider. You should retain absolute ownership of all data.

Date: 10 March 2017

THE COUNCIL OF THE LAW SOCIETY OF SINGAPORE

Annex A: Overview of Cloud Service and Deployment Models

Annex A gives background information on cloud computing for members' understanding.

There are three common service models:

(a) Software as a Service (SaaS), where the service provider makes available software applications to customers;

(b) Platform as a Service (PaaS), where the service provider provides a computing platform for customers to develop and run their own applications; and

(c) Infrastructure as a Service (IaaS) where the service provider delivers IT infrastructure e.g. storage space or computing power.

There are four common deployment models, with Public Cloud being the most common:

(a) Public Cloud: Infrastructure is owned and managed by the service provider and located off-premises from the customer. Although data and services are protected from unauthorized access, the infrastructure is accessible by a variety of customers.

(b) Private Cloud: Infrastructure is usually managed by the service provider but sometimes by the customer. Infrastructure is located either on the customer's premises or, more typically, on the service provider's premises. Data and services are accessible exclusively by the particular customer.

(c) Community Cloud: Serves members of a community of customers with similar computing needs or requirements. Infrastructure may be owned and managed by members of the community or the service provider. Infrastructure is located either on the customer's premises or the service provider's premises. Data and services are accessible only by the community of customers.

(d) Hybrid Cloud: A combination of two or more of Public Cloud, Private Cloud, or Community Cloud.

Annex B: Accreditations and Further Resources

Annex B gives a non-exhaustive list of accreditations:

(a) Multi-Tier Cloud Security (MTCS): The MTCS Singapore standard is developed under the Information Technology Standards Committee (ITSC) for service providers in Singapore. A list of MTCS-certified service providers can be found on the Infocomm Media Development Authority's website.

(b) ISO 27018: Focuses on privacy and personally identifiable information.

(c) ISO 27001: Focuses on cybersecurity.

(d) SSAE 16 SOC 1 and 2.

(e) CSA Star.

The following resources may also help you to better understand cloud security measures:

(a) The Personal Data Protection Commission's Guide to Securing Personal Data in Electronic Medium (first issued on 8 May 2015, revised on 20 January 2017). Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf.

(b) The Legal Cloud Computing Association (LCCA) Security Standards. The LCCA is a group of cloud computing companies which collaborates with bar associations and law societies to formulate standards. These are available at http://www.legalcloudcomputingassociation.org/standards/.