DREW & NAPIER

# Legal Considerations in Negotiating Cloud Contracts

10 April 2017


Charmian Aw
Director, Commercial Services

# Overview

1. Legal framework in Singapore
2. Stages in the cloud vendor and customer relationship
    a) Due diligence
    b) Contract drafting and negotiation
    c) Ongoing audit, review and enforcement

# 01
# Legal framework

# Personal data protection regime

A “data intermediary” is an organisation which:

•processes personal data **on behalf of** and **for the purposes of** another organisation (but does not include an employee of that other organisation)

•**pursuant to a contract** which is evidenced or made in **writing**

*“processing”, in relation to personal data, means the* ***carrying out of any operation or set of operations in relation to the personal data****, and includes any of the following:*

a) *recording;*
b) *holding;*
c) *organisation, adaptation or alteration;*
d) *retrieval;*
e) *combination;*
f) *transmission;*
g) *erasure or destruction*

# Personal data protection regime

- "*An organisation* ***shall have the same obligation under this Act*** *in respect of personal data processed on its behalf and for its purposes by a data intermediary* ***as if the personal data were processed by the organisation itself****.*" (Section 4(3), PDPA)

- A data intermediary is subject to limited data protection obligations under the PDPA, in respect of its data processing activities as a data intermediary, namely:
  - Protection Obligation (Section 24, PDPA)
  - Retention Limitation Obligation (Section 25, PDPA)

# Personal data protection regime

| Organisation | Data Intermediary |
|---|---|
| 1. Consent Obligation | |
| **2. Purpose Limitation Obligation** | |
| 3. Notification Obligation | |
| **4. Access and Correction Obligation** | |
| 5. Accuracy Obligation | |
| **6. Protection Obligation** | **6. Protection Obligation** |
| **7. Retention Limitation Obligation** | **7. Retention Limitation Obligation** |
| **8. Transfer Limitation Obligation** | |
| 9. Openness Obligation | |

# Personal data protection regime

- Many of the PDPC's enforcement decisions released to-date deal with the breach of the Protection Obligation by organisations and/or their data intermediaries
  - 7 PDPC's enforcement decisions to-date involve data intermediaries
  - Most involved web hosting and/or website design and maintenance services
  - Data intermediaries breached the PDPA in 6 cases to-date

# Personal data protection regime

How can organisations discharge their Protection Obligation?

- *Central Depository (Pte) Limited and Toh-Shi Printing Singapore Pte Ltd*:
  - The PDPC found that CDP had complied with the Protection Obligation, by **putting in place an agreement obliging Toh-Shi** to take the necessary actions and precautionary measures to protect the CDP account holders' personal data during the printing process.
  - The PDPC also noted that CDP had in place **processes** for the secure transfer of personal data between CDP and Toh-Shi.
- *AVIVA Ltd and Toh-Shi Printing Singapore Pte Ltd*:
  - The PDPC found that Aviva had discharged its Protection Obligation, by **stipulating in the agreement with Toh-Shi** that Toh-Shi had to put in place adequate measures to safeguard the confidentiality of the Aviva policyholders.
  - In addition, the PDPC was satisfied that Aviva had undertaken an **appropriate level of due diligence** to assure itself that Toh-Shi was **capable of complying** with the PDPA.

# Personal data protection regime

- The contract should clearly specify the parties' obligations and responsibilities
  - "*It is important to note that if [the vendor] uses or discloses personal data in a manner which goes beyond the processing required by [the customer] under the contract, then [the vendor] will not be considered a data intermediary in respect of such use or disclosure.*" (Advisory Guidelines on Key Concepts in the PDPA)

- NB: A **data intermediary remains responsible for complying with all Data Protection Obligations** in respect of its **other data processing activities** which are not performed on behalf of and for the purposes of another organisation.

# Personal data protection regime

Relevant guidance issued by the PDPC:

•Advisory Guidelines on Key Concepts in the PDPA

•Guide to Securing Personal Data in Electronic Medium – in particular, chapter 15 (Websites and Web Applications), and new chapters 16 (Patching), 17 (ICT Outsourcing), and 18 (Cloud Computing)

•Guide to Disposal of Personal Data on Physical Medium

•Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data

•Guide on Building Websites for SMEs

# Sector-specific laws and regulations

ICT framework:

•Cloud Outage Incident Response Guidelines

Financial regulatory framework:

•Technology Risk Management Guidelines

•Guidelines on Outsourcing

•Business Continuity Management Guidelines

•Notice to Banks on Banking Secrecy – Conditions for Outsourcing

•Proposed Notice on Outsourcing

Healthcare/medical confidentiality framework:

•Sections 13 and 16 of the Private Hospitals and Medical Clinics Act, Regulation 12 of the Private Hospitals and Medical Clinics Regulations

•MOH's National Guidelines for Retention Periods of Medical Records

# Laws of other jurisdictions

- Data protection and privacy laws and regulations of other jurisdictions may apply, where there is a foreign link
- For example, the EU General Data Protection Regulation (which is expected to come into effect in 2018) applies to:
  - "*the processing of personal data **in the context of the activities of an establishment of a controller or a processor in the Union**, regardless of whether the processing takes place in the Union or not*"
  - "*the processing of personal data of **subjects who are in the Union by a controller or processor not established in the Union**, where the processing activities are related to: (a) **the offering of goods or services**, irrespective of whether a payment of the data subject is required, **to such data subjects in the Union**; or (b) the **monitoring of their behaviour as far as their behaviour takes place within the Union***"

02

# The cloud vendor and customer relationship

# 3 key stages

a) Due diligence
b) Contract drafting and negotiation
c) Ongoing audit, review and enforcement

DREW & NAPIER

# Strategies for contract drafting and negotiation

# Common clauses in cloud agreements

1. **Scope of the agreement**
2. **Performance, operational, internal control and risk management standards**
3. **Confidentiality and security**
4. **Business continuity management**
5. **Monitoring and control; audit and inspection**
6. **Reporting of adverse events**
7. Dispute resolution
8. Default termination and early exit
9. **Service Level Agreements and Remedies**
10. **Sub-contracting**
11. **Indemnities**
12. Limitation of liability
13. Variation
14. Applicable laws

# Common clauses in cloud agreements

Scope of the agreement

•Clearly define the customer and the vendor's obligations and responsibilities

–Generally

–In respect of data security

• C.f. Breach of Protection Obligation by Smiling Orchid: the PDPC found that:

–No clear designation of security responsibilities by Smiling Orchid and its vendor (who was engaged to design Smiling Orchid's website and build a Content Management System ("**CMS**") to manage website content)

–Smiling Orchid had merely relied on the vendor to be "in charge of the site" without properly engaging the vendor to provide security oversight for the site:

- matters relating to the security of the site were not included under the vendor's contractual scope of work;
- Smiling Orchid conceded that issues of security did not cross their mind; aspects of website security were not discussed with the vendor.

# Common clauses in cloud agreements

Performance, operational, internal control and risk management standards

- Set minimum data security standards, with reference to applicable laws and regulations, industry standards, and/or the customer's data security policies and industry standards
- Set data security performance measures (e.g., in an overall Service Level Agreement ("**SLA**"))

# Common clauses in cloud agreements

Confidentiality and security

- Identify and specify requirements for confidentiality and security
- Specify who may have access to the customer's IT systems / to whom the customer's information may be disclosed (e.g., on a "need-to-know basis)
  - State responsibilities of parties in ensuring the adequacy and effectiveness of security policies
  - Specify circumstances under which each party has the right to amend security requirements
  - Liability for losses in the event of a breach of security or confidentiality
- Ensure that vendor is able to protect confidentiality of customer data, especially in multi-tenancy arrangements (e.g., data centres)

**3.3 Data Secrecy.**

For processing Personal Data, SAP and its Subprocessors shall only use personnel who are subject to a binding obligation to observe data secrecy or secrecy of telecommunications, to the extent applicable, pursuant to the Data Protection Law. SAP shall itself and shall require that its Subprocessors regularly train individuals to whom they grant access to Personal Data in data security and data privacy.

**3.4 Technical and Organizational Measures.**

(a) SAP shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in Appendix 2 of the Schedule.

(b) Appendix 2 applies to the production system of the Cloud Service to keep Personal Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage. Non-production environments (e.g. a test instance of the Cloud Service) provide for a lower level of security and SAP recommends that Customer does not store any Personal Data in such non-production environments.

(c) Since SAP provides the Cloud Service to all customers uniformly via a hosted, web-based application, all appropriate and then current technical and organizational measures apply to SAP's entire customer base hosted out of the same data center and subscribed to the same Cloud Service. Customer understands and agrees that the technical and organizational measures are subject to technical progress, development and improvements for the protection of Personal Data shall automatically apply.

**3.5 Verification.**

SAP shall regularly test the measures described in Appendix 2. If a Data Controller believes that additional measures are required under the applicable Data Protection Law Customer shall submit an instruction according to Section 3.1 above.

Source: Data Processing Agreement for SAP Cloud Services enGLOBAL.v.4-2016, accessible at: http://sapassets.edgesuite.net/agreements/product-use-and-support-terms/cls/en/data-processing-agreement-for-sap-cloud-services-english-v4-2016.pdf

# Common clauses in cloud agreements

Business continuity management

- The agreement should contain business continuity plan ("**BCP**") requirements on the vendor, e.g., recovery time objectives ("**RTO**"), recovery point objectives ("**RPO**"), and resumption operating capacities
- Consider providing for regular testing of the BCP to ensure that the RTO, RPO and resumption operating capacities are feasible.
- Reporting requirements: any test finding that may affect the vendor's performance; (substantial) changes to the vendor's BCP; adverse developments

# Common clauses in cloud agreements

Monitoring and control; audit and inspection

- The agreement may provide for mechanisms by which the customer is able to monitor the vendor, to ensure that the specified performance, operational, internal control and risk management standards are upheld
  - Consider using a combination of monitoring/review methods (review meetings; regular self-assessment surveys; etc.)
  - The customer may also put in place internal policies and procedures to ensure that the outsourced services are monitored and controlled by the relevant staff on an ongoing basis
- The agreement may include clauses that allow the customer to conduct audits on the vendor (and its sub-contractors), and to obtain copies of any resulting reports/findings – see next section on *Ongoing audit, review and enforcement*
  - Remedial obligations and/or penalties if the findings of audit disclose that the vendor is not compliant with its data security obligations

# Common clauses in cloud agreements

Reporting of adverse events

- The agreement should specify the types of events and the circumstances under which the vendor should report to the customer
  - To allow the customer to take prompt risk mitigation measures, and notify any relevant authorities (e.g., PDPC, MAS, etc.) if necessary
- Specify timeframes for reporting specific types of events
- Consider expressly providing for the vendor's responsibilities during such adverse events, e.g.,
  - Cooperation with the customer during investigations
  - Notification/approval requirements before any information in respect of adverse events are disclosed to third parties
  - Remedial actions

**3.6 Security Breach Notification.**

SAP shall promptly inform Customer as soon as it becomes aware of serious disruptions of the processing operations, or any Security Breach in connection with the processing of Personal Data which, in each case, may significantly harm the interest of the Data Subjects concerned.

Source: Data Processing Agreement for SAP Cloud Services enGLOBAL.v.4-2016, accessible at: http://sapassets.edgesuite.net/agreements/product-use-and-support-terms/cls/en/data-processing-agreement-for-sap-cloud-services-english-v4-2016.pdf

# Common clauses in cloud agreements

Service Level Agreements and Remedies

•Consider including data security performance expectations in the overall SLA

- Sets out the customer's expectations in respect of data security, and draws the vendor's attention to the same
- Allows incentives to be assigned, and penalties to be imposed, in respect of data security performance

Sub-contracting

•Ensure that the customer has the ability to monitor and control arrangements when the vendor uses a sub-contractor

•Consider setting out restrictions on sub-contracting arrangements, e.g.,

- Approval/notification requirements in engaging/changing sub-contractors
- Obligations of vendor/sub-contractor in sub-contracting arrangements
- Right to audit/inspect sub-contractor's operations
- Liability for any breaches of data security practices by the sub-contractor

# Common clauses in cloud agreements

Indemnities

•Vendor may indemnify the customer against any losses in the event that the vendor (and/or its sub-contractors) breach their data security obligations

– Ensure enforceability of indemnity clause

–Check for application of any limits to the indemnity

–If using vendor's standard terms, there may be clauses which limit the vendor's data security commitments, or which push liability back to the customer

# Sample Clauses – The PDPC's Guide On Data Protection Clauses For Agreements Relating To The Processing Of Personal Data

| Sample Data Protection Clause | D&N comments |
|---|---|
| **2 HANDLING AND PROTECTION OF PERSONAL DATA**<br><br>2.1 Compliance with PDPA. The Contractor shall comply with all its obligations under the PDPA at its own cost. | • Could be extended to require vendor to comply with all applicable laws, regulations and industry standards<br>• A minimum standard of care can also be defined with regard to the customer's data security policies and any other specific safeguards |
| 2.2 Process, Use and Disclosure. The Contractor shall only process, use or disclose Customer Personal Data:<br>(a)strictly for the purposes of [fulfilling its obligations and providing the services required] under this Agreement;<br>(b)with the Customer's prior written consent; or<br>(c)when required by law or an order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs. | • Consider whether vendor also *collects* Customer Personal Data<br>• Consider whether vendor will have access to customer's IT systems<br>• Consider specifying purposes in greater detail<br>• Consider setting out restrictions on sub-contracting arrangements |

| Sample Data Protection Clause | D&N comments |
| --- | --- |
| 2.3 Transfer of personal data outside Singapore. The Contractor shall not transfer Customer Personal Data to a place outside Singapore without the Customer's prior written consent. [If the Customer provides consent, the Contractor shall provide a written undertaking to the Customer that the Customer Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the Contractor transfers Customer Personal Data to any third party overseas, the Contractor shall procure the same written undertaking from such third party]. | • Consider whether there are additional risks associated with the transfer of data to the particular country/countries<br>• Consider applicability of foreign laws, regulations and/or industry standards to any data transferred overseas<br>• Consider the legality and enforceability of the agreement in the relevant overseas jurisdiction<br>• Consider specifying data security obligations in greater detail |

| Sample Data Protection Clause | D&N comments |
| --- | --- |
| 2.4 Security Measures.<br>2.4.1 The Contractor shall protect Customer Personal Data in the Contractor's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Customer Personal Data, or other similar risks. For the purposes of this Agreement, "reasonable security arrangements" include arrangements set out [below / in the attached Schedule A1] (which shall not be varied without the Customer's prior written consent): [State the specific security measures that you want the Contractor to adopt or insert a separate Schedule listing the required security measures.]<br><br>2.4.2 The Contractor shall only permit the authorised personnel set out in [Schedule A2] to access Customer Personal Data on a need to know basis. | • Consider having broader security measures to protect other important data<br>• Consider requiring the vendor to notify the customer in the event of any changes in the vendor's data security policies<br>• Security measures should be reviewed regularly in light of new data protection best practices – provide for list of security measures to be updated from time to time |

| Sample Data Protection Clause | D&N comments |
| --- | --- |
| 2.5 Access to Personal Data. The Contractor shall provide the Customer with access to the Customer Personal Data that the Contractor has in its possession or control, as soon as practicable upon Customer's written request | Consider whether vendor will receive access requests (e.g., if vendor collects personal data on behalf of the customer as well). If so, vendor may be required to notify the customer of any such requests. |
| 2.6 Accuracy and Correction of Personal Data. Where the Customer provides Customer Personal Data to the Contractor, the Customer shall make reasonable effort to ensure that the Customer Personal Data is accurate and complete before providing the same to the Contractor. The Contractor shall put in place adequate measures to ensure that the Customer Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Contractor shall take steps to correct any errors in the Customer Personal Data, as soon as practicable upon the Customer's written request. | • Consider whether vendor will receive correction requests (e.g., if vendor collects personal data on behalf of the customer as well). If so, vendor may be required to notify the customer of any such requests.<br>• Vendor may also be required to ask any sub-contractors to correct such data |

| Sample Data Protection Clause | D&N comments |
| --- | --- |
| 2.7 Retention of Personal Data.<br>2.7.1 The Contractor shall not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this Agreement.<br><br>2.7.2 The Contractor shall, upon the request of the Customer:<br>(a)return to the Customer, all Customer Personal Data; or<br>(b)delete all Customer Personal Data in its possession,<br>and, after returning or deleting all Customer Personal Data, provide the Customer with written confirmation that it no longer possesses any Customer Personal Data. Where applicable, the Contractor shall also instruct all third parties to whom it has disclosed Customer Personal Data for the purposes of this Agreement to return to the Contractor or delete, such Customer Personal Data. | • May provide customer with right to inspect the vendor's property (e.g., hard disks) to ensure that all customer data is deleted / destroyed<br>• Vendor may be required to take reasonable efforts to ensure that the data is disposed of or deleted in a permanent and complete manner (since data which has been deleted/disposed of may nonetheless be retrievable)<br>• In certain cases, the agreement may allow for the vendor to cease to retain personal data by anonymising the same. |

| Sample Data Protection Clause | D&N comments |
|---|---|
| 2.8 Notification of Breach. The Contractor shall immediately notify the Customer when the Contractor becomes aware of a breach of any of its obligations in Clauses [2.2 to 2.7]. | • Procedures in respect of reporting data security incidents should be set out in greater detail<br>• Vendor's responsibilities to cooperate with the customer in the event of data security incidents, and/or to undertake remedial actions, may be provided |
| 2.9 Indemnity. The Contractor shall indemnify the Customer and its officers, employees and agents, against all actions, claims, demands, losses, damages, statutory penalties, expenses and cost (including legal costs on an indemnity basis), in respect of:<br>(a)the Contractor's breach of Clauses [2.2 to 2.7]; or<br>(b)any act, omission or negligence of the Contractor or its subcontractor that causes or results in the Customer being in breach of the PDPA. | • Consider the enforceability of such indemnity clauses.<br>• Check if any limits apply to such indemnity (e.g., in the main agreement)<br>• Consider whether to provide for a breach of data security obligations to be a material breach of the agreement (which may provide the customer a right to terminate the agreement immediately) |

# Common issues in negotiations

These are our standard terms and conditions. We can't change them.

Our product needs to be scalable in order for us to offer it at this price

We can't change our standard terms and conditions without permission from XXX

You need to sign by XXX date in order to get this year's special price

XXX is not available for our meeting

We need to sign by YYY date in order for us to start work to meet implementation timelines

We write these things into our contract, but trust us. For our reputation, we won't exercise these rights.

# Contract drafting and negotiation tips

- Parties typically seek to use their own standard contracts, which would include their standard data security clauses
  - Cross-check agreement against your own company's standard data security provisions to see if and where the clauses fall short of the requirements of your company, the specific risks at hand, and applicable laws, regulations and industry standards
  - Check for clauses which limit the other party's data security commitments, or which push liability back to your company
- Develop standard data security clauses/addendums for dealing with customer/vendor arrangements beforehand, taking into consideration the company's policies and practices, and applicable laws, regulations and industry standards
  - Streamlines contract drafting process
  - Allows company to drill down on its baseline requirements before entering into negotiations with prospective customers/vendors on their standard terms

# Contract drafting and negotiation tips

- Depending on the relative bargaining power between parties, the prospective vendor may be willing to vary its standard contract
  - Use addendum, side letter, change order
  - Ensure that the relevant terms in the addendum supersedes the corresponding terms in the main agreement
- A request for proposal ("**RFP**") or other formal vendor selection process can allow the customer to:
  - Dictate standard data security terms
  - Require specific vendor responses, which may require the prospective vendor to provide written explanations or commitments if it rejects any standard term
  - Compare a range of prospective vendors based on their responses and/or willingness to accept the standard terms
  - Reduce time spent on subsequent negotiations
- Negotiate data security terms together with commercial terms

# 03 Conclusion

# Conclusion

Contractual safeguards are essential.

In practice, it would also be important to maintain a good relationship with the customer/vendor's Chief Information Officers, Data Protection Officers, or other relevant personnel, to encourage sharing of information and to adopt a collaborative attitude in ensuring that data is safeguarded.

**You can outsource responsibility, but not accountability!**

# Questions?