asia cloud computing association

# The Impact of Data Sovereignty on Cloud Computing in Asia


# *The Impact of Data Sovereignty on Cloud Computing in Asia*

# Table of Contents

# *Foreword*

***"The Impact of Data Sovereignty on Cloud Computing" was created by the Asia Cloud Computing Association (ACCA) to offer detailed information describing the implications of data sovereignty law and policy on the adoption of cloud computing-based infrastructures and services in Asia. By describing and analyzing data sovereignty regulations in 14 countries in this study, the Association identifies potential bottlenecks that could slow adoption and threaten Asia's digital future.***

***The study serves to identify the gaps between an "ideal state" and the actual realities in Asian countries around policy, legal and commercial cloud drivers to provide a tool for businesses organizations, cloud service providers and policy makers to look at cloud in a more holistic manner.***

***This report provides substantive detailed analysis for each of the 14 countries, including 4-5 page detailed insights into the regulatory environment for data sovereignty in each country and recommendations for each country to bring attention to the highest priority issues that if addressed will bring the country closer to the "ideal state."***

## Why Cloud Computing?

Technology, in general, has always been a great leveler of opportunity for business, communities, and citizens. Just think about how access to the PC and the Internet has helped bridge the divide for millions across Asia in terms of access to information and the opportunities to tap into new economic opportunities.

Cloud technologies offer the opportunity to lower technology costs and to create time to market advantages. Additionally, cloud technologies promise to securely democratize data access – and in doing so, create a myriad of value-add possibilities across Asia.

The potential socio-economic impact in different parts of the world is still unclear. There are no exhaustive studies for Asia at this point in time but the benefits of cloud computing are potentially huge – it could possibly become one of the biggest drivers of economic growth over the next decade.

IDC predicts that cloud computing will create 14 million new jobs globally between 2011-2015, of which 10 million will be in Asia. This mirrors the forecasted growth in cloud revenue in Asia. Forester[1] estimates the public cloud market in Asia Pacific will grow from $2.3 billion in 2010 to $21.8 billion in 2020.

## Why Asia?

To realize the potential in Asia, the region needs to harmonize policy and regulatory frameworks to promote effective trade in digital information and services. It is therefore necessary to have an active debate with an Asia focus. This study was developed by the ACCA to inform this discussion.

While cloud is truly the globalization of information technologies, historically, much of the debate and discussion regarding the intersection of public policy and information technology has taken place in Europe and the United States (US). However, we see new conditions developing, wherein countries in Asia are moving as fast – and in some cases, faster than Europe and the US – to consider public policy issues dealing with cloud computing. We believe Asia's cloud computing market is poised to grow faster on both sides of cloud services: i.e., both cloud consumers and cloud providers. In order to contribute to further growth in Asia, it is crucial for public policy makers to look beyond the opportunities for cloud in their individual economies.

[1] Forrester Research, "Sizing The Cloud Markets In Asia Pacific", February 2012

The knowledge economy will fuel Asia's future and we think that cloud computing is the next great "leveler" for the region, poised to help accelerate the momentum around trade and economic integration in the region.

# About The Asia Cloud Computing Association

The Asia Cloud Computing Association (ACCA), launched in November 2010, is a forum for hardware and software developers, carriers, enterprise users, policy makers, and researchers. We aim to drive the adoption of cloud computing by addressing regional issues of regulation and policy, security infrastructure and awareness.

As the only forum focused on cloud computing issues in Asia, the Association is a place for collaboration and innovation for all stakeholders with an interest in Asia's cloud market.

The ACCA's primary mission is to accelerate the growth of the cloud market in Asia. This is done through working groups where best practice recommendations and other thought leading outputs are produced. The working groups draw on subject matter expertise and experience from the member companies. Current working groups include: Public Policy and Regulatory Working Group, Data Sovereignty Working Group, SME Working Group and Cloud Assessment Working Group.

For more information, visit www.asiacloudcomputing.org. For membership, contact info@asiacloudcomputing.org.
For more information about the Data Sovereignty Study, contact info@asiacloudcomputing.org.

# Acknowledgements

The Asia Cloud Computing Association would like to acknowledge members of the Data Sovereignty Working Group who assisted in the preparation of this report in their individual capacities. This report is the work of the Asia Cloud Computing Association and the views herein do not necessarily reflect the Working Group members or their companies. Participation in the Working Group is not an endorsement of any particular viewpoint expressed.

| Role | Name | Company |
|---|---|---|
| **Chairman** | Stacy Baird | |
| **Members** | Bernie Trudel | Cisco Asia Pacific |
| | Bill Padfield | Dimension Data Asia Pacific Pte Ltd |
| | Brad Banerd | Cisco Asia Pacific |
| | Colin Chan | Datapipe |
| | Jerry Wertelecky | Cloud Transformation & Security Solutions (CTSS) |
| | John Galligan | Microsoft |
| | Lim May-Ann | TRPC |
| | Lydia Johnston | Taylor Vinters |
| | Mark Ross | Asia Cloud Computing Association |
| | Michael Thatcher | Microsoft |
| | Omid Mahboubi | Asia Cloud Computing Association |
| | Paul Nichols | AT&T |
| | Per Dahlberg | Asia Cloud Computing Association |
| | Rey Coloma | Smart Communications |
| | Tim Pullan | Taylor Vinters |

# *Executive Summary*

## Introduction

The adoption of cloud computing by companies, governments, and individuals around the world continues to grow. Decision to use cloud computing is based on a variety of factors including the business drivers, security, commercial offerings, and impact of data sovereignty.

While many of the factors driving adoption are clearly understood by cloud users and providers, data sovereignty is an area that is increasingly discussed, but often misconstrued. Traditionally, data sovereignty is the respect for the rights associated with data – based on where the entity that has control of the data resides. However, with the globalization of data flows, the picture is less clear. A government's claim of legal jurisdiction over data may be based on the law of the country where the control over that data resides, based on jurisdiction over that same entity in another country where it does business, or by virtue of jurisdiction over a third party that may have access to or control of the data. Each country may have laws that impact the determination of which country has a claim of jurisdiction over data. We consider the sets of laws, regulation, guidelines and government policies as "data sovereignty regulations." This paper discusses the impact data sovereignty regulations have on the adoption of cloud computing.

Onerous data sovereignty regulations can stifle the adoption of cloud computing by mandating specific locations for data. These regulations may necessitate the need for organizations to leverage a local data center versus using the best solutions available – either in-house, outsourced, or cloud.

The regulatory landscape becomes even more clouded by the various jurisdictions involved. Imagine the scenario:

- Company based in Country A
- With operations in Country B
- Capturing data on citizens in Countries A, B, C, and D
- Leverages a Cloud Service Provider based in Country E
- Cloud Service Provider replicates data across facilities in Countries B, E, F, and G

This introduces complexities based on the trans border data flows involved. However, with a good understanding of the applicable regulations and restrictions, cloud computing can still be adopted.

To determine the impact of data sovereignty regulations, 14 countries were examined and scored from the perspective of an "ideal country." This is an environment where unambiguous regulations enable cross-border transfers in a way that protects the information in-line with global norms.

The following sections highlight the dominant data sovereignty factors that may impact adoption of cloud services in the respective countries. Besides introducing readers to challenges involved in the legal and regulatory environment of these countries, recommendations are also provided to help tackle these challenges. With the insights provided, this paper will assist readers in relation to their business decisions, services and activities when adopting or providing cloud computing services.

## Scope

This report begins with a background of cloud computing services and its growth prospects in Asia. The countries covered are Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand and Vietnam. For each, there is an overview of the factors encouraging or inhibiting cloud adoption, impacts of changing regulatory environment for cloud computing services and some industry specific concerns for the finance and telecommunications sectors.

Based on the data collected on the regulatory landscape in each country, the scorecard illustrates how conducive the legal and regulatory environment is in each of the 14 countries for cloud computing services. For each country, the current legal and regulatory environment for each of the country are analysed against the same five categories that were used for scoring them in the previous section.

Lastly, the paper will be concluded with key challenges of the current legal and regulatory environment and some recommendations to tackle those challenges.

This report does not, in any ways, attempt to discredit or promote any of the subject countries in relation to cloud computing services. Instead, this paper serves to provide opinions and suggestions from a neutral standpoint to help readers in their business decisions.

# Defining the "ideal" state

Each element of the score could be considered a positive or negative depending on the reader's perspective. To provide a common framework and facilitate scoring, an ideal state for each criterion was defined as outlined below.

| Assessment Criteria | Ideal Criteria |
|---|---|
| **Cloud Access**: Regulations support the usage of cloud computing. | • There are no prohibitive regulations that restrict cloud computing.<br>• Various incentives (financial and non-financial) are available to encourage cloud adoption.<br>• Cloud users are able to select the providers that best meet their needs regardless of the provider's geographic location.<br>• There is no prohibition or differentiation of cloud computing from other IT or outsourcing services for compliance. |
| **Data Safety**: Data is safe from access and liability regulations. | • There is a transparent mechanism for obtaining access to data via warrant or similar process that is based on proper due diligence, reasonable frequency of request and ability for cloud provider to challenge the request.<br>• There is no censorship or liability for content. |
| **International Consistency:** Regulations are clear, well understood, reasonable to comply with, and aligned to global norms. | • Regulations are aligned to global norms.<br>• It is clear what is allowed and not allowed for cloud computing users and providers.<br>• There are clearly defined and strong data protection laws that provide a sufficient baseline of protection of data but at the same time are not prohibitive for usage of cloud services.<br>• There are no country specific technical requirements that would require changes to the standard product.<br>• Compliance needs are not onerous, clearly defined, not subject to frequent change and does not require modifications to standard offerings. |
| **Cross Border Movement**: Consumers can leverage cloud providers from other jurisdictions. | • There are no restrictions on where data can reside.<br>• Cross border transfer of data compliance between countries is straightforward or is simplified due to country being a member of regional / global frameworks.<br>• There is no discrimination between local and foreign providers. |
| **Regulatory Stability and Enforcement**: Legal environment is predictable, fair, and aligned with international regulations. | • It is easy to setup business with minimal requirements.<br>• There are no restrictions that would hinder cloud providers ability to contract services.<br>• The country is a member of fair trade agreements, are part of non-discriminatory procurement agreements, regional / member of global frameworks to simplify compliance.<br>• Legal enforcement is fair and consistently applied. Potential penalties are commensurate with violations. |

# Scorecard approach

The scorecard is based on a scoring model developed to measure the consistency of application of relevant laws and the clarity of laws relating to data sovereignty for cloud computing. The steps involved in the development of the scorecard were:

1. Determine data sovereignty factors affecting cloud computing
2. Compiling the relevant data points
3. Identification of key criteria
4. Defining the ideal state
5. Scoring the responses
6. Assigning a weightage to each factor

# Scorecard results

Based on the approach outlined above, the countries were scored as follows:

| Assessment Criteria | Cloud Access | Data Safety | International consistency | Cross Border Movement | Regulatory Stability and Enforcement | Total Score |
|---|---|---|---|---|---|---|
| **Japan** | 61% | 63% | 88% | 87% | 76% | **80%** |
| **New Zealand** | 69% | 61% | 88% | 80% | 82% | **79%** |
| **Singapore** | 77% | 58% | 87% | 73% | 88% | **78%** |
| **Australia** | 61% | 61% | 87% | 76% | 78% | **76%** |
| **Hong Kong** | 70% | 59% | 88% | 69% | 88% | **76%** |
| **South Korea** | 71% | 74% | 74% | 67% | 80% | **72%** |
| **Taiwan** | 70% | 46% | 72% | 71% | 66% | **68%** |
| **Malaysia**[2] | 67% | 57% | 67% | 73% | 63% | **67%** |
| **India** | 53% | 41% | 64% | 73% | 66% | **65%** |
| **Indonesia** | 49% | 56% | 61% | 65% | 67% | **62%** |
| **Thailand** | 50% | 39% | 60% | 71% | 62% | **62%** |
| **Philippines** | 57% | 30% | 59% | 71% | 51% | **59%** |
| **Vietnam** | 43% | 30% | 52% | 66% | 58% | **56%** |
| **China** | 47% | 34% | 44% | 49% | 59% | **48%** |
| **Weightage** | 0.1 | 0.1 | 0.2 | 0.4 | 0.2 | **1.00** |

*Note: percentages represent the score obtained for each criterion out of the maximum available. See the Appendix for the detailed factors for each criterion.*

Modelling the impact of the law shows slight modification in the scoring for several of its assessment criteria.

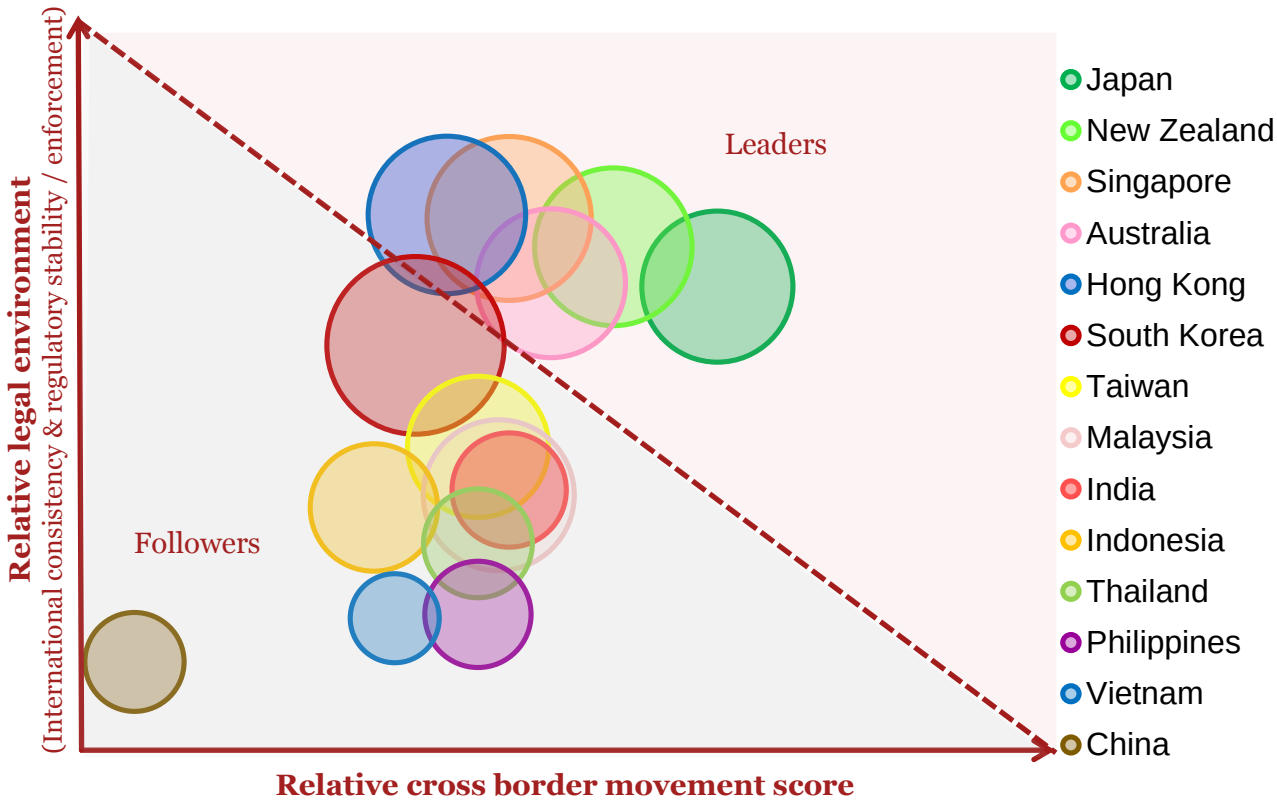
Cloud Access scoring would increase from 67% to 69%, International Consistency scoring would increase from 67% to 69%, and Regulatory Stability and Enforcement would increase from 63% to 64%. This positive change is primarily due to more certainty on the impact of the Act and the law being not prohibitive on cloud.

Cross Border Movement scoring, on the other hand, would decrease from 73% to 69%. This negative change for cross border movement is due to limitations in destination countries in the new legislation and the uncertainty around how that will be enforced.

[2] Malaysia's Personal Data Protection Act 2010 was published in the country's Gazette came into force on November 15, 2013. Since the Act was not in force, it was not included in the Malaysia's scores.

# Key scorecard observations

The scorecard highlights considerable differences between the 14 countries. Given the weightage of the criteria, these are primarily driven by the ability of organizations to move data across borders easily and having a stable legal environment in-line with global norms. As shown in the chart below, the countries can be grouped into two broad categories “leaders” and “followers”.




*Note: size of bubble indicates relative average of data safety and cloud access scores.*

Analysing the data shows some common differences between the leaders and followers. While these factors may not be uniform across all of the countries in the group, they provide context and perspective on how the relative rankings were developed.

| Factor | Leaders | Followers |
|---|---|---|
| **Data protection law** | Clear data protection law with reasonable requirements that correspond to globally accepted best-practices | No formal data protection law |
| **Protected data elements** | Personal Identifiable Information (PII) is defined and subject to regulations consistent with international or regional guidelines (such as APEC and OECD) | Inconsistent or not clearly defined |
| **Applicability of cloud computing regulations** | Clearly understood what laws affect cloud computing users and providers; in addition, laws are technology neutral and do not discriminate between technical options, except where justified | Unclear what applies (i.e., telecommunications laws) or laws that restrict cloud usage |
| **Law transparency** | Laws are introduced in a transparent manner with public input | Little consultation or advance notice provided |
| **Censorship** | No filtering or censoring requirements by Internet Service Provider or Cloud Service Providers | Mandatory filtering and / or censoring requirements |
| **Transfer of data outside of jurisdiction** | Can be accomplished with reasonable controls | Not clear or involves onerous requirements |
| **Effective agency (or regulator)** | Enforcement conducted in fair and impartial manner | Ad-hoc enforcement; varying enforcement between different agencies of the same government; regulators have high degree of discretion over enforcement decisions and regulatory interpretation, with little accountability or public scrutiny |
| **Product preference** | No country specific technical requirements that would require changes to the standard product | technical restrictions that may require country-specific changes to standard product |
| **Localization requirements** | No discrimination between local and foreign service provider | Foreign Cloud service providers may be subject to additional requirements and / or restrictions than local providers |

While the factors above indicate key differences between the groups, other factors examined had little impact on the resulting scores:

- Regulations on cloud computing relating to business function most countries did not have any prohibitions against the use of cloud computing services in relation to particular functions, but have some limits on data sets, such a medical and financial information on data subjects.

- Sector specific laws - most countries have regulations regarding the usage of cloud computing in specific industries. The financial services industry was the example cited most often.

- Penalties for non-compliance - almost all countries had commercially reasonable civil penalties for non-compliance; however, a few do have the potential for criminal charges.

- Material obligations on cloud computing service providers - cloud providers do not have onerous requirements such as data retention obligations, data security standards, duties to notify of security breaches and duties to disclose processed data to regulators or law enforcement officials.

- Government access – most of the countries do not provide unfettered access to cloud environments to foreign governments. On the other hand, mutual law enforcement treaties may provide access with valid justification.

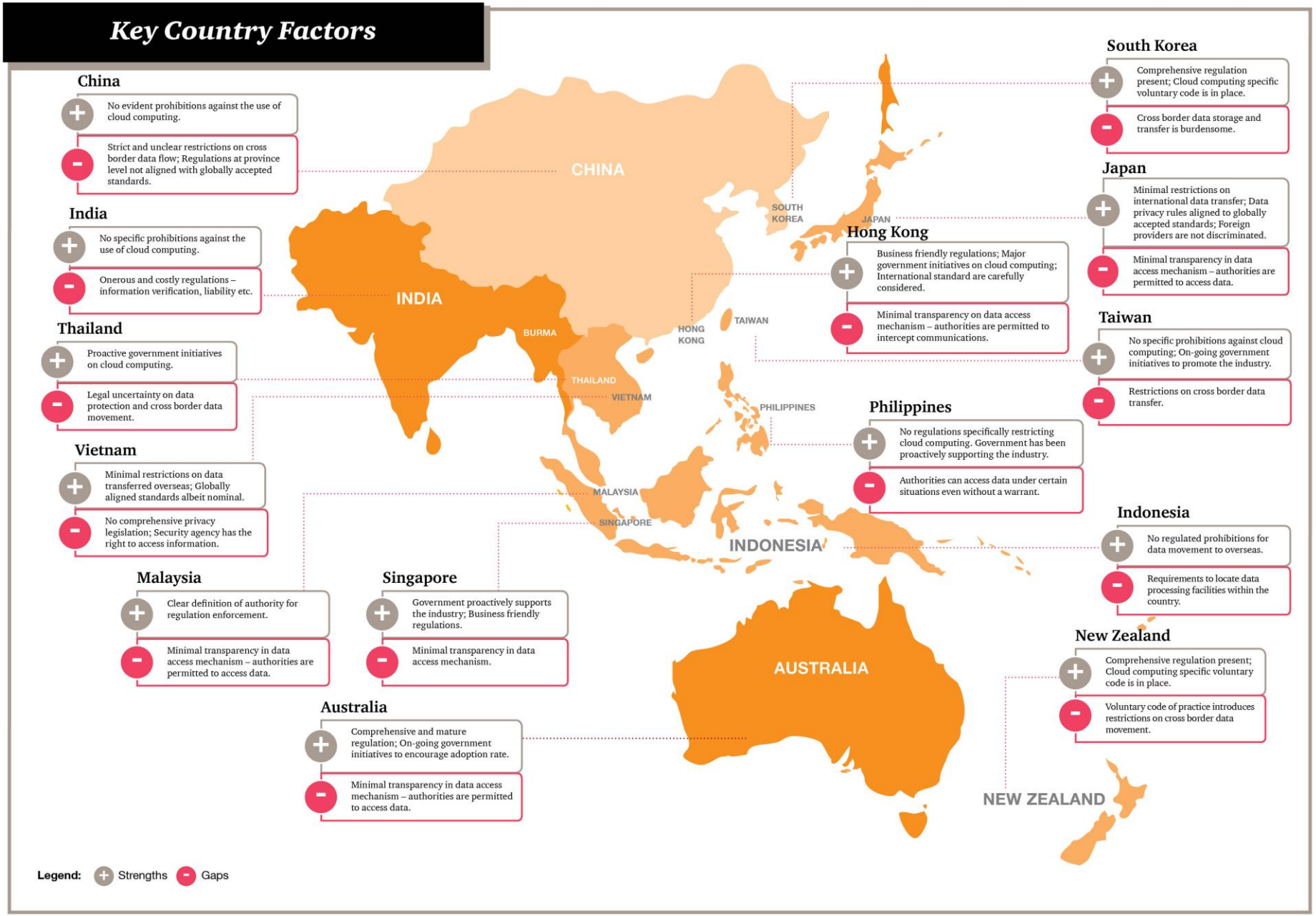
- Regional data protection framework – many of the countries covered are members of APEC or another regional framework for sharing data across boundaries. However, these rules have not necessarily been adopted yet by all countries in the study.

- WTO membership – all of the countries covered are members of the World Trade Organization. This can help ensure trade barriers are not unjustly enacted for cloud computing.

# Country analysis

On an individual country level, many data sovereignty factors helped or hindered the adoption of cloud computing (see map).

# Key Country Factors




## China

- (+) No evident prohibitions against the use of cloud computing.
- (-) Strict and unclear restrictions on cross border data flow; Regulations at province level not aligned with globally accepted standards.

## India

- (+) No specific prohibitions against the use of cloud computing.
- (-) Onerous and costly regulations – information verification, liability etc.

## Thailand

- (+) Proactive government initiatives on cloud computing.
- (-) Legal uncertainty on data protection and cross border data movement.

## Vietnam

- (+) Minimal restrictions on data transferred overseas; Globally aligned standards albeit nominal.
- (-) No comprehensive privacy legislation; Security agency has the right to access information.

## Malaysia

- (+) Clear definition of authority for regulation enforcement.
- (-) Minimal transparency in data access mechanism – authorities are permitted to access data.

## Singapore

- (+) Government proactively supports the industry; Business friendly regulations.
- (-) Minimal transparency in data access mechanism.

## Australia

- (+) Comprehensive and mature regulation; On-going government initiatives to encourage adoption rate.
- (-) Minimal transparency in data access mechanism – authorities are permitted to access data.

## South Korea

- (+) Comprehensive regulation present; Cloud computing specific voluntary code is in place.
- (-) Cross border data storage and transfer is burdensome.

## Japan

- (+) Minimal restrictions on international data transfer; Data privacy rules aligned to globally accepted standards; Foreign providers are not discriminated.
- (-) Minimal transparency in data access mechanism – authorities are permitted to access data.

## Hong Kong

- (+) Business friendly regulations; Major government initiatives on cloud computing; International standard are carefully considered.
- (-) Minimal transparency on data access mechanism – authorities are permitted to intercept communications.

## Taiwan

- (+) No specific prohibitions against cloud computing; On-going government initiatives to promote the industry.
- (-) Restrictions on cross border data transfer.

## Philippines

- (+) No regulations specifically restricting cloud computing. Government has been proactively supporting the industry.
- (-) Authorities can access data under certain situations even without a warrant.

## Indonesia

- (+) No regulated prohibitions for data movement to overseas.
- (-) Requirements to locate data processing facilities within the country.

## New Zealand

- (+) Comprehensive regulation present; Cloud computing specific voluntary code is in place.
- (-) Voluntary code of practice introduces restrictions on cross border data movement.

**Legend:** (+) Strengths (-) Gaps

# Key country considerations

While no country meets the ideal country definition, the following details highlights the dominant factors that should be considered for the adoption of cloud services in the respective countries:

| Country | Highlights | Areas for improvement |
|---|---|---|
| **Australia** | **Comprehensive and mature data protection legislation is in place:** OAIC is overseeing the Privacy Act, and the drafting for most laws on technology include public consultations. **On-going initiatives to encourage greater take-up of cloud services:** The Federal Government's National Cloud Computing strategy includes initiatives such as the development of a voluntary Cloud Consumer Protocol. | **Minimal transparency in the current data access mechanism:** Legislations currently permit access to data by individuals and the Privacy Commissioner, and authorities are permitted to intercept access or conduct surveillance on data. |
| **China** | **No evident prohibitions against the use of cloud computing:** Some form of regulation and guidelines covering personal data, contracts, and archives is present. | **Strict restrictions on cross border data flow regulated by provinces:** Ordinances in provinces such as Jiangsu and Shenzhen prohibit outward transfer of personal data without authorization. Other restrictions include censorship and government surveillance. |
| **Hong Kong** | **Business friendly regulations and major initiatives on cloud computing:** Several initiatives to be rolled out by the government to support their vision of becoming the data center hub of the world. International standards are carefully considered. | **Minimal transparency in the current data access mechanism:** Possible enhancement to the Interception of Communications and Surveillance Ordinance to better regulate the interception of communications by authorities. |
| **India** | **No specific prohibitions against the use of cloud computing:** Some form of regulation and guidelines covering personal data, contracts, and archives is present. | **Onerous and costly regulations:** Several requirements in the Information Technology Act, 200 are rather onerous and can be costly if legal proceedings are involved, for example, providers of sensitive information are currently required to verify the given information, and Cloud service providers can be held liable for the illegal data they may be hosting. |
| **Indonesia** | **No regulated prohibitions for data movement to overseas:** Regulation 82 does not include specific requirement that prohibits storage/transfer of general data outside of Indonesia. | **Requirements to locate data processing facilities within Indonesian territory:** Regulation 82 states that where cloud providers offer services to the public, the data center must be located within the country. |
| **Japan** | **Minimal restrictions on international data transfer:** While there are no specific rules that relate to the transfer of data in general, APPI states that consent must be obtained from individuals when their personal data will be transferred to a third party, whether within or outside Japan. **Censorship is prohibited and secrecy of communications is guaranteed** under the Japanese Constitution. | **Minimal transparency in the current data access mechanism:** Act on Wiretapping for Criminal Investigation (Act No. 137 of 1999) currently allows the investigative authorities to intercept communications with a warrant to the extent necessary to investigate serious organized crimes. |
| **Malaysia** | **Clear definition of authority for regulation enforcement:** The Personal Data Protection Commissioner can | **Minimal transparency in the current data access mechanism**: Currently authorities may search any premises without |

| Country | Highlights | Areas for improvement |
|---|---|---|
| | implement and enforce personal data protection laws, monitor and supervise compliance with the provisions of the PDPA. There are penalty clauses defined for PDPA violation. | a warrant for general computerised or encrypted data. A more transparent mechanism can be achieved via incorporating amendments on warrants and requirements for cloud service providers to challenge data access requests to the recently passed Personal Data Protection Act in 2013. |
| **New Zealand** | **Regulations are comprehensive including cloud computing specific voluntary code:** The Office of the Privacy Commissioner's Cloud Computing Guidance, which provides accessible guidance for NZ businesses about how they can move to the cloud. The NZ Cloud Code is a code of practice that has been developed by the Institute of IT Professionals (formerly the NZ Computer Society) which is a strictly voluntary code that is not mandated by Government. | **Voluntary code of practice introduces certain restrictions on the usage of cloud computing services:** Restrictions on export of data included and disclosure requirements in the voluntary cloud code of practise is not aligned with globally accepted standards. |
| **Philippines** | **No regulations specifically restricting the use of cloud computing:** The government has been pro-actively supporting the advancement of cloud computing practice. They see this as one of the keystone that will strengthen the country's position as a leader in IT-Business Process Outsourcing. | **Authorities can access data under certain situations** stated in the Cybercrime Prevention Act, even without a warrant. |
| **Singapore** | **Government proactively support the adoption and growth of cloud computing:** Regulations such as Personal Data Protection Act (PDPA) 2012 which is the baseline legislation on data privacy, and 160 disparate, sector specific statutes include requirements that are relevant to the cloud computing industry. In spite of seemingly numerous rules and regulations, the regulatory framework in Singapore has been perceived to be very business friendly. | **Minimal transparency in the current data access mechanism:** Singapore law can compel the disclosure of data including encrypted data to government bodies and law enforcement agencies. While a warrant is typically required for investigations; however, the Computer Misuse (Amendment) Act (CMA) provides for exemptions. |
| **South Korea** | **Cloud computing specific legislation**: The draft of "Bill for the Development of Cloud Computing and Protection of Users" is including details that impact cloud servicing and international trade. | **Cross border data storage and transfer is burdensome:** The Proposed Act prohibits the provision of information to 3rd parties, unless consent is obtained, and requires the service provider to disclose when information is stored overseas. |
| **Taiwan** | **No specific prohibitions against the use of cloud computing:** "Taiwan Cloud Valley", initiated and promoted by Cloud Computing Association in Taiwan (TWCLOUD), aims to cluster Taiwan's complete supply chain and functions as a window of Taiwan and international cloud computing suppliers. | **Restrictions on cross border data transfer:** According to the PDPA of Taiwan, cross-border transfer of personal data constitutes an "international transmission". The National Communications Commission, Taiwan's communications and media regulator, has imposed a directive on telecom and media operators to prohibit them from conducting international transmission of personal data to China. |
| **Thailand** | **Pro-active government initiatives on cloud computing:** An initiative to launch Thailand Government Cloud in May 2012 | **Legal uncertainty on data protection and cross border movement:** The Telecommunications Business Act ("TBA") |

| Country | Highlights | Areas for improvement |
|---|---|---|
| | by the Electronic government Agency (EGA) and another by Software Park, a government agency under the National Science and Technology Development Agency, to encourage local software companies to go on cloud and innovate local cloud platform. | states requirements that may result in onerous operations for the cloud service providers including minimum legal terms for contracts, and consent for personal data transfer. |
| **Vietnam** | **Minimal restrictions on data transferred overseas:** The Law of Information Technology and Law of Media state reasonable requirements on consent for transfer and types of prohibited data, which are aligned with globally accepted standards. As a whole, Vietnam has no comprehensive privacy legislation; however, it does have a short privacy section in its Law on E-Transactions 2005 that is relevant to cloud computing. | **Security Agency has the right to access all information** including encrypted data under certain circumstances under the Law on National Security. |

# Moving forward

The promise of cloud is yet to be fully realized in Asia as it continues to remain surrounded by concerns around data sovereignty, cross border data flow and data security. Regulators and authorities in Asia have rapidly responded to these concerns by introducing new laws, regulations and compliance requirements which attempt to mitigate the security and data privacy risks associated with the use of cloud computing platforms. However, it is unclear whether regulations are effectively addressing the key risks and may create inconsistencies from one country to another. The pace of regulation is also creating substantial uncertainty in the region.

Findings from our study suggest each country presents a mix of opportunity and challenges for cloud providers to supply their products in this region. As cloud computing evolves, so will the legal and regulatory environment managing it including:

- Individual country rules – while concepts like privacy and data protection have been present in Europe and other countries for many years, they are still relatively new in Asia. Over the last three years, many Asian countries have introduced their first industry agnostic data protection / privacy regulations. In some cases, these laws are not enforced yet and will mature over time. In addition, regulations are inconsistent from jurisdiction to jurisdiction, interfering with the deployment of cross-jurisdictional technology solutions (i.e., cloud).

- Regional regulations – regional frameworks like the APEC Cross Border Privacy Rules System and Trans-Pacific Partnership promise to introduce simplified measures for each exchanging data across boundaries. The full effects of these will not be known until fully implemented.

This is an area undergoing much change. Organizations can successfully adopt cloud computing now in most locations, but will need to monitor the regulatory landscape since recommendations and practical solutions may over time, be rendered obsolete or not be necessary anymore.

# *The Impact of Data Sovereignty on Cloud Computing in Asia*

# 1. Introduction

## 1.1. Cloud Adoption in Asia

The global market for cloud computing is forecasted to continue growing dramatically exceeding $75 billion USD in 2014[3]. The extent of cloud adoption however, is quite fragmented across Asia. Some countries such as Australia, Singapore, Taiwan, and South Korea have comparatively higher rate of cloud adoption (around 40-50%) whereas some countries such as China, India, Indonesia, Thailand, Vietnam and Philippines are still warming up to usage of cloud services on an enterprise level with adoption rates below 15%. The impetus for adoption of cloud is steadily growing amongst these emerging economies both in terms of government incentives as well as strategic directions taken by business leaders who want to realize the benefits that cloud computing offers for the organization. The decision to sign-up for cloud services is predicated on a number of factors including cost, availability, data security, benefits, availability of services, infrastructure, and various regulations. While cloud computing offers considerable promise in increasing scalability, agility and reducing IT costs for the enterprise, many organizations are still trying to understand the regulatory implications of adopting cloud services.

## 1.2. Key Barriers to Adoption

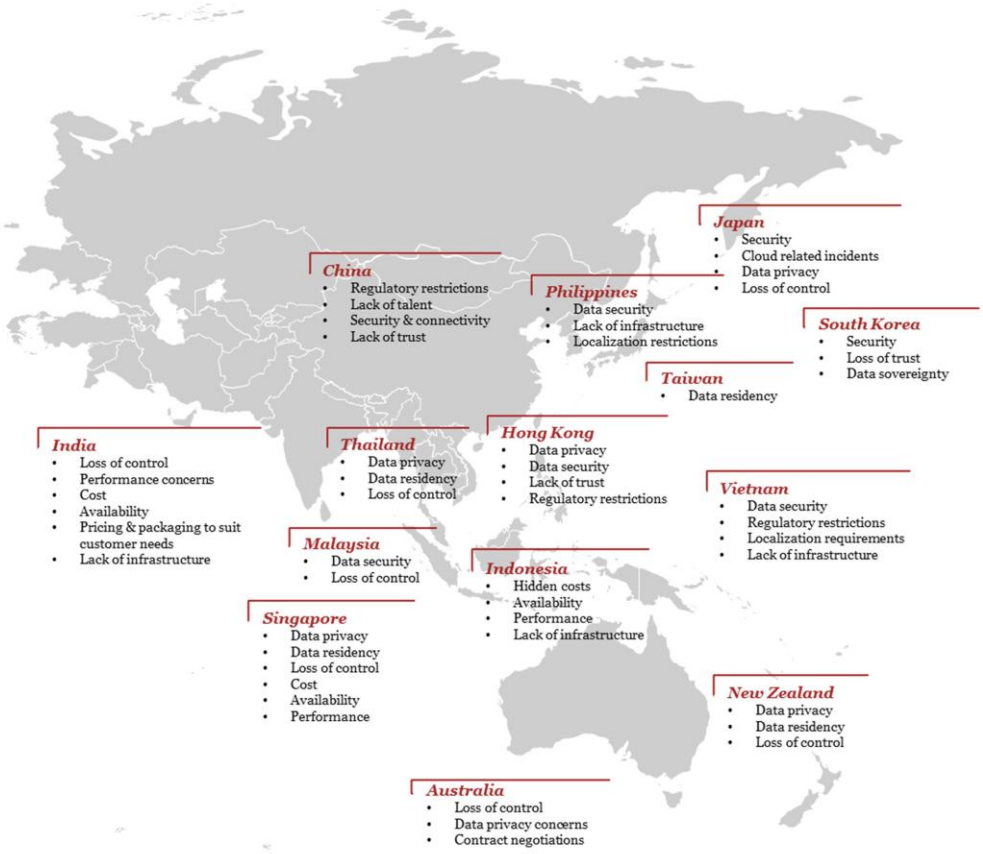
We reviewed the law with a team of lawyers for a factual understanding of the regulatory environment and conducted an informal survey including lawyers, technology professionals, and cloud customers in each country to identify key barriers to adoption. A summary of key concerns hindering organizations from using cloud adoption services across countries in Asia is illustrated in the next figure. Data privacy, data security, data residency and loss of control are some of the top concerns commonly observed across the various countries. Regulatory restrictions can be used by some governments as a protectionist measure to secure local businesses from foreign competition entering the domestic markets.

## 1.3. Impact of Changing Regulations

The regulatory landscape affecting cloud computing is in its early stages of development in Asia. Many countries are still in the process of formulating legislations that define permissibility of various cloud computing aspects such as cross border data transfer, taxation, data sovereignty, etc. This is an area witnessing a lot of changes with many new regulations either already introduced this year or expected to come into force in the next few years.

Much of the new law in this area has been adopted in the past one to two years. With governments across the region introducing relevant new laws in a relatively short period of time, the regulations have multiple impacts on the adoption of cloud computing. First, uncertainty around what will be allowed or prohibited by the regulations may encourage cloud users to delay usage. Second, regulations introduced without fully considering the impact may have unintended consequences that stifle innovation and adoption of cloud technologies and services. Finally, when regulations are introduced without consideration of the global nature of cloud computing there may little consistency between jurisdictions. As legal environments among the 14 countries significantly differ, there is a huge challenge for those adopting cloud services in satisfying requirements across the multiple jurisdictions.

[3] Forrester Research, "A Mixed Outlook For The Global Tech Market In 2013 And 2014", July 2013




**Organizations are still trying to understand the regulatory implications of adopting cloud services.**

## 1.4. Impact of Government Monitoring

Most jurisdictions require a warrant or other legal "due process" to access or intercept electronic records and data. However, during the first half of 2013 a number of practices were revealed globally showing the extent that governments may be accessing electronic data, without disclosure, for national security purposes. The possibility that various governments may monitor and store Internet traffic can affect IT procurement decisions, including the decisions regarding the use of cloud computing services, if the nature, intent, and scope is not understood.

## 1.5. Industry Specific Concerns

Besides navigating country specific regulations, cloud users and providers must address industry specific regulations. Many of the countries covered in this whitepaper have industry specific regulations that either directly / indirectly impact elements of cloud computing. For instance, Singapore has 160 disparate, sector specific statutes that regulate the use and disclosure of data management in Singapore including in relation to consumer protection laws, employment laws, ecommerce, telecommunication and sector specific laws in healthcare, banking and insurance. These sectoral regulations require modernization to now encompass cloud computing.

## 1.5.1. Financial services

Across Asia, the financial services industry tends to be one of the most highly regulated industries. Regulatory restrictions remain the topmost concern facing players in the financial services industry who are currently using / planning to use cloud services. These concerns specifically pertain to cross border data flow and ability to access data that is physically stored within one jurisdiction from outside. Another major challenge for companies in this industry is to maintain compliance with regulatory requirements across all operating locations of the organization. Since legal requirements may differ significantly from one country to another, companies often find it difficult to organize cloud services for the whole enterprise in a manner that complies with all laws under each of the relevant jurisdictions.

Companies also need to deal with the uncertainty on how regulations apply. For example, outsourcing guidelines may or may not be applicable to cloud computing. Conversely, for regulators, the laws aren't clear as to cloud, but there is a fear that cloud computing will make access and oversight more difficult. The bottom line is that many governments are resistant to approving the use of cloud services, even if regulations do not contain clear restrictions. However, there is greater acceptance of cloud as an option. For example, in November 2013 a senior official from the Monetary Authority of Singapore publicly declared there is no blanket ban on cloud in Singapore.

## 1.5.2. Healthcare

There are numerous studies showing the benefits of electronic health records and the use of cross-institution data systems in healthcare. The regulatory environment in many countries does not necessarily enable cloud adoption in healthcare. This mean patients and providers may be missing out on tools which can facilitate better medical outcomes by greater accuracy in health records and better, more efficient sharing of patient data.

## 1.5.3. Telecommunications

Worldwide information and communications technology (ICT) spending attributed to telecom services has been experiencing a steady decrease from 2010 to 2012. Telecom services spending will continue to trend downward and is projected to be less than half of overall ICT spending by 2016.[4] Profitability of telecom services providers was diluted over a broad and over customised portfolio. With insufficient attention in process manager and service delivery, ICT capabilities of telecom services providers were costly and complex, and customer service, often, unpredictable.

As consumers become more accustomed to the delivery of ICT through cloud delivery models, traditional delivery models for ICT may gradually be replaced by cloud models. Telecom services providers have previously faced situations where new technologies (e.g., mobile/cellular, VoIP, IP, etc.) replaced legacy models, some of which are actually cloud services. Providers have acknowledged the need to sacrifice legacy service models to better meet the needs of the changing marketplace. Emerging services may look at the current state and see opportunities to offer better, more innovative services at a lower cost. This means regulators have made decisions (and have to make additional decisions) on how to accommodate the changing technologies (e.g., universal access, 5-nines reliability, wiretap access and emergency services).

To transform from an old operating model and implement a new operating model is a daunting and difficult task for an industry with large-scale, historically static legacy infrastructure, upon which the regulatory environment is based. So service providers currently providing / planning to provide telecom related cloud services face legal and regulatory challenges. These challenges include the need to reconcile between regulations that may not apply well outside of traditional telecom. In addition, incumbents may encourage broader application of regulations to increase the burden and potential costs for compliance for new entrants. Scorecard

[4] John-David Lovelock "Forecast Alert: IT Spending, Worldwide, 4Q12 Update" (Gartner, Market Analysis and Statistics, January 2013), http://www.gartner.com/id=2291618

# 1.6. Scorecard overview

The scorecard is based on a model developed to measure the impact of data sovereignty on the adoption of cloud computing. The goal is to highlight how the underlying factors may affect adoption in various jurisdictions.

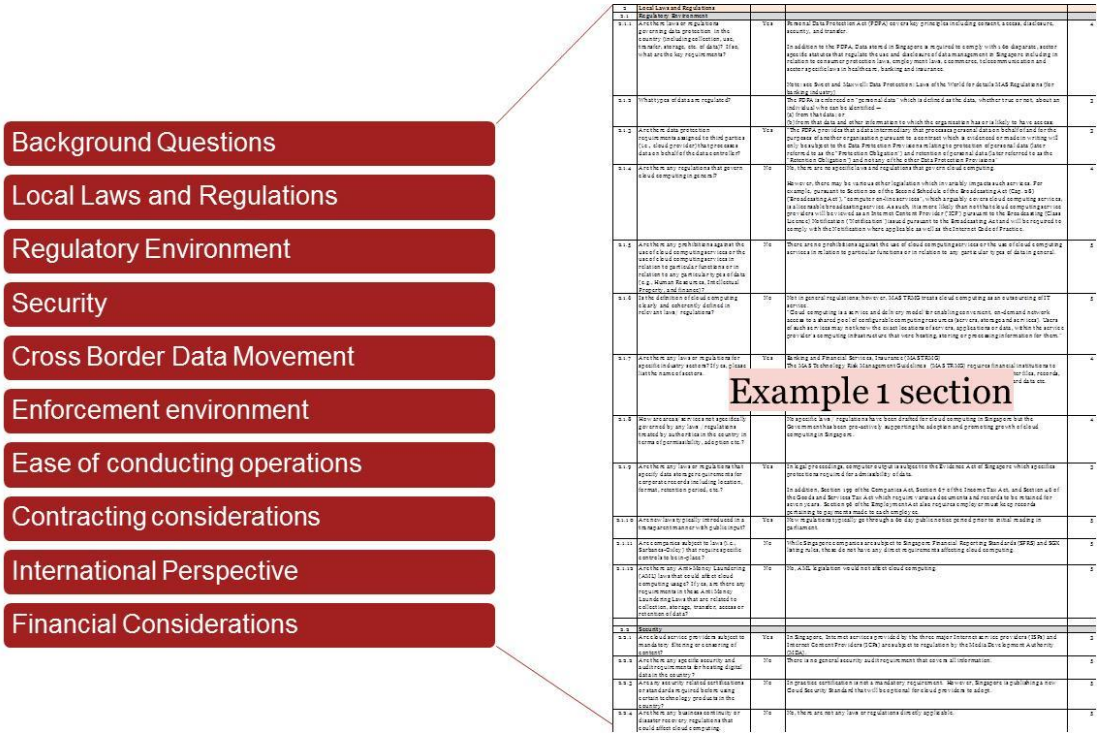
Weightage and score ranges are assigned to each measured criterion as they best-fit. While weightage is allocated according to criticality of the factor, score ranges are defined specific to the measured component. For example, the score range dictates 5 is the ideal scenario, 3 for an acceptable scenario, and 1 for unfavourable scenario. The overall scores represent the percentage of points received for a category compared to the total number possible.

# 1.7. Scorecard process

The scorecard was created by gathering the relevant information on the data sovereignty factors affecting cloud computing in each country and assigning a score for each factor. The details of the process are outlined below. Additional details can be found in Appendix 1.

## 1.7.1. Determine data sovereignty factors affecting cloud computing

The scorecard was developed by gathering information on the legal environment and actual practices in the 14 countries. The data encompassed 68 different topics across 10 categories of questions.



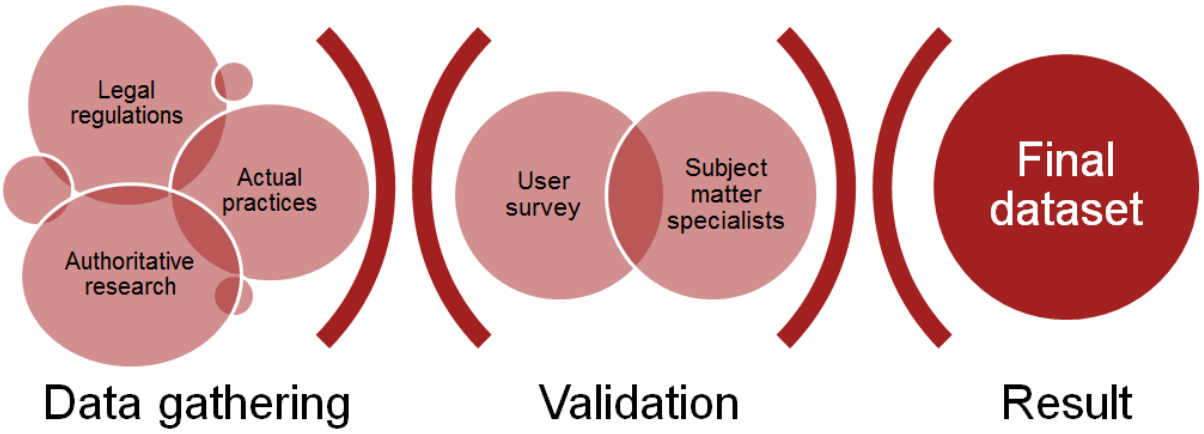

The process encompassed the following activities:

- Gather information on required regulations for 14 countries listed
- Identify relevant rules/ laws for each activity / area
- Analyse implications of rules / laws
- Identify inter country relationships that may exist in form of agreements/pacts and conflicts if any

- Identify issues that may arise for stakeholders in the cloud computing ecosystem due to specific laws or regulatory requirements

## 1.7.2. Compiling the dataset

The dataset gathered in 6.2.1, was compared to authoritative research to identify any anomalies. Once complete, the dataset was compared to results of a user survey and reviewed with specialists covering the cloud computing landscape across Asia. The validated dataset was used as the foundation for the scoring.




## 1.7.3. Identification of key criteria

To organize the results into logical areas, 5 key criteria were selected:

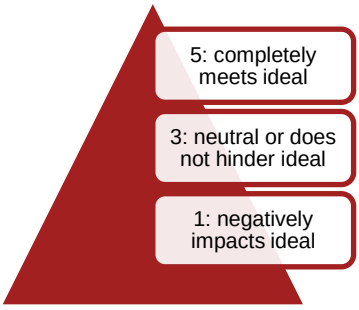
- **Cloud Access**: Regulations support the usage of cloud computing.
- **Data Safety**: Data is safe from access and liability regulations.
- **International Consistency**: Regulations are clear, well understood, reasonable to comply with, and aligned to global norms.
- **Cross Border Movement**: Consumers can leverage cloud providers from other jurisdictions.
- **Regulatory Stability and Enforcement**: Legal environment is predictable, fair, and aligned with international regulations.

## 1.7.4. Defining the ideal state

As outlined in section 6.3, the ideal state was defined for each criterion. This ideal state was designed to form the basis for each score.

## 1.7.5. Scoring the responses

The response for each question was evaluated against the ideal state to determine the extent it is aligned with the ideal. Scores were provided as shown below:



Note: in some cases, background data was gathered that was not included in the scoring.

### 1.7.6. Assigning a weightage to each factor

Each question may affect one of more of the criteria. Since the magnitude of the impact varies and some questions may not be impacted by a question, each question is assigned a weighting of 0 – 5 to reflect impact to each criteria. See Appendix 1 for details.

The 5 criteria vary in importance to the overall impact of data sovereignty on cloud computing. Consequently, in the final score for each country the criteria are weighted as outlined below:

| Assessment Criteria | Weightage |
|---|---|
| **Cloud Access**: Regulations support the usage of cloud computing. | 0.1 |
| **Data Safety**: Data is safe from access and liability regulations. | 0.1 |
| **International Consistency**: Regulations are clear, well understood, reasonable to comply with and aligned to global norms. | 0.2 |
| **Cross Border Movement**: Consumers can leverage cloud providers from other jurisdictions. | 0.4 |
| **Regulatory Stability and Enforcement**: Legal environment is predictable, fair, and aligned with international regulations. | 0.2 |

## 1.8. Ideal state

Each element of the score could be considered a positive or negative depending on the reader's perspective. To provide a common framework and facilitate scoring, an ideal state for each criterion was defined as outlined below.

| Assessment Criteria | Ideal Criteria |
|---|---|
| Cloud Access: Regulations support the usage of cloud computing. | • There are no prohibitive regulations that restrict cloud computing usage.<br>• Various incentives (financial / non-financial) are available to encourage cloud adoption.<br>• There are no restrictions on where data can reside and cross border transfer of data compliance across countries is simplified due to country being a member of regional / global frameworks.<br>• There is no prohibition or differentiation of cloud computing from other IT services for compliance. |
| Data Safety: Data is safe from access and liability regulations. | • There is a transparent mechanism for obtaining access to data via warrant or similar process that is based on proper due diligence, reasonable frequency of request and ability for cloud provider to challenge the request.<br>• There is no censorship or liability for content. |
| International consistency: Regulations are clear, well understood, reasonable to comply with, and aligned to global norms. | • Companies can quickly understand what they are required to do and what is not allowed.<br>• There are clearly defined and strong data protection laws that provide a sufficient baseline of protection of data but at the same time are not prohibitive for usage of cloud services.<br>• There are no country specific technical requirements that would require changes to the standard product.<br>• Compliance needs are not onerous, clearly defined, not subject to frequent change and does not require modifications to standard offerings. |

| | |
|---|---|
| Cross Border Movement: Consumers can leverage cloud providers from other jurisdictions. | • There are no restrictions on where data can reside and cross border transfer of data compliance across countries is simplified due to country being a member of regional / global frameworks.<br>• There is no discrimination between local and foreign providers.<br>• Customers are free to choose from both foreign and domestic providers that best meets their needs. |
| Regulatory Stability and Enforcement: Legal environment is predictable, fair, and aligned with international regulations. | • Laws are fairly, consistently enforced. It is easy to setup business with minimal requirements.<br>• There are no restrictions that would hinder cloud providers ability to contract services.<br>• The country is a member of fair trade agreements, are part of non-discriminatory procurement agreements, regional / member of global frameworks to simplify compliance.<br>• Legal enforcement is fair and consistently applied. Potential penalties are commensurate with violations. |

## 1.9. Scorecard results

Based on the approach outlined above, the countries were scored as follows:

| Assessment Criteria | Cloud Access | Data Safety | International consistency | Cross Border Movement | Regulatory Stability and Enforcement | Total Score |
|---|---|---|---|---|---|---|
| **Japan** | 61% | 63% | 88% | 87% | 76% | **80%** |
| **New Zealand** | 69% | 61% | 88% | 80% | 82% | **79%** |
| **Singapore** | 77% | 58% | 87% | 73% | 88% | **78%** |
| **Australia** | 61% | 61% | 87% | 76% | 78% | **76%** |
| **Hong Kong** | 70% | 59% | 88% | 69% | 88% | **76%** |
| **South Korea** | 71% | 74% | 74% | 67% | 80% | **72%** |
| **Taiwan** | 70% | 46% | 72% | 71% | 66% | **68%** |
| **Malaysia**[5] | 67% | 57% | 67% | 73% | 63% | **67%** |
| **India** | 53% | 41% | 64% | 73% | 66% | **65%** |
| **Indonesia** | 49% | 56% | 61% | 65% | 67% | **62%** |
| **Thailand** | 50% | 39% | 60% | 71% | 62% | **62%** |
| **Philippines** | 57% | 30% | 59% | 71% | 51% | **59%** |
| **Vietnam** | 43% | 30% | 52% | 66% | 58% | **56%** |
| **China** | 47% | 34% | 44% | 49% | 59% | **48%** |
| **Weightage** | 0.1 | 0.1 | 0.2 | 0.4 | 0.2 | **1.00** |

*Note: percentages represent the score obtained for each criterion out of the maximum available. See the Appendix for the detailed factors for each criterion.*

Modelling the impact of the law shows slight modification in the scoring for several of its assessment criteria.

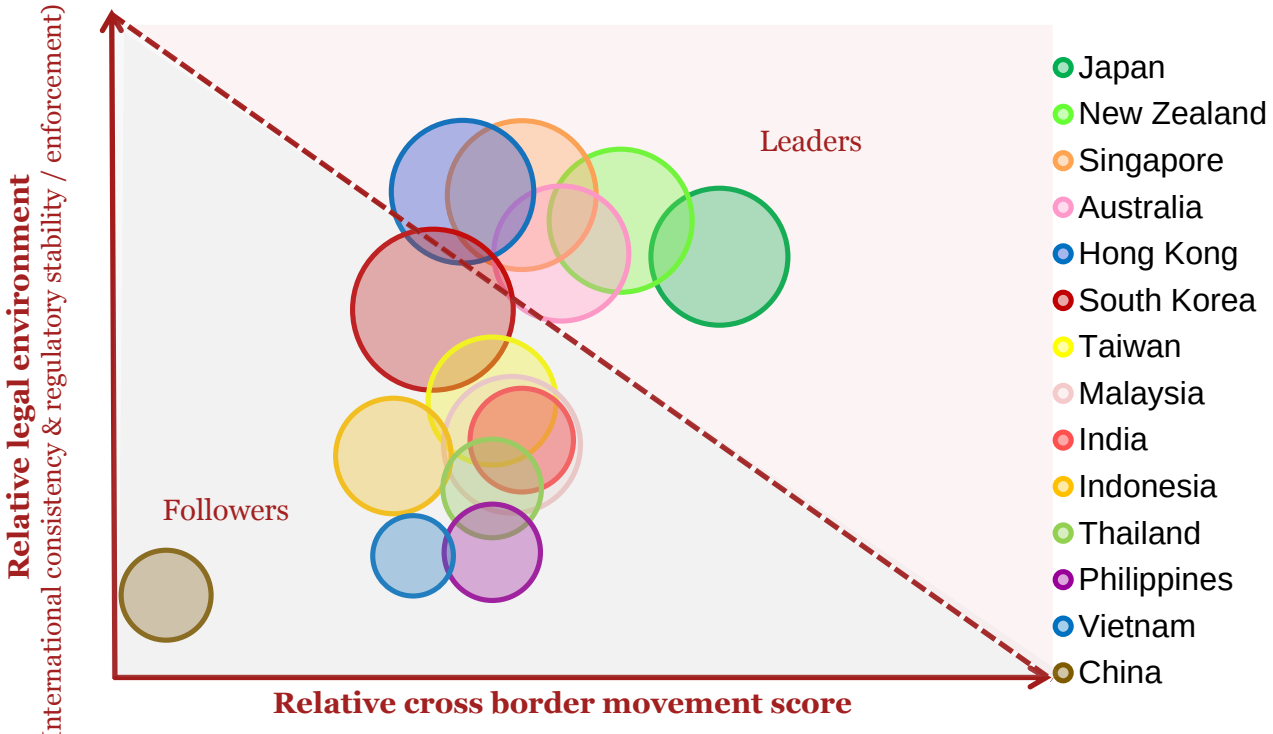
Cloud Access scoring would increase from 67% to 69%, International Consistency scoring would increase from 67% to 69%, and Regulatory Stability and Enforcement would increase from 63% to 64%. This positive change is primarily due to more certainty on the impact of the Act and the law being not prohibitive on cloud.

Cross Border Movement scoring, on the other hand, would decrease from 73% to 69%. This negative change for cross border movement is due to limitations in destination countries in the new legislation and the uncertainty around how that will be enforced.

## 1.10. Scorecard interpretation

The scorecard highlights considerable differences between the 14 countries. Given the weightage of the criteria, these are primarily driven by the ability of organizations to move data across borders easily and having a stable legal environment in-line with global norms. As shown in the chart below, the countries can be grouped into two broad categories “leaders” and “followers”.

[5] Malaysia’s Personal Data Protection Act 2010 was published in the country's Gazette came into force on November 15, 2013. Since the Act was not in force, it was not included in the Malaysia’s scores.




*Note: size of bubble indicates relative average of data safety and cloud access scores.*

Analysing the data shows some common differences between the leaders and followers. While these factors may not be uniform across all of the countries in the group, they provide context and perspective on how the relative rankings were developed.

| Factor | Leaders | Followers |
|---|---|---|
| **Data protection law** | Clear data protection law with reasonable requirements that correspond to globally accepted best-practices | No formal data protection law |
| **Protected data elements** | Personal Identifiable Information (PII) is defined and subject to regulations consistent with international or regional guidelines (such as APEC and OECD) | Inconsistent or not clearly defined |
| **Applicability of cloud computing regulations** | Clearly understood what laws affect cloud computing users and providers; in addition, laws are technology neutral and do not discriminate between technical options, except where justified | Unclear what applies (i.e., telecommunications laws) or laws that restrict cloud usage |
| **Law transparency** | Laws are introduced in a transparent manner with public input | Little consultation or advance notice provided |
| **Censorship** | No filtering or censoring requirements by Internet Service Provider or Cloud Service Providers | Mandatory filtering and / or censoring requirements |
| **Transfer of data outside of** | Can be accomplished with reasonable controls | Not clear or involves onerous requirements |

| Factor | Leaders | Followers |
|---|---|---|
| **jurisdiction** | | |
| **Effective agency (or regulator)** | Enforcement conducted in fair and impartial manner | Ad-hoc enforcement; varying enforcement between different agencies of the same government; regulators have high degree of discretion over enforcement decisions and regulatory interpretation, with little accountability or public scrutiny |
| **Product preference** | No country specific technical requirements that would require changes to the standard product | technical restrictions that may require country-specific changes to standard product |
| **Localization requirements** | No discrimination between local and foreign service provider | Foreign Cloud service providers may be subject to additional requirements and / or restrictions than local providers |

**Overall area for improvement: Data Safety**

From the scorecard results, it is observed that one of the key challenges in promoting cloud computing as an industry is the overall data safety. Specific pain points for most countries are: (1) data access and security, and (2) the lack of regulation on cross border data flow.

The findings gathered for fundamental data safety areas, particularly on regulatory matters, are among the areas that require further attention by the local regulators and international bodies alike. Regulations on areas such as warrants, data access by law enforcement authorities and overseas governments, data surveillance, extraterritorial effect, law enforcement in a foreign country, and customs monitoring are still fairly fresh, and mostly riding on the existing regulations that are industry specific. Countries such as Vietnam, Indonesia, India and Taiwan scored the lowest on data safety.

**Overall strength: Regulatory Stability and Enforcement**

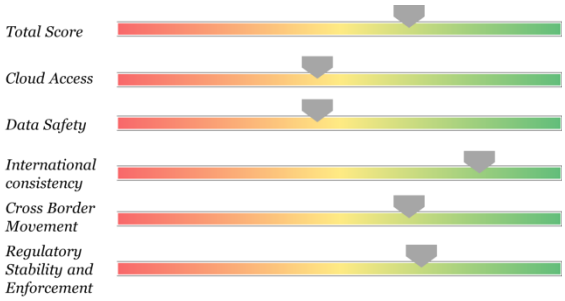
On a positive note, most countries are reasonably stable when it comes to regulatory enforcement. The legal environment is predictable, and laws are fairly and consistently enforced for both local and foreign companies in most countries. Additionally, most countries are aligned with some form of international regulations. International standards are general favoured over domestic standards, and many countries are party to international agreements such as the UN Convention on electronic contracting, World Trade Organization (WTO), APEC, EU and others regional privacy and data protection frameworks.

**Plus point: Incentives and Tax-Exemptions**

Some countries such as South Korea, Singapore, Taiwan and India do offer some form of incentive and/or tax exemption to encourage growth in the cloud computing industry. While not all financial assistance directly correlate with the cloud computing industry; as some are riding on other areas such as R&D and IT, Cloud service providers should take the opportunity to be one of the pioneers in the industry within the region, and gain competitive advantage via these vehicles.

# 2. Country Reports

## 2.1. Australia




The Australian Commonwealth Government has embraced cloud and a number of agencies such as Australian Government Information Management Office (AGIMO) have published cloud related standards and policies to guide the public sector cloud adaptation approach. Despite the lack of financial incentives, these standards and policies have been influential across the private sector. Local, regional, and global cloud service providers are well represented and used by Australian business.

The Australian IT services market remains biased towards a traditional bricks and mortar on-premise IT approach. While cost savings have driven a degree of cloud adaptation, the adoption rate has disappointed (and surprised) many of the Cloud service providers. Concerns relating to cloud computing revolve around compliance with Australian privacy laws (particularly security obligations and trans-border data flow constraints), the ability to audit compliance, concerns about subcontracting and a perception that service providers are inflexible in contract negotiations.

Key laws are based on international models, and Australia is an active participant in the development of international standards. Australia has up-to-date cybercrime laws and ratified the Convention on Cybercrime in late 2012. Australia also has comprehensive electronic signature and electronic commerce laws in place. Also in 2012, Australia dropped a long-term proposal for mandatory Internet content filtering that may have acted as a barrier for innovation in the digital economy. In addition to this, further improvements were passed to its existing privacy legislation, including stronger powers for the regulator. Intellectual property laws in Australia provide a comprehensive and balanced layer of protection for cloud computing services and the digital economy. Australian ICT infrastructure is reasonably well developed, and significant progress has been made in the rollout of a National Broadband Network that will provide further capacity to facilitate the digital economy.

### 2.1.1. Details on factors affecting cloud computing

**Regulatory Environment**

Australian legislation is broken to two levels: Commonwealth (federal) and State. The Privacy Act 1988 is federal legislation and is the main piece of legislation that governs the handling of personal data in Australia. The Privacy Act contains principles about the way in which personal information should be handled. There are currently separate principles governing the handling of information by the public sector (known as the Information Privacy Principles (IPPs)) and by the private sector (known as the National Privacy Principles (NPPs)).

The IPPs pertain to collection, use and disclosure, data quality, data security, openness, access and correction, whilst the NPPs additionally regulate the use of government identifiers by the private sector, anonymity, trans-border data flows and sensitive information. On 13 March 2014, amendments to the Privacy Act will become effective and the IPPs and NPPs will be replaced by a single new set of common principles known as the Australian Privacy Principles (APPs).

In addition, each of the states has additional legislation such as Privacy and Personal Information Protection Act (New South Wales) 1998, State Records Act (New South Wales) 1998 and Health Records and Information Privacy Act (New South Wales) 2002. Some of the key considerations are that data can be stored in the cloud outside of Australia but “appropriate” controls must be in place. It is also at the discretion of the data custodian whether to disclose any suspected data breaches. To date, only the

Australian Prudential Regulation Authority (APRA), the financial regulator, has the power to enforce data protection control requirements across the financial sector.

Although the Privacy Act is federal legislation, it does not regulate State or Territory agencies, except for the Australian Capital Territory (ACT). A State or Territory government which is outsourcing its data may seek a contractual commitment by the service provider to comply with the State or Territory privacy principles in addition to the service provider's obligation to comply with the NPPs.

#### 2.1.1.1. Cloud access

While there are no specific laws and regulations that govern cloud computing, there may, nevertheless, be incidental regulation of cloud-based activities, principally as a consequence of the Privacy Act 1988 and, in the case of internet service providers, schedule 5 to the Broadcasting Services Act 1992 (which regulates the content of online services). The Australian Internet Industry Association (AIIA) has also promoted codes of practice in relation to cybercrime and content.

In addition, though there are no tax benefits to encourage the use of cloud computing, there are also no tax benefits that encourage the use of internal resources and discourage the use of cloud computing.

#### 2.1.1.2. Data safety

A warrant is typically required, though not directly, to access data held or transmitted by data hosting providers, carriers or other service providers. There is an obligation under the Privacy Act and other legislation to permit access by individuals and by the privacy Commissioner and other authorities in specific circumstances, and the question of a warrant in these circumstances would only arise in the event of non-cooperation. Australian law incorporates powers for investigators to compel the disclosure of data, including encrypted data, to law enforcement agencies under specified, but limited, circumstances.

Also, the Telecommunications (Interception and Access) Act 1978 which permits access for authorities to intercept/access or conduct surveillance on data under warrant by law enforcement agencies in specific, but limited, circumstances.

The Privacy Act 1988 also has exterritorial effect, under section 5B, where an organization handling information is Australian or the organization has collected information from within Australia. With regards to enforcement by a foreign entity, the Foreign Judgments Act 1991 is a statutory scheme under which Foreign Judgments can be enforced in Australia. With respect to enforcing Australian judgments overseas, the Foreign Judgments Regulations 1992 identify those countries with which Australia has reciprocal enforcement arrangements, a notable exception being the United States of America.

#### 2.1.1.3. International consistency

The Office of the Australian Information Commissioner (OAIC) is the national data protection regulator responsible for overseeing the Privacy Act. The Privacy Commissioner's office being under-resourced means that enforcement is sometimes selective. The Act also does not provide the Commissioner with the power to directly enforce his or her determinations (although application can be made to the Federal Court or Federal Circuit Court for an enforcement order).

There are penalties enforced for non-compliance under the Privacy Act. There is overlapping regulation but no evidence of "turf wars". The most common overlap occurs between the Office of the Privacy Commissioner which administers the Privacy Act, and the Australian Communications and Media Authority which administers the Spam Act 2003.

#### 2.1.1.4. Cross border movement

Privacy legislation at commonwealth level, and in most states and territories, incorporates restrictions on trans-border data flows. At state level there is an obligation to inform the State Records Authority that personal information about the state citizens are stored outside of the state borders. APRA has also

guidelines to dictate de-identification of customer records if stored outside of Australia but this applies for the financial sector only.

Personal information may only be transferred outside of Australia or to a different organisation (including a parent company) where the organisation reasonably believes that the information is subject to a law, binding scheme or contract which effectively provides for no less protection than the Privacy Act and it has been disclosed in the organization's privacy policy. There can be no reliance on contractual provisions and the organisation must also ensure that there are mechanisms that the individual can access to take action to enforce the protections of that law or binding scheme. This means under The Privacy Reform Act of 2012, cloud users may be held "strictly liable" for their cloud providers non-compliance violations.

The National Privacy Principle 9 prevents a private sector organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or some other circumstances. Consent is not mandatory under the NPPs (or APPs[6] which will come into force on 13 March 2014). If consent is obtained, however, it is lawful for data to be transferred overseas. Such consent can be express or inferred.

A foreign company conducting business in Australia, other than through an Australian subsidiary, must also register as a foreign company with the Australian Securities and Investment Commission.

#### 2.1.1.5. Regulatory stability & enforcement

While the existing legislation is ambiguous enough to cover all normal circumstances and any court of law would interpret existing acts (e.g., Privacy Act) to apply in a case where no direct match would exist, various guidelines have been published for government departments, however, particularly the Cloud Better Practice Guides released by the Commonwealth Department of Finance and Deregulation in February 2012, and the Guidelines for Victorian Public Sector Organisations in respect of Cloud Computing published by the Victorian Privacy Commissioner in May 2011.

New laws are typically introduced in a transparent manner with public input. For example, there is a fifteen month transition period granted by the Privacy Amendment Act 2012 so that organisations can prepare for the amended legislation which comes into effect in March 2014. Whilst there is no legal requirement or established convention relating to public input prior to the enactment of legislation, laws which are relevant to cloud computing have typically involved public consultation.

In relation to the example we provided regarding the Privacy Amendment Act 2012, the reforms were the subject of public consultation in relation to recommendations by the Australian Law Reform Commission in 2007, public consultation regarding proposed new privacy principles in June 2010 and public consultation regarding credit reporting components of the legislation in June 2011.

In related areas, the government released a consultation paper regarding mandatory data breach notification in 2012 (which has been followed by legislation enacted on 29 May 2013) and previously, in 2011, a public discussion paper on the introduction of a statutory privacy right.

In short, where laws tend to involve technology or various forms of radical change, it is more likely than not that there will be public consultation.

There are also no industry agnostic rules or regulations which apply specifically to subcontracting arrangements under a cloud computing services contract outside of the APPs noted above. In circumstances where the Australian Consumer Law applies, there are restrictions on excluding statutory guarantees relating to the quality of goods and services in some circumstances. Similarly, liability for false or misleading conduct, and various breaches of the Competition and Consumer Act, cannot be excluded. The Australian Consumer Law can also have the effect of invalidating unfair terms in standard form contracts.

[6] http://www.oaic.gov.au/images/documents/privacy/privacy-guides/comparison_guide_APP_NPP.pdf

Although, there are no laws or regulations that discriminate based on the nationality of the vendor, developer or service provider, the State of Victoria has an Industry Participation Policy (VIPP) which requires government departments and agencies to consider opportunities for local industry when inviting tenders for projects valued in excess of $3,000,000. Shortlisted bidders are required to provide VIPP Plans which demonstrate the benefits to local industry if they are the successful tenderer.

There are no requirements covering the establishment of a taxable nexus on equipment and services that are involved in providing cloud computing services. Although there are no specific tax related to cloud computing, general tax principles apply.

Australia has been a WTO member since 1 January 1995 and a member of APEC since 1989. Australia has committed to WTO and ISO best practice regarding the prioritization of international standards. In addition, Australia is party to UN Convention on Electronic Contracting.

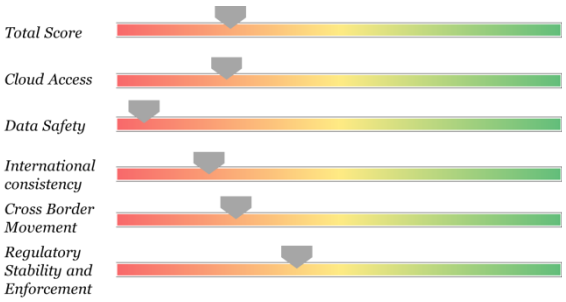
## 2.1.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Privacy Act 1988** | Personal data | Contains principles about the way in which personal information should be handled. | Data can be stored in the cloud including outside of Australia but "appropriate" controls must be applied. It is at the discretion of the data custodian whether to disclose any suspected data breaches. |
| **Australian Privacy Principles (APPs) Effective March 2014** | Personal data | Single set of principles to replace the current IPPs and NPPs as outlined below. | Consolidated principles apply to both government agencies and other organizations. Organizations must ensure third parties do not breach the APPs (except for APP 1) and may be held liable for violations. |
| **Information Privacy Principles (IPPs)** | Personal data | Contains principles about collection, use and disclosure, data quality, data security, openness, access and correction. | Although IPPs mainly cover how government agencies collect personal information, on 13 March 2014, amendments to the Privacy Act will result in the IPPs and NPPs being merged into a new set of common principles known as the Australian Privacy Principles (APPs). |
| **National Privacy Principles (NPPs)** | Personal data | Contains principles about the use of government identifiers by the private sector, anonymity, trans-border data flows and sensitive information in addition to IPPs. | An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.<br><br>Prevents a private sector organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or some other |

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| | | | circumstances. |
| **Broadcasting Services Act 1992** | Online services | Regulates the content of online services. | If the internet content hosted outside Australia is prohibited content or potential prohibited content, the ACMA must: (a) if the ACMA considers that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency--notify the content to an Australian police force; and (b) notify the content to internet service providers so that the providers can deal with the content in accordance with procedures specified in an industry code or industry standard (for example, procedures for the filtering, by technical means, of such content).<br><br>Bodies and associations that represent the internet service provider section of the internet industry may develop industry codes. |

# 2.2. China

In 2012, China's State Council issued the "Twelfth Five-Year" national strategic emerging industry development plan "to regard cloud computing as an important direction to support the development of the next generation of information technology and strategic emerging industries.




Cloud computing is one of seven strategic industries included in the latest Five-Year Plan (2011–15), giving it a share of a $600 billion investment by the government. Within the plan, there is also a focus on developing indigenous hardware and software to enable the cloud.

The National Development and Reform Commission, Ministry of Industry and Information Technology have carried out cloud computing innovation and development of pilot demonstration in five cities (Beijing, Shanghai, Shenzhen, Hangzhou, and Wuxi). Also, more than 30 local governments have announced a cloud computing industry development plan but domestic enterprise demand for public cloud services is still low due to security and connectivity issues and access to broadband is not consistent or continuous. Another challenge for public cloud adoption is trust, and more work needs to be done to build enterprises' trust in cloud computing.

Investments in research and data centers have also been made by cities (such as Shanghai and Chongqing) and corporations (most notably, Chinese telecom and network companies such as China Mobile and Huawei).

## 2.2.1. Details on factors affecting cloud computing

**Regulatory Environment**

There are no specific laws and regulations that govern cloud computing or prohibit against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data in general. However, the Decision of the Standing Committee of the National People's Congress on Strengthening Protection of Network Information, promulgated on December 28, 2012 (the "Decision") contains high-level requirements for Internet service providers and other types of entities (Data Collectors) on protecting “electronic personal data” which means electronic data that may identify a person and electronic data that relate to a person’s privacy.

The Decision (a) prohibits illegal collection or sales of electronic information that involves personal identity or privacy; (b) requires data collectors and users to disclose their policies, purposes, means and scopes, and to obtain prior consent from data providers for the collection and use of personal data; and (c) demands strict safeguard and protection of confidentiality for personal data.

The Guideline on Protection of Personal Information within Information Systems for Public and Commercial Services (the "Guideline") jointly issued by the General Administration of Quality Supervision, Inspection and Quarantine of PRC and the Standardization Administration of PRC provides a non-binding standard on how to protect privacy and improve data security. In addition, several provisions that touch on the protection of privacy and data security can be found in different regulations issued by lower-level authorities (e.g., the Ministry of Industry & Information Technology (the "MIIT")).

Under the Notice of the People's Bank of China on Banking Financial Institutions Protecting Personal Financial Information (the “Notice), financial institutions are obliged to protect individuals' personal financial information, and the notice forbids banks from storing or processing personal financial information obtained in China outside of the country.

People's Republic of China on Guarding State Secrets the Law prohibits the transfer of information related to China's national security and interests outside of China's borders without the approval of relevant Chinese authorities, which can include information pertaining to the economic development of state-owned enterprises.

#### 2.2.1.1. Cloud access

While there are no regulations that govern cloud computing specifically, there are also no prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data in general.

The banking and telecommunications sector have specific laws and regulations governing them though they are not directly related to cloud computing.

#### 2.2.1.2. Data safety

The Decision provides broadly that competent authorities have the authority to take enforcement actions for breaches of the Decision, generally the enforcement powers include warnings, monetary penalties, confiscation of illegitimate gains obtained from violation, revocation of permits or cancellation of registrations, suspension of websites, prohibiting the responsible person from engaging in internet service provision and noting such violation on the records of the entity in question and making such records public.

The Chinese regulations have no extraterritorial effect unless the related violation falls within the PRC Criminal Law sections containing provisions on extraterritorial offences. Action can also be enforced by a foreign authority on request, though it is subjected to recognition and enforcement procedures in accordance with convention or treaty binding to the PRC government.

#### 2.2.1.3. International consistency

As there is no national data protection authority in the People's Republic of China (PRC), regulators for different sectors will be responsible for the enforcement of regulations in their respective sectors (e.g., MIIT, China Security Regulatory Commission (CSRC), China Banking Regulatory Commission (CBRC), China Insurance Regulatory Commission (CIRC), etc.). While individual regulators may overlap in terms of regulations and differing interpretation, this may not cause an undue burden on companies. Of greater concern for many companies, many national regulations may be applied differently on a province by province perspective.

The Guideline is a voluntary national standard (lacking of the force of law).The Decision has the same legal effect as a law. However, for State Secret Law, Chinese authorities have broad discretion to determine the scope of State secrets. China's definition of a state secret often includes commercial information related to transactions with state owned enterprises. A determination as to whether the information at issue is considered to be a State Secret may depend on many criteria, including the nature of the industry involved and the State's interest in the company and the political climate at the time the issue arises.

Although China does not favour international standards over domestic standard, they have committed to a 'target' of 70% of standards being compliant with international standards by 2014. China is a signatory to the UN Convention on Electronic Contracting and has applied to accede to the WTO Agreement on Government Procurement.

#### 2.2.1.4. Cross border movement

Under the Guideline, without expressed consent from the subject of the personal information, or explicit authorization by laws or regulations, or approval of the competent authorities, the administrator of the personal information is not allowed to transmit any personal information to any overseas recipient (including any overseas individual and any organization or institution registered overseas).

In additional to the Guideline, one section of the PBOC (i.e., People's Bank of China) rules prohibits financial institutions from providing personal financial information to foreign entities unless otherwise stipulated by laws and regulations or other rules of PBOC.

Under certain circumstances, foreign cloud service providers may need to have local presence, such as the following: (a) PRC laws require that certain data (such as data of government authorities or financial institutions) be processed or stored within the PRC. In order to provide cloud computing services for such data, foreign service providers may need to set up local companies, (b) if a foreign service provider plans to rent infrastructure or facilities within the PRC to provide cloud computing services, it may also need to set up a local company, (c) with respect to the government procurement, in order to provide domestic products or services which are preferentially considered, the foreign companies may need to set up local companies in China to carry out the manufacturing or provision of service.

China is an observer, but not a full member, of the WTO plurilateral Agreement on Government Procurement. However, in 2012 China began negotiating accession to full membership.

#### 2.2.1.5. Regulatory stability & enforcement

The PRC laws require telecommunication business operators to protect the network security by implementing certain safety measures, including evaluating potential security risks, carrying out rehearsals to test the effectiveness of security measures and ensuring backup of key infrastructure and data. In addition, it is a general requirement under the PRC laws that telecommunication business operators should have the capacity/credibility to provide long-term services to their customers. Since some types of cloud service are likely deemed telecommunication services in the PRC, the providers of cloud computing services may also need to satisfy this requirement.

Although there is no general security and audit requirement for hosting digital data, the PRC laws stipulate specific security requirements for data relating to state secrets.

In additional, for special products relating to computer information system, information security products and encryption products, compulsory certification, manufacture permit or sales permit may be necessary.

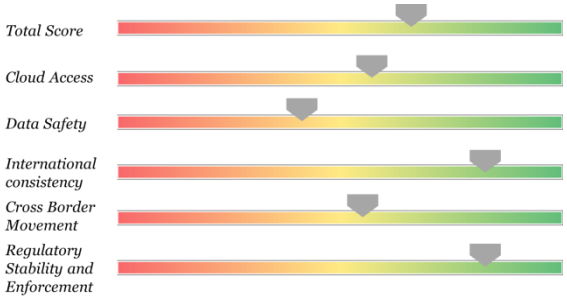
PRC laws do provide for, in particular cases, some different treatment based on nationality of the vendors, developers or service providers. For instance, in the event of government procurement under Article 10 of the Law on Government Procurement (2003), goods may only be purchased from foreigners under exceptional circumstances — although, in practice, procurement from foreign suppliers appears to occur routinely for some products, and in addition, China offers favourable market access treatment to qualified service suppliers from Hong Kong, Macao and Taiwan in accordance with partnership arrangements with these regions. In addition, enforcement of laws may vary between local and international providers.

### 2.2.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Information security technology – Guideline for personal information protection within information system for public and commercial services ("Guideline")** | Personal data | Contains detailed personal information protection requirements on each of data collection, data possessing, data transfer and data retention phases. | The "recipient of personal information" (by definition including cloud provider) shall process the personal information in accordance with the Guidelines and the entrustment agreements entered into with the information controller, and, shall delete the related information immediately after the processing task. |
| **The Decision of the Standing Committee of the National People's Congress on Strengthening Protection of Network Information, promulgated on** | Personal data | Contains high-level requirements for Internet service providers and other types of entities (Data Collectors) on protecting "electronic | The Decision affirms existing obligations on governed entities to police information posted on a website or transmitted over a network.<br><br>Provides broadly that competent authorities have the authority to take enforcement actions for breaches of the |

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **December 28, 2012 ("Decision")** | | personal data" | Decision.<br><br>Violations may subject Data Collectors to a series of penalties, including warning, monetary fine, confiscation of illegal gains, revocation of license, take-down of website and disbarment of relevant personnel from engaging in Internet services. |
| **Other** | Various | Each province may have their own laws which may not align to national laws. | Organizations must navigate potentially conflicting laws across multiple jurisdictions. |

# 2.3. Hong Kong




Hong Kong is increasingly becoming the North Asia data hub with many cloud service providers setting up data centers in the SAR. World leading broadband penetration and excellent international connectivity, coupled with good policy governance, provides a strong platform for cloud adoption by HK government and local businesses.

In general, there is no specific incentive provided to adopt cloud computing in Hong Kong. However, various funding schemes about information technology are in place. Innovation and Technology Fund provides funding to research and development projects of Hong Kong companies, including cloud computing. SME Funding Schemes also provide funding to assist the development of SMEs in Hong Kong, including adoption of cloud-based services.

The main concerns inhibiting cloud adoption include data privacy, security, concerns from banking regulators, cost, and transparency of Cloud service providers' security controls.

In 2012, privacy laws were tightened based on a case of illegal data sharing for marketing purposes. While this was not related to cloud computing / cross-border data movement, it may have an impact on these areas.

## 2.3.1. Details on factors affecting cloud computing

**Regulatory environment**

The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data (PCPD). It was recently amended by the Personal Data (Privacy) (Amendment) Ordinance in July 2012. Most of the amendments introduced by this Ordinance came into force on 1 October 2012.

The PDPO's core provisions are set out in six Data Protection Principles ("DPP"). These principles are the cornerstones of the Ordinance and can be summarised as follows: Purpose and manner of collection, accuracy and duration of retention, use of personal data, security of personal data, information to be generally available and access to personal data.

In addition, the Hong Kong Monetary Authority (HKMA) provides supervisory guidelines to all authorized institutions on outsourcing which include cloud-based services. HKMA requires authorized institutions to ensure that each outsourcing arrangement complies with relevant statutory requirements and common law customer confidentiality; controls must be in place to ensure that requirements of customer data confidentiality are observed and proper safeguards must be established to protect the integrity and confidentiality of customer information.

**Enforcement environment**

The PCPD is responsible for overseeing compliance with the Ordinance. If a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Such enforcement notice may include penalties for non-compliance.

### 2.3.1.1. Cloud access

While there are no specific laws and regulations that govern cloud computing, there are various pieces of legislation that may impact the cloud service. For instance, the Electronic Transaction Ordinance provides a legal framework for the conduct of secure electronic transactions. Also, Cloud Telecommunications

Service Provider (CTSP) is regulated under the Class Licence for Offer of Telecommunications Services, created under Telecommunications Ordinance.

#### 2.3.1.2. Data safety

The Interception of Communications and Surveillance Ordinance regulates the interception of communications by authorities. This Ordinance allows official authorities to intercept/ access or conduct surveillance on data. The Ordinance specifies the authorizations allowed (judge, executive, and emergency) along with the types of interception and duration permitted.

#### 2.3.1.3. International consistency

Laws are also generally fairly and consistently applied in Hong Kong. While individual regulators may overlap, this does not cause an undue burden on companies. Regardless, the HKMA tends to have more restrictions on cloud usage by financial institutions.

#### 2.3.1.4. Cross border movement

Hong Kong does not currently have any prohibitions or conditions for storage or transfer of general data outside of their jurisdiction. However, section 33 of the PDPO prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions set out in section 33(2) is met. Section 33 is currently not in force, but could be enabled in the future.

Despite section 33 not being in force, the Privacy Commissioner recommends that companies that transfer collected personal data to places outside Hong Kong should ensure that such data is treated with a similar level of protection as if it resides in Hong Kong in order to meet the expectations of individuals providing their personal data. Furthermore, individuals who provide their personal data to such companies should be made aware of the trans-border arrangements with regards to how their personal data is protected.

Hong Kong currently has no laws or policies that mandate the use of or specify a preference for certain products or cloud service provider. Foreign Cloud service providers are also not subject to additional material obligations or requirements compared to local Cloud service providers.

#### 2.3.1.5. Regulatory stability & enforcement

New laws are typically introduced in a transparent manner though public consultation may not necessarily occur. In some cases the Government may decide to publish a “White Bill” for consultation to invite public views on the contents, before finalizing the policy.

Also, Hong Kong has an Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) and the Prevention of Bribery Ordinance (Cap. 201) that would relate to the collection, storage, transfer, access or retention of data.

Although there are no specific security and audit requirements for hosting digital data or security related certifications or standards required before using certain technology products in the country, the PDPO would apply to regulate personal data that is hosted.

Hong Kong currently has no rules or regulations which apply to subcontracting arrangements under a cloud computing services contract. There are also no legal terms and conditions that a cloud computing service provider is required or recommended to incorporate into its cloud service agreements.

Hong Kong is expected to follow OECD guidance in the treaty context for a taxable nexus regarding equipment and people.

Hong Kong does not impose specific tax legislation with regards to cloud computing service providers but the general tax principles are applicable. Cloud computing usage is also not subjected to VAT in Hong Kong.

Though there is no specific tax levied on cloud computing, there are also no benefits that could encourage cloud adoption.

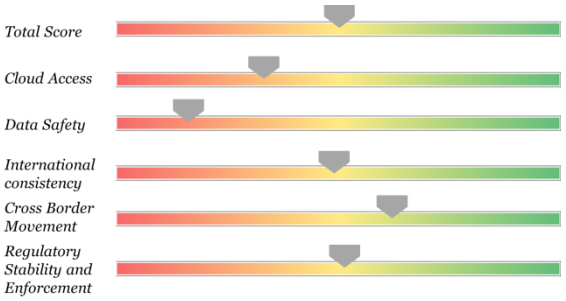
International standards are carefully considered in Hong Kong since government authorities such as the Office of the Telecommunications Authority (OFTA) in Hong Kong has accepted the WTO TBT Code of Good Practice for the Preparation, Adoption and Application of Standards.

As China is party to UN Convention on Electronic Contracting, Hong Kong would be included as well.

## 2.3.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Personal Data (Privacy) Ordinance (PDPO)** | Personal data | Contains principles governing the collection, access, processing, transfer and security of personal data. | Written consent of the individual is required before data is transferred to an overseas location. |

# 2.4. India




India has a strong interest in ICT services development. The law in India has not entirely kept pace with developments in cloud computing, and some gaps exist in key areas of protection. India's cybercrime legislation also requires updating to conform to international models. Some laws and standards in India are not technology neutral (e.g., electronic signatures), and these may be a barrier to interoperability.

However, in 2012, India finally updated its copyright laws to cover modern copyright issues such as rights management information and technical protection measures. India is now expected to ratify the WIPO Copyright Treaty. The development of India's technology sectors remains challenging, with low levels of broadband and personal computer penetration.

India is forecasted to enjoy aggressive cloud growth. However, there are significant challenges at present for India taking on a leading role across the region for Cloud Computing including the quality of its network, broadband and power grid capabilities. An improved and clearer regulatory situation in India would also make India more attractive to Cloud Computing customers and service providers.

At this time, there are Special Economic Zones (SEZ) created to provide incentives to organizations in IT and IT-enabled services. However, there is no specific focus on cloud-computing.

## 2.4.1. Details on factors affecting cloud computing

**Regulatory environment**

India's Information Technology Act, 2000 ("Act") deals with the regulations regarding data privacy and data protection. It contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically) and covers key principles for data transfer, storage, etc. for the protection of data. The two primary sources of regulation are Sections 43A and 72A of the Act.

In 2011, India adopted new rules as part of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules. India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("Privacy Rules"). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information, to comply with certain procedures.

The regulations introduced in 2011, were applicable to all companies and had many unintended consequences on cloud providers and outsourcers. Due to these concerns, the regulations were clarified to sensitive personal data originating outside of India is not covered. Now the regulations only apply to Indian companies collecting data from "natural persons".

### 2.4.1.1. Cloud access

While India has no specific regulation that governs cloud computing in general, there may be other legislation or implications with respect to various other laws and regulations directly or indirectly impacting such services. There are also no specific prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular type of data.

### 2.4.1.2. Data safety

Under Section 90 of the Criminal Procedure Code 1973, a 'document' may be sought from any person for the purpose of investigation of an offence. As a general rule some form of written order is required for grant of access to data available with an intermediary.

Section 69 of the Information Technology (Amendment) Act, 2008 empowers the Central or the State Government or any of its officers to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer source where it is necessary to do so in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign states, or public order. This affects any electronic information including encrypted data. Organizations may be forced to provide assistance to allow access to computer resources, intercept data, decrypt information, and provide stored data. Reasons for providing access are documented, but may not go through formal judicial oversight. Section 1(2) and Section 75 of the Act provide that the Act applies to the whole of India and to any offence or contravention of the Act committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Though an action arising out of the violation of a foreign data protection law cannot be brought in India, in appropriate cases of civil liability a decree of a foreign court may be enforced in India.

India does not conduct customs monitoring for data flowing over borders.

### 2.4.1.3. International consistency

There is no effective agency which is specifically responsible for enforcement of regulations for data storage and transfer. However, a special Adjudicating Authority has been appointed under Section 46 of the Act for adjudicating claims under the Act. There are penalties for non-compliance with the Act, including imprisonment. At present the Ministry of Communications and Information Technology is the nodal ministry for both telecommunications and information technology and we do not foresee a turf war of ministries. Regulations appear to be consistently applied to local and international companies.

### 2.4.1.4. Cross border movement

India has no restrictions for cross border data transfer from an overall perspective but there may be specific industries that have regulatory or statutory requirements towards data filtering (e.g., banking).

Rule 7 of the Security Practice Rules states that sensitive personal data or information can be transferred to any person or body corporate in or outside India if the level of data protection as provided under the Security Practice Rules is adhered to. In addition, transfer will only be allowed if it is necessary for the performance of the lawful contract between the body corporate and any person on its behalf or where the data subject has consented to data transfer.

Rule 5 of the Security Practices Rules states that for the collection of sensitive personal data, the consent of a data subject should be in writing through letter, fax or e-mail. Nevertheless, there is no mandatory data transfer agreement required by the national regulator for the transfer of data to an overseas location. However, the revised privacy rules only apply to Indian companies that collect information from "natural persons". It is the companies collecting and sending the data, as opposed to outsourcers, who are responsible for data privacy according to the rules of their respective countries.

India currently has no laws or policies that mandate the use of /specify a preference for certain products (including, but not limited to types of software), services, standards or technologies. There are also no laws/regulations that discriminate cloud service providers based on their nationalities.

### 2.4.1.5. Regulatory stability & enforcement

Unless there is a restriction imposed on a particular trade/service, authorities cannot consider it impermissible. Cloud service providers are also likely to face challenges in interface with law enforcement agencies in relation to request for information about users/data. In the absence of clear guidelines, a balance between compliance with lawful requests of law enforcement agencies and privacy of users has to be maintained.

In India, a consultative process is generally undertaken before introduction of a law. A law cannot be introduced without receiving assent of a majority of both houses of the Indian Parliament.

India also has a Prevention of Money Laundering Act (PMLA), 2002. Under the PMLA the Directorate of Enforcement is responsible for investigation of money laundering offences and tracing and securing of proceeds of crime, though there are no specific requirements for the collection, storage, transfer, access or retention of data. However, investigative agencies have wide powers to request for user information from service providers.

Based on the Security Practice Rules, Cloud service providers must have a privacy policy published on its website. Also, they have to comply with International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" when dealing with sensitive personal data. The reasonable security practices and procedures may be specified in an agreement between the parties.

In respect of financial data the Reserve Bank of India prescribes guidelines from time to time for various banking practices which include IT infrastructure security requirements and these may be relevant for servicing financial sector clients.

India has no effective agency which is specifically responsible for enforcement of regulations for data storage and transfer. However, a special Adjudicating Authority has been appointed under Section 46 of the Act for adjudicating claims under the Act. Penalties are enforced for non-compliance with the Act.

There are no rules or regulations which apply to subcontracting arrangements under a cloud computing services contract. However, every person to whom data is transferred must maintain the same level of security practices as applicable to the entity collecting data.

In addition, there are no legal restrictions on the exclusion of warranties (both statutory implied warranties and express warranties) in a cloud computing services contract. There are also no legal restrictions on the limitation of liability in a cloud computing services contract. However, a contract cannot over-ride or exclude a statutory liability.

There are no tariffs or other trade barriers on the downloading of software or to the physical transfer of software. There are no other specific rules or regulations that may be construed as trade barriers, when it comes to the downloading of applications or software from foreign sources.

India does not have any specific tax legislation governing cloud computing service providers. However, in April 2000, the government of India introduced Special Economic Zones. Overall Indian IT industry benefitted from the SEZ concept which included various duty and tax exemptions, including direct and indirect taxes.

India has been a WTO member since 1 January 1995 and prioritizes compliance with international standards. Currently, India is not a party to UN Convention on Electronic Contracting though it has expressed its interest to join APEC.

There is no mandatory requirement under the Act or Privacy Rules to report data security breaches. However, a corporate entity can be asked to furnish information to the Indian Computer Emergency Response Team (CERT-IN) related to cyber security incidents.

An intermediary is under an obligation to retain third party information for a period of ninety days and is required to provide information or other such assistance to government agencies that are lawfully authorized for investigative and protective cyber security activity.

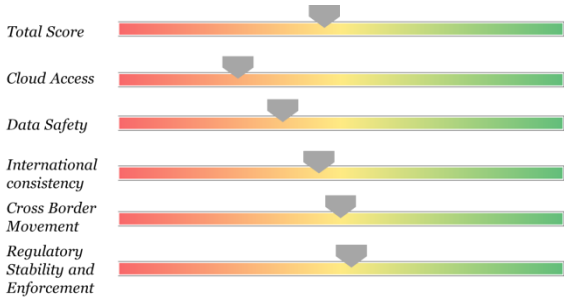
Section 79 of the Act provides an over-arching protection to intermediaries from liability for content so long as the due diligence requirements are fulfilled. The regime under the Copyright (Amendment) Act 2012 is specific to copyrighted content and is on similar lines as the intermediary guidelines. Infringing work found on an ISP's system would also not make the ISP liable unless the ISP is aware or has reasonable grounds to believe that the content is infringing material.

## 2.4.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Information Technology Act 2000** | Computer security and data protection | Contains key principles for data transfer, storage, etc. for the protection of data. | Provides the Controller of Certifying Authorities with the power to intercept any information transmitted through a computer resource, if certain criteria are satisfied.<br><br>Provides that the law shall apply to an offense (under the law) or contravention of the law committed outside India if the act or conduct involves a computer, computer system, or computer network located in India. |
| **The Information Technology (AMENDMENT) Bill, 2008** | Computer security and data protection | Updates to the Information Technology Act of 2000. | Mandatory requirements around interception of data, blocking access to sites, and cyber security. Non-compliance can expose cloud providers to civil and criminal penalties. |
| **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules)** | Personal data | Contains rules governing corporate entities collecting, processing and storing personal data, including sensitive personal information. | The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection. However, this rule only applies to Indian companies that collect information from "natural persons" |
| **Privacy Rules, 2012 revision** | Personal data | Revised to exempt "data outsourcing" and data related to non-Indian citizens. | Specifically designed to fix a problem in the 2011 law that would have been a challenge to outsourcers based in India (e.g., cloud providers, call centers). |

# 2.5. Indonesia

Indonesia continues to update and reform laws and regulations in the ICT sector, and the result is not always positive for cloud computing. In 2012 Indonesia introduced a new regulation to complement its existing electronic commerce laws. The new regulation is positive in some areas, such as the introduction of strengthened privacy rules. However, in other areas the regulation introduces significant barriers for cloud service providers.




According to the VMware Cloud Index 2012 commissioned by VMware in October 2012, 41% of business organizations in Indonesia said they already have adopted cloud solutions or approaches and this is projected to grow to 70% by early 2014. From the same report, the main concerns that may continue to hinder adoption of cloud services are access to reliable and affordable broadband, data privacy and security.

Although the copyright law in Indonesia is closely aligned with international models, some concerns remain regarding resources for investigating and enforcing copyright protections. The law remains uncertain regarding the exact role and liability of ISPs in relation to copyright breaches.

## 2.5.1. Details on factors affecting cloud computing

**Regulatory environment**

The types of data that are regulated may vary depending on the specific industry or sector. As an example, according to the Population Administration Law, the personal data that has to be protected includes: the particulars stated on a person's Family Registration Card, the Population Identification Number (PIN), date, month and year of birth, description of physical and/ or mental disability, PIN of biological mother, PIN of father, and records of certain important life events including records of birth, death, divorce, recognition of paternity, adoption, change of name, and change of citizenship.

Currently, the biggest impact on cloud computer in Indonesia is Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions. This Regulation has applies to individuals, government agencies, and companies that provide or operate electronic devices with electronic data. Providers delivering "public services" (which is not clearly defined) are subject to a registration requirement. Failure can range from fines to suspension of services. Beyond registration, additional requirements exist such as the need to have data center and disaster recovery location in Indonesia. Providers are also required to disclose minimum information to customers including terms and conditions, data protection, rights, and obligations as well as must obtain a certificate of reliability.

### 2.5.1.1. Cloud access

While there is no specific regulation governing cloud computing, a cloud provider may be categorised as an "Electronic System" provider under Law No. 11 of 2008 on Electronic Transactions and Information ("ETI Law"). There is also a general principle that the data of a person can only be used with the permission of the person concerned, unless otherwise provided by the relevant law or regulation.

Indonesia has a number of laws that concern data protection. These include Law No. 7 of 1971 on Basic Provisions on the Maintenance of Archives, Law No. 8 of 1997 on the Corporate Documents, Law No. 10 of 1998 on the Amendment of Law No. 7 of 1992 on Banking ("Banking Law") and Law No. 36 of 1999 on Telecommunications ("Telecommunications Law").

### 2.5.1.2. Data safety

Under the ETI Law, authorities can access and intercept data held or transmitted by data hosting providers as long as the process is carried out with the permission of the relevant head of the district court.

The ETI Law also has extraterritorial effect where electronic systems involved are located in the Indonesian jurisdiction.

### 2.5.1.3. International consistency

Since the legislative provisions governing privacy and/or data security are found in a number of different laws and regulations, restrictions on the use of personal data vary depending on the specific industry or sector.

According to Law No. 8 of 1997 on Corporate Document, corporate documents consisted of financial documents and other documents. The financial documents consisted of records, proof of bookkeeping, financial administration supporting data, which are evidence of the rights and obligations as well as the business activities of a company. The retention period of financial documents is 10 (ten) years. The retention period of other documents is adjusted to the needs of a company. This requirement is longer than typically required and may increase the retention requirements at cloud providers.

The Capital Markets and Financial Bodies Supervisory Body ("Bapepam LK") functions as the regulator of data privacy in the capital markets sector. Bank Indonesia also acts as the regulator with regard to banks' customer data privacy issues.

The financial industry is leading in consistently applying laws and regulations; however, this is not the case with other industries.

### 2.5.1.4. Cross border movement

While there is no specific regulation that provides prohibitions or conditions for storage/transfer of general data outside of Indonesia, the Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction (an ancillary regulation for the ETI Law) ("Reg. 82") regulates the transfer of data in Article 22 which provides that in any case that electronic information and/or electronic document is transferred, the provider has to explain the control and possession of the electronic information and/or electronic document. Where cloud providers offer services to the public, the data center must be located in Indonesia. However, further clarification on this requirement is still forthcoming. In addition, the country where the data is located must have the same standard of data privacy, and the regulators should be able to gain access to the data without hindrance of any local regulation or laws. However, electronic transaction for public services must have their data centre and recovery centre in Indonesia (Chapter 17).

Also based on Reg. 82, the data collector must ensure that the use or disclosure of personal data is based on the consent of the owner of such personal data, and in accordance with the purpose of being delivered to the owner of personal data on acquisition data.

### 2.5.1.5. Regulatory stability & enforcement

Although this is an area/service that not specifically governed by law/regulation in terms of use of data, there is general principle that the data of a person can only be used with the permission of the person concerned, unless otherwise provided by the relevant law or regulation.

According to Law No. 20 of 2012 on Formation of Legislation, parliament and government do dissemination a draft of law in order to obtain public input. The law also provides that public has the right to provide input verbally and /or written in the formation of legislation process.

Law No. 8 of 2010 on Prevention and Eradication of the Crime of Money Laundering does not specifically regulate cloud computing usage but imposes an obligation on financial services providers or other providers to report when they find suspicious financial transactions, whether the transaction data is stored in the cloud computing or not.

As an "Electronic System" provider, there are obligations of electronic system providers on security and audit requirements. These obligations include: ensuring agreements on minimum service level and

information security as well as internal communication security, protecting and ensuring the privacy and personal data protection of users, and providing audit records on all electronic systems activities.

Nevertheless, some of these obligations still require ancillary regulations, namely specification of software used by electronic system provider, audit mechanism, security system, worthiness certificate, personal data protection, data centre and disaster recovery centre.

As Indonesia has no specific regulation governing cloud computing, there are no legal terms and conditions that Cloud service providers are required or recommended to incorporate into their service agreements. In addition, there are no specific legal restrictions on the exclusion of warranties and limitation of liabilities in service contracts.

Since there is no specific regulation that governs cloud computing, legislative provisions governing privacy and/or data security are found in a number of different laws and regulations. Therefore, restrictions on the use of personal data vary depending on the specific industry or sector. Penalties for offences related to personal data would also vary for the same reason.

As an example, parties failing to comply with Reg. 82 are subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions can come in the form of: written warning, administrative fines, temporary dismissal, and/or expulsion from the list of registrations.

While Bank Indonesia can impose penalties if any non-compliance is found, such penalties are specifically for the financial industry.

Indonesia does not currently have any requirements covering the establishment of a taxable nexus on cloud computing services. There are also no rules for characterising income from cloud computing for taxation purposes though Cloud service providers are subjected to withholding tax for providing services. Lastly, cloud computing is subjected to VAT.

Domestic standards in Indonesia are still favoured over international standards due to compliance risk even though most regulations were adopted from international standards.

To date, the government has not imposed any tariffs or other trade barriers on the downloading of software or applications from foreign sources.

Besides being party to UN Convention on Electronic Contracting, Indonesia has been a WTO member since 1995 and a member of APEC since 1989.

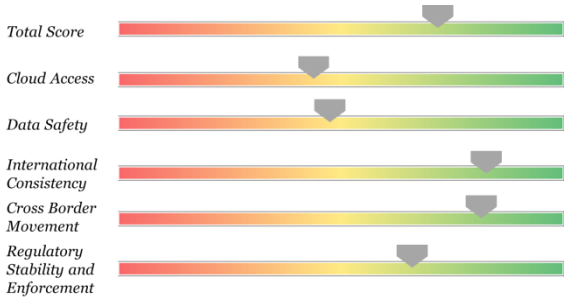
## 2.5.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Law No. 11 of 2008 on Electronic Transactions and Information ("ETI Law")** | Electronic information | Contains principles governing electronic systems preparing, collecting, processing, analysing, storing, displaying, announcing, sending, and/or disseminating electronic information. | Any Electronic System provider must provide its Electronic Systems in a reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems. Essentially, an Electronic System provider shall be liable for the provision of its Electronic Systems.<br><br>Hardware used by an electronic system provider shall obtain certificate of worthiness from the Minister. Software used by an electronic system provider for public interest shall be registered in the Ministry of Communication and |

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| | | | Information Technology.<br><br>An individual must be informed about the collection and use of their personal data. The data collector must ensure that the use or disclosure of personal data is based on the consent of the owner of such personal data, and in accordance with the purpose of being delivered to the owner of personal data on acquisition data. |
| **Provision of Electronic System and Transaction ("Reg. 82")** | Personal data | Contains principles regulating data protection and/or collection of personal data/personal information | Provider of an Electronic System must provide written notification to the owner of personal data, upon its failure to protect the personal data.<br><br>Provides the specific provisions on the obligation to set up a data centre in Indonesia for services to the public.<br><br>In any case that electronic information and/or electronic document is transferred, the provider has to explain the control and possession of the electronic information and/or electronic document. |

# 2.6. Japan

Japan ranks highly in the cloud computing world as it has a comprehensive suite of modern laws that support and facilitate the digital economy and cloud computing. Japan has also ratified the Convention on Cybercrime in 2012, setting a positive example for other countries. The government has committed to ensuring that by 2015, all households will have very high-speed fiber broadband connections even though broadband penetration rates are already very high.




According to the White Paper on Information and Communication in Japan published by the Ministry of Internal Affairs and Communications in 2012, 21.6% of businesses are using cloud computing services as of the end of 2011, and the Government is continuously promoting the spread of cloud computing in Japan.

Although Japan has a comprehensive suite of modern laws supporting and facilitating cloud computing, barriers inhibiting cloud adoption still exist. Some of the customer concerns, outside of regulations, include costs involved in upgrading or acquiring new systems, security and the difficulty of realising merits of cloud computing.

## 2.6.1. Details on factors affecting cloud computing

**Regulatory environment**

The Act on the Protection of Personal Information (Act No. 57 of 2003) ("APPI") governs the collection and use of personal information in Japan. It prescribes the rules and duties to be observed by entities handling personal information. The APPI applies to a business operator who uses, for its business in Japan, a personal information database, which contains personal information for more than 5,000 individuals, on any day in the previous six-month period (Business Operator Handling Personal Information ("BOHPI")).

In addition, various ministries, including the Ministry of Health, Labour and Welfare, the Japan Financial Services Agency and the Ministry of Economy, Trade and Industry have created guidelines regarding the APPI. These Guidelines are not laws, but are very persuasive in Japan and generally followed by business operators to which they apply.

The APPI distinguishes the terms "Personal Information", "Personal Data" and "Retained Personal Data" from each other. The duties imposed on BOHPI also vary among those terms. "Personal Information" is information about a living individual that can identify the specific individual by name, date of birth or other description contained in the information. "Personal Data" is Personal Information contained in a Personal Information Database. "Retained Personal Data" is Personal Data over which the BOHPI has the power to disclose, correct, add to, delete, cease to use, and delete or cease its provision to a third party.

**Security**

Japan has an entirely self-regulatory system of content regulation for online services. When requested to do so by a person who receives the provision of an Internet service, the Internet service provider must provide software for filtering content harmful to young people or a service to filter content harmful to young people.

**Enforcement environment**

As there is no one single central data protection authority in Japan, the Consumer Affairs Agency (CAA) will be the central authority for the APPI in general. In addition, each Ministry or Agency which governs

respective industrial sectors or matters is a competent authority to regulate and enforce the proper handling of personal information by a BOHPI.

Under Article 34.2 and 34.3 of the APPI, a competent minister can (1) require a BOHPI to file a report on its handling of Personal Information (Article 32), (2) advise a BOHPI on its handling of Personal Information (Article 33), (3) recommend a BOHPI to take necessary measures to correct a violation of certain APPI requirements (Article 34.1), (4) order a BOHPI to: (i) take the recommended measures in the APPI if the BOHPI did not implement such recommended measures without good reason, or (ii) correct a violation of certain requirements under the APPI when there is an urgent need.

#### 2.6.1.1. Cloud access

Though Japan has no specific laws and regulations that govern cloud computing in general, there are also no specific prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data in general.

The Japanese government and other relevant authorities have published guidelines relating to the protection of personal information in the industrial sectors they regulate, therefore, there are various guidelines for specific industry sectors, such as health-care, science, finance, employment, legal, education, welfare, in particular each affairs governed by each Ministry. These guidelines are not legally binding, but they function as the standards for the relevant law enforcement and are respected and usually followed by Japanese courts.

While there are no tax benefits that encourage cloud adoption, there are also no tax benefits for other IT resources which may discourage cloud adoption.

#### 2.6.1.2. Data safety

While Japan has no specific law that addresses the types of data that authorities can get access to for gathering of evidences, a search warrant allows authorities to intercept communications or obtain access to encrypted data.

In some situations when service providers voluntarily reply to inquiries from investigative authorities, the investigative authorities can access the data without a warrant. In this regard, if cloud computing service providers fall under “specified telecommunications service providers” under the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (“Provider Liability Limitation Act,” Act No. 137 of 2001), and if the requirements under the Provider Liability Limitation Act are satisfied, such service provider can be released from its civil liabilities by disclosing such information.

The Act on Wiretapping for Criminal Investigation (Act No. 137 of 1999) allows the investigative authorities to intercept communications with a warrant to the extent necessary to investigate serious organized crimes such as drug crimes, crimes using firearms, etc.

APPI can be applied to service providers who operate its business inside Japan even though APPI does not have an extraterritorial effect. On the contrary, a foreign company may directly file a lawsuit in a Japanese court. In addition, a final and binding judgement rendered by a foreign court or arbitration award is effective and enforceable as long as requirements set forth in Article 118 of the Code of Civil Procedure Law are met.

#### 2.6.1.3. International consistency

Although laws, regulations and guidelines applied to each sector or matter are applied to cloud computing service providers and users, overlapping regulations or inter-ministry turf wars do not take place as ministries and agencies involved usually discuss and harmonise their views among themselves. These laws, regulations and guidelines also tend to be consistently applied to local and international companies who operate their business in Japan.

No explicit preferences are granted to domestic suppliers with regard to procurement covered by the Agreement on Government Procurement. However, government guidelines for application service providers and other policies raise concerns about restrictions on data centre locations.

### 2.6.1.4. Cross border movement

While there are no specific rules that relate to the storage/transfer of data in general, Article 23 of the APPI states that consent must be obtained in advance from individuals when their personal data will be transferred to a third party, whether within or outside Japan.

Japan is a member of the WTO plurilateral Agreement on Government Procurement, which includes rules guaranteeing fair and non-discriminatory conditions of international competition. As such, there are no specific mandatory requirements or preferences in laws or policies for certain products and services. Foreign providers are also not subjected to additional localisation requirement nor are they discriminated against.

The Foreign Exchange and Foreign Trade Act contains regulations to enable proper expansion of foreign transactions and in the international community through the minimum necessary control or coordination of foreign transactions, and thereby to ensure equilibrium of the international balance of trade. The act states that the transfer of certain technical information is restricted based on the destination country.

### 2.6.1.5. Regulatory stability & enforcement

Although Japanese laws contain some unique provisions, the core principles are based on a mix of the OECD Guidelines and the EU Directive. The exemption for small data holdings in Japanese law is not compatible with the EU Directive. While laws that support and facilitate the digital economy and cloud computing exist, Japan still does not have a regulation that governs specifically cloud computing. Almost all private areas/services are governed by the APPI and the Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information ("METI Guidelines").

New laws to be introduced in Japan are typically made public over the Internet via the website of the House of Representatives and the House of Councillors prior to the discussion in the National Diet, Japanese legislative body. In addition, many guidelines to be established by government authorities are subject to public comments before being officially published. After enactment of new laws, they are made in public by publishing in the official gazette.

While the APPI requires that business operators prevent the leakage of personal data, it does not set out specific steps that must be taken. Guidelines from various ministries impose specific steps that business operators should take to ensure that personal data is secure.

Also, while there are no security related certifications or standards required or business continuity or recovery regulations, the METI have published the Information Security Management Guidelines for the Use of Cloud Services ("ISM Guidelines") for the benefit of secured use of cloud computing services. Additional management procedures were also set out in the ISM Guidelines.

Although respective laws, regulations and guidelines applied to each industrial sector or matter are applied to cloud computing services providers and users respectively, the Ministries and Agencies usually discuss and harmonize views among themselves. Thus, this would not be an obstacle to operate or use cloud computing services in Japan.

Japan does not require cloud service providers to incorporate specific legal terms and conditions into its cloud service agreements. However, the Japan Information Technology Services Industry Association (JISA), an industrial organization consisting of leading system integrators, computer system designers, development and related service providers, data processing service providers, and system operation and management services vendors, has published a model of terms and conditions for application services providers.

While there are no legal restrictions on the exclusion of warranties in a cloud computing services contract, Article 10 of the Consumer Contract Act (Act No. 61 of 2000) sets out that any clause that is extremely

disadvantageous to the consumer is invalid. Thus, if users of such services fall under the category of consumers, clauses which provide for the exclusion of warranties could be considered invalid (Article 8 and 10). In addition, even if the users are not consumers, such exclusion of warranties is considered invalid if it contradicts public order and morals.

Japan has no requirements covering the establishment of a taxable nexus on equipment/services that are involved in providing cloud computing services. There are also no rules for characterizing income from cloud computing services for taxation purposes. While cloud computing is not subjected to withholding tax on payments, cloud service usage is subjected to consumption tax.

Based on Article 19 and Article 20 of the APPI, a BOHPI, not only cloud computing service providers but also in general, has obligations to (1) make efforts to maintain personal data accurate and up to date, and (2) take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.

While there are no specific requirements to notify data subjects of personal data security breaches in the APPI, other guidelines such as the FSA (Article 22.3) and TB Guidelines (Article 22.1) include provisions that recommend the BOHPI to notify the data subject of security breaches. In addition, the FSA and TB Guidelines also require the BOHPI to report security breaches to its supervisory authorities.

Under the Provider Liability Limitation Act a cloud service provider is a "specified telecommunications service provider" and if the provider fails to take necessary steps to take down illegal materials despite a claim by a copyright holder, such provider may be responsible for the loss and damage incurred by the copyright holders under the Provider Liability Limitation Act.

The Copyright Act contains a controversial issue whether an indirect infringer of copyright is liable or not, because there is no explicit clause which prohibits indirect infringement of copyright. The Supreme Court held that, when the court decides who is the infringer of copyright, the court should consider the totality of the circumstances concerning the subject and the ways of reproduction, to what extent does the defendant engage in the reproduction of users, and other elements. Thus, depending on the situation, a court possibly could find that the cloud provider is responsible for the infringement of copyright. Japan prioritises compliance with international standards and is a party to the WTO Agreement on Technical Barriers to Trade. Japan, being a member of APEC, also has its privacy laws comply with the APEC Privacy Framework. However, Japan is not a party to UN Convention on Electronic Contracting.

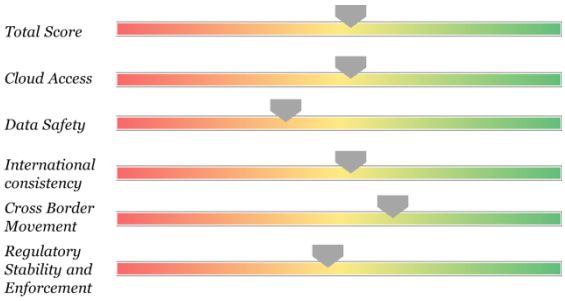
## 2.6.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Act on the Protection of Personal Information (Act No. 57 of 2003) ("APPI")** | Personal data | Contains rules and duties to be observed by entities handling personal information. | Regardless of whether the transfer is within or outside Japan, when Personal Data is transferred to a third party for their own use, consent must be obtained in advance from such individual to whom the Personal Data belongs.<br><br>A BOHPI, not only cloud computing service providers but also in general, has obligations to (1) make efforts to maintain personal data accurate and up to date (Article 19), and (2) take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data. |
| **Foreign Exchange and** | Foreign | Contains regulations to enable proper | Transfer of certain technical information is |

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Foreign Trade Act** | transactions | expansion of foreign transactions and the maintenance of peace and security in Japan and in the international community through the minimum necessary control or coordination of foreign transactions, and thereby to ensure equilibrium of the international balance of trade | restricted based on the destination country. |
| **Provider Liability Limitation Act** | Copyright | Contains guidelines relating to copyright and neighbouring rights | If the cloud computing service provider fails to take necessary steps to take down illegal materials despite a claim by a copyright holder, such provider may be responsible for the loss and damage incurred by the copyright holders. |
| **Consumer Contract Act** | Consumer interest | Contains regulations to protect the interests of consumers, and thereby contribute to the stabilization of and the improvement in the general welfare and life of the citizens | Any clause extremely disadvantageous to the consumer is invalid.<br><br>Some clauses that exempt or limit liabilities of cloud provider are void. |

# 2.7. Malaysia

The VMware Cloud Index 2012 indicates clear progress and a new era of IT transformation in Malaysia as half of Malaysian respondents (50%) planning to adopt cloud computing are projected to do so within the next 18 months. Based on news reports, one-third of organizations in Malaysia are using now some form of cloud computing. While reports indicate some progress in cloud adoption, concerns still surround cloud computing. Some of these concerns include security, privacy and sovereignty of data.




Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 ("PDPA"), has been passed by the Malaysian Parliament and came into force in November 2013 and is estimated to be fully implemented by January 2014[1]. The key principles of the PDPA are that of consent, notice and choice, disclosure, security, retention, data integrity and access.

*Note: due to the timing of the Act coming into force it is not included in the scoring.*

## 2.7.1. Details on factors affecting cloud computing

**Regulatory environment**

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 ("PDPA"), came into force in November 2013 and is estimated to be fully implemented by January 2014.[7]

The PDPA defines "personal data" as any information in respect of commercial transactions which – (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion but does not include any information processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Additionally, "sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinion, his religious beliefs or other beliefs of a similar nature, or the commission or alleged commission by him of any offence.

The PDPA principles state that it is the data user, and not the third parties that need to comply with the PDPA principles. Cloud service providers will fall within the definition of a 'data processor' i.e. any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes. The security principle (section 9 of the PDPA) provides that where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, ensure that the data processor – (a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and (b) takes reasonable steps to ensure compliance with those measures.

In legal proceedings, computer output is subject to the Evidence Act of Malaysia which specifies protections required for admissibility of data. In addition, Section 82 of the Income Tax Act 1967 and Section 167 of the Companies Act 1965 require various documents and records to be retained for seven years. However, Section 10 of the PDPA 2010 does not specify an exact retention period but merely states that the personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

[7] http://www.kpkk.gov.my/index.php?lang=en

**Security**

Although the Malaysian Government has pledged not to censor the Internet and there is no evidence of technological Internet filtering in Malaysia, state controls on traditional media do however spill over to the Internet such that there are instance of self-censorship and investigations of online dissidents.

**Enforcement environment**

The Personal Data Protection Commissioner ("Commissioner") can implement and enforce personal data protection laws, monitor and supervise compliance with the provisions of the PDPA, including issuance of circulars, enforcement notices or any other instruments to any person and investigate complaints. The Commissioner will be advised by a Personal Data Protection Advisory Committee. Decisions of the Commissioner can be appealed against through the Personal Data Protection Appeal Tribunal.

### 2.7.1.1. Cloud access

Presently there is no specific legislation in Malaysia which governs the provision of cloud computing services however certain licensing requirements may apply if the services fall within the scope of the Communications and Multimedia Act 1998.

Some laws or regulations that govern specific industry sectors are the Guidelines on the Provisions of Electronic Banking (e-banking) Services by Financial Institutions (Banking), General Consumer Code ('GCC') (Telecommunications), Malaysian Communications and Multimedia Content Code (Communications and Multimedia) and the Insurance Act 1996 (Insurance).

### 2.7.1.2. Data safety

While a warrant is usually required, authorities may search any premises without a warrant if they have reasonable cause to believe that the delay in obtaining the warrant will adversely affect investigations or will likely result in the opportunity for the tampering of or destruction of evidence. Such evidence may include general computerised or encrypted data.

Section 9 of the Computer Crimes Act 1997 states that the law applies, within and outside Malaysia, where the offense in question, the computer, program, or data were in Malaysia or capable of being connected to or sent to or used by or with, a computer in Malaysia at the material time. In addition, foreign judgements from superior courts of reciprocating countries may be registered in Malaysia to be enforced at any time within six years after the date of the judgment. The Reciprocal Enforcement of Judgements Act 1958 contains a list of the reciprocating countries.

### 2.7.1.3. International consistency

The Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Violation of the PDPA attracts criminal liability. The prescribed penalties include the imposition of fines or a term of imprisonment or both. Laws and regulations in Malaysia tend to be generally fairly and consistently applied, regardless of the nationality of the provider. While individual regulators may overlap, this does not cause an undue burden on companies.

### 2.7.1.4. Cross border movement

Section 129 of the PDPA 2010 provides that a data user shall not transfer any personal data outside Malaysia unless to such place as specified by the Minister, by notification published in the Gazette.

However, a data user may transfer any personal data outside Malaysia if – (a) the data subject has consented to the transfer; (b) transfer is necessary for performance of a contract; (c) transfer is necessary for conclusion of contract between the data user and third party; (d) transfer is for purpose of legal proceedings; (e) data user has reasonable grounds to believe transfer is for the avoidance or mitigation of adverse action against the data subject; (f) data user has taken all reasonable precautions to ensure personal data will not in that place be processed in any manner which would be a contravention of this

Act; (g) transfer is necessary to protect vital interests of data subject; or (h) transfer is necessary in the public interest.

### 2.7.1.5. Regulatory stability & enforcement

New laws do not go through any public notice period and are passed after a majority vote in the Dewan Rakyat (House of Representatives) and Dewan Negara (Senate).

The Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) makes provision for any authorization to release information (Section 9), disclosure to a corresponding authority of a foreign State (Section 10), prohibited disclosures (Section 11), permitted disclosures (Section 12), record keeping by reporting institutions (Section 13) and retention of records (Section 17). The AMLATFA also overrides all other secrecy obligations contained in other legislation.

The Communications and Multimedia Act 1998 established the Malaysian Communications and Multimedia Commission to regulate the information technology and communications industries. The Commission has the authority to regulate online speech. It has also established the Content Forum which implements voluntary guidelines for content providers in relation to the handling of content deemed offensive and indecent ('Content Code'). While there are no specific audit requirements, security measures and requirements are provided for under the PDPA.

Violation of the PDPA attracts criminal liability. The prescribed penalties include the imposition of fines or a term of imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defence. However, there is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

While there are no there are no requirements to use a specific product or service, the Government of Malaysia does however encourage the use of Open Source Software in the Public sector. Although there are such requirements, the Government procurement policy is to favour locally owned businesses and to consider international tenders if suitable ones are not available locally.

If the services provided fall within the scope of the Communications and Multimedia Act 1998, certain licensing requirements may apply and Section 263 of the Communications and Multimedia Act 1998 ("CMA") provides that, (a) a licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia; and (b) a licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security.

Also, if a foreign provider wishes to provide services in Malaysia, they cannot do so unless they incorporate a local company or register the company in Malaysia.

While there are no legal terms and conditions that a cloud service provider is required or recommended to incorporate into its cloud service agreements, there are some legal restrictions on the limitation of liability in a cloud computing services contract.

Under Part IIIA of the Consumer Protection Act ("CPA") (which came into force on 1 February 2011), certain provisions of a consumer contract which are substantively unfair would be unenforceable or void ("Unfair Contracts Law"). A term would be deemed substantively unfair if, for instance, it excludes or restricts liability for negligence, or excludes or restricts liability for breach of express or implied terms of the contract without adequate justification (Section 24D(1), CPA).

International standards are favoured over domestic standards in the country as Malaysia prioritises compliance with international standards. While Malaysia is not party to the UN Convention on Electronic

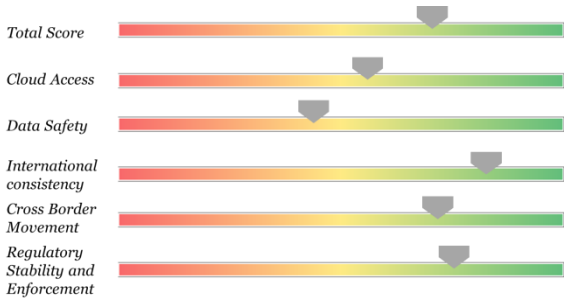
Contracting, the Electronic Commerce Act 2006 closely mirrors the UN Convention on Electronic Contracting. Malaysia became an observer to the WTO plurilateral Agreement on Government Procurement in July 2012. In addition, Malaysia is also a member of APEC. The PDPA is very similar to the principles in the EU Directive, with some variations that appear to adopt parts of the APEC Privacy Framework.

Malaysia is expected to follow OECD guidance in the treaty context for a PE taxable nexus regarding people. Cloud computing usage in Malaysia is also subjected to GST.

## 2.7.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Personal Data Protection Act 2010 ('PDPA 2010')** | Personal data | Contains principles that relate to consent, notice and choice, disclosure, security, retention, data integrity and access. | A data user shall not transfer any personal data outside Malaysia unless to such place as specified by the Minister, by notification published in the Gazette or one of the exceptions apply. |
| **Electronic Commerce Act 2006** | Commercial transactions | Contains principles that relate to commercial transactions through the use of electronic means and other matters. | This act is the key source of electronic commerce regulation for the private sector, which closely mirrors the UN Convention on Electronic Contracting. However, Malaysia is not party to the abovementioned UN Convention. |
| **Communications and Multimedia Act** | Online speech | Empowers the Commission with broad authority to regulate online speech. | Empowers the Commission with broad authority to regulate online speech, providing that "no content applications service provider or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person". |

# 2.8. New Zealand




According to a report by Frost & Sullivan, around 40% of companies within New Zealand are using cloud services and an increasing trend is observed. Local, regional, and global cloud service providers are well represented and used by New Zealand businesses. However, the New Zealand government has introduced a cloud-first strategy which supports onshore productivity cloud. In the future, this may expand to offshore cloud in certain circumstances.

Some of the concerns inhibiting cloud adoption, identified during the data gathering, include data privacy, residency and loss of control. While there are no incentives encouraging cloud adoption, some of the top criteria for selecting a cloud provider in New Zealand are security, reliability and support, as well as hosting capabilities in New Zealand.

## 2.8.1. Details on factors affecting cloud computing

**Regulatory environment**

The Privacy Act 1993 (the Act) is the legislation in New Zealand that regulates the collection, storage, correction, use and disclosure of personal information by agencies. These agencies are defined to include both public and private section persons with some exclusion such as members of Parliament, courts and individuals who hold personal information for their own person, family or household affairs.

The key obligations on agencies in respect of personal information are contained in the 12 Information Privacy Principles (IPPs) from section 6 of the Privacy Act. The IPPs include requirements for how and when personal information can be collected, stored, used or disclosed by an agency and individuals' rights of access and correction. The Government has recently agreed with a recommendation that the Act be replaced by a new Privacy Act made by the Law Commission after a recent review of the Act. Therefore, there are likely to be significant privacy law reforms in the future.

New Zealand defines personal information as any piece of information that relates to an identifiable human being such as their names, contact details, financial health and purchase records.

### 2.8.1.1. Cloud access

While New Zealand has no regulations that govern specifically cloud computing, the New Zealand Cloud Computing Code of Practice – a voluntary code of practice – was introduced in 2012. The Code covers issues such as security and disclosure statements. It does not place participating parties under any legal obligations. While the Privacy Commissioner recognizes leveraging the cloud can enhance privacy, the Code of Practice has had limited traction to date.

While not directly related to the use of cloud computing, the Reserve Bank, as part of its prudential supervisory function, has an outsourcing policy which requires large or systemically important financial institutions, in complying with their conditions of registration, to control and execute any outsourced functions with a view to ensuring that the financial institution has the ability to continue to provide core liquidity, payment and transaction services in the event that one of its service providers fails or becomes dysfunctional, or if the bank itself fails. Any specific outsourcing restrictions contained in the relevant financial institution's conditions of registration would need to be considered, and perhaps revisited, as part of an institution's cloud assessment.

### 2.8.1.2. Data safety

Under Information Privacy Principles (IPP) 9, an agency must not keep personal information longer than is required for the purposes for which the information may lawfully be used. There is no express requirement for the deletion of data after a specific time period, but the requirements of IPP 9 would likely

require data to be deleted or removed when it is no longer required for lawful purposes. While the IPPs contain principles governing the storage and usage of personal information, they will not override other statutory requirements requiring certain data to be retained for minimum periods (e.g., Health (Retention of Health Information) Regulations 1996, Tax Administration Act 1994 and the Goods and Services Tax Act 1985).

In normal circumstances (i.e. other than in declared states of emergency), data could only be accessed by NZ law enforcement agencies pursuant to a valid search warrant or a production order, or in certain urgent and extreme situations (e.g. to preserve material relating to an offence punishable by at least 14 years' imprisonment, in particularly urgent cases of suspected espionage, imminent danger to life or safety, etc.).

The Telecommunications (Interception Capability) Act 2004 requires network operators to assist government agencies to carry out surveillance pursuant to a valid interception warrant or where otherwise authorised by law. It is anticipated this will be repealed and replaced by the Telecommunications Interception Capability Bill (TICS Bill) in late 2013. To the extent that a cloud service provider were a "network operator" under that Act (which includes, for example, where a provider provides a public data network, e.g. for internet access by the public), it is required to have the technical capability to intercept communications on its network. The duty to provide assistance will only arise where the provider is shown a copy of a valid interception warrant or other evidence of the relevant agency's authority to carry out interception activities (e.g. under the New Zealand Security Intelligence Service Act 1969, the Government Communications Security Bureau Act 2003, the International Terrorism (Emergency Powers) Act 1987, or the Search and Surveillance Act 2012).

The TICS Bill does not change the circumstances in which data may be accessed by law enforcement agencies in New Zealand. That access question is addressed in separate legislation. The TICS Bill governs the extent of pre-investment that network operators and service providers must make in interception capability so that if there is a valid law enforcement request, granted pursuant to the checks and balances in the authorising legislation, then the network operator or service provider will be able to assist as required by the TICS Bill.

Under the Search and Surveillance Act 2012, warrants can be issued for remote access searches (section 111) where the issuing officer is satisfied that an offence punishable by imprisonment has been or will be committed and that there are reasonable grounds to believe that evidential material relating to the offence will be found in the specified place or thing (section 6).

Persons who have how-to knowledge of a data storage device subject to a warrant have a duty to assist the person exercising the search to gain access to the device or system (section 130).

The Government Communications Security Bureau Act 2003, amended in August 2013 by the Government Communications Security Bureau Amendment Act, allows the authorisation of access to a computer system of a specified foreign organisation where necessary to maintain New Zealand national security (sections 7 and 19). Similar powers also exist under the New Zealand Security Intelligence Service Act 1969, where a foreign intelligence warrant can be issued authorising a person to intercept or seize any communication or document where necessary for the detection of activities prejudicial to security or for gathering foreign intelligence information essential to security (section 4A).

The Government can also endow Police with broad powers to take control of any apparatus, implement, or equipment where necessary for the purpose of dealing with an international terrorist emergency under the International Terrorism (Emergency Powers) Act 1987 (section 6 and 10). This is likely to encompass access to data storage systems if the need should arise.

The Privacy Act can have some extraterritorial effect in respect of data processing activities that are performed outside New Zealand by an agency that is subject to the laws of New Zealand, if that data has been transferred by the agency from New Zealand (and would therefore have originally been subject to the Privacy Act).

If a foreign country / regulator obtained judgment in a New Zealand court, or had a foreign judgment enforced in New Zealand, then in most cases that judgement would be enforceable against a cloud provider based in New Zealand.

### 2.8.1.3. International consistency

The Office of the Privacy Commissioner (Commissioner) is an effective agency which educates the public, advises the government, conducts investigations and handles complaints. Under section 46 of the Act, the Commissioner may also issue Codes of Practice that may modify and override the application of the IPPs for certain industries.

Laws tend to be fairly and consistently applied in New Zealand. There are penalties enforced for non-compliance under the Privacy Act. The Commissioner will typically pursue conciliation and mediation first to resolve privacy complaints. Obstruction, giving false or misleading information, failing to comply with the lawful requirements of the Commissioner or any other person under this Act, and false representation of authority holding are summary offences, punishable by a fine of NZ$2,000 (section 127). Similarly, failing to produce records and documents in a timely manner may constitute a failure to comply with the lawful requirements of the Privacy Commissioner, or otherwise obstructing or hindering the Privacy Commissioner, and these activities could result in penalties. .Cross border movement

While there are no general prohibitions on international transfers of data, the Inland Revenue Department (IRD) requires that certain business records, relating to a person's tax affairs, be stored within New Zealand, unless an exemption has been granted. An exemption can be granted to a particular taxpayer, or to a third party (such as a cloud provider) who stores records on behalf of multiple NZ taxpayers. The IRD has stated that it is their practice to authorize offshore storage provided that it does not impede the IRD's compliance activities.

Part 11A of the Privacy Act 1994 empowers the New Zealand Privacy Commissioner to prohibit the onward transfer of personal information received in New Zealand from overseas if the onward transfer country does not offer comparable safeguards to New Zealand's Privacy Act. This power is intended to avoid New Zealand being used as a conduit to avoid other countries' privacy laws. It will not be relevant to a typical cloud services engagement for a New Zealand-based customer where the personal information is first collected in New Zealand... There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information.

Although there are no specific restrictions on exports of data, the customer (or other organisation responsible for Privacy Act compliance) will remain responsible for ensuring that personal information is kept securely, and the security given to more sensitive types of data in certain destination countries will need to be assessed on a case by case basis.

### 2.8.1.4. Regulatory stability & enforcement

In the absence of specific regulation, organisations are generally free to adopt / offer new products and services, subject to compliance with existing generic laws and regulation.

In New Zealand, new laws are typically introduced in a transparent manner with public input. A bill is publicly available after its introduction. Introduction is an administrative process that is later announced in the House. A bill that does not go through that administrative process has no formal existence.

The Anti-Money Laundering (AML) laws in New Zealand apply to reporting entities, which are defined as including financial institutions, and casinos, unless specifically excluded by regulation. Therefore, unless the cloud computing system provides some sort of special functionality that brings it within the definition of a financial institution, the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 is unlikely to apply to providers of cloud computing services.

The Consumer Guarantees Act creates statutory guarantees that are provided by suppliers of goods and/or services to consumers. These include guarantees as to reasonable care and skill, fitness for particular purpose, time of completion, and price. Liability under the Consumer Guarantees Act cannot legally be excluded, except in business to business transactions. Most business to business contracts will therefore

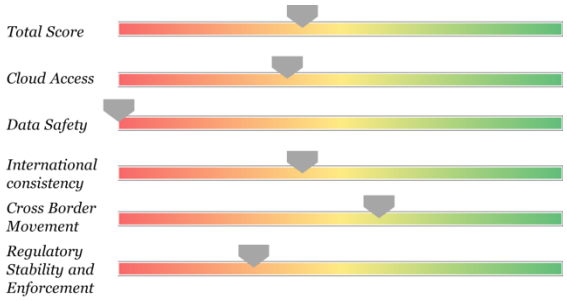
record that the customer is not acting as a consumer, and that the Consumer Guarantees Act does not apply.

## 2.8.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **The Privacy Act 1993** | Personal data | Contains principles governing the collection, storage, correction, use and disclosure of personal information by both public and private sector persons. | Under IPP 5 (see section 6 of the Privacy Act), agencies that hold personal information are required to ensure that such information is protected by 'such security safeguards as it is reasonable in the circumstances to take' against loss, unauthorised access, use, modification and disclosure or other misuse. |

# 2.9. Philippines

According to an IT infrastructure company executive, the adoption rate of cloud technology is only around 11-15%. The adoption rate is what countries like Singapore or Australia would have had a few years ago, signalling potential headroom for growth.




Some of the concerns that have been inhibiting cloud adoption are data security, state of telecommunications infrastructure, and nationality restrictions on provision of value-added services.

## 2.9.1. Details on factors affecting cloud computing

**Regulatory Environment**

Where no specific law or regulation on cloud computing is applicable, general laws on data processing and data services would apply, such as, the Data Privacy Act and E-Commerce Act. General provisions of the Civil Code on human relations and contracts that govern all types of transactions, would also apply.

The Anti-Money Laundering (AML) Act requires all records of all transactions of covered institutions to "be maintained and safely stored for five years from the dates of the transactions. Covered institutions generally include banks, insurance companies, and securities companies.

Existing laws and regulations do not prescribe a specific security and audit protocol, procedure, or requirement for hosting digital data. The Data Privacy Act ("DPA"), however, generally requires personal information controllers to observe personal information processing principles and implement reasonable and appropriate organizational, physical and technical measures to protect personal information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing. While there is no specifically prescribed protocol or procedure for data security audits, the DPA requires the appointment of a privacy officer who will ensure the organization's compliance with the DPA. Also, since the DPA's implementing rules and the National Privacy Commission have yet to be established, these requirements may still change.

### 2.9.1.1. Cloud access

The Philippines does not have any regulations specifically governing cloud computing. However, cloud services may be subject to regulation by the National Telecommunications Commission ("NTC") as a value-added service.

While there are no laws giving specific tax benefits to encourage cloud adoption. , there are also no tax benefits encourage other technology resources which can discourage adoption.

### 2.9.1.2. Data safety

The Philippine's' law recognizes a citizen's constitutional right to privacy of communication and correspondence. Unauthorized access to data communications is illegal except upon lawful order of the court or when public safety or order requires otherwise. Data or any evidence obtained in violation of this right is inadmissible for any purpose or in any proceeding.

Under the Cybercrime Prevention Act, law enforcement authorities, with due cause, can collect or record traffic data associated with specific communications transmitted by means of a computer system, even without a warrant. Traffic data refers only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities. All other data to be collected or seized or disclosed will require a court warrant. Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The Anti-Wiretapping Law allows court-authorised police recording of communication or spoken word in cases involving crimes against national security, public order and kidnapping. The Human Security Law allows court-authorised police surveillance of telecommunications messages to or from suspected terrorists. Operators are expected not to unjustifiably refuse such types of interceptions. Both laws require the recordings to be deposited with the authorising court.

### 2.9.1.3. International consistency

The Data Privacy Act applies to entities which, although not found or established in the Philippines, use equipment that are located in the Philippines, and, those that maintain an office, branch, or agency in the Philippines. Even if the entities do not have equipment or offices here, the law provides for extra-territorial application where the act or processing (which includes collection and disclosure) relates to personal information about a Philippine citizen or resident, or the entity processing personal information has a "link" in the Philippines. There is no specific definition as to what the "link" is, but based on the law, this could be carrying out businesses in the Philippines, or having a contract with a Philippine person or entity.

### 2.9.1.4. Cross border movement

While there are no restrictions on specific countries based on data types transferred, the Presidential Decree No. 1718 generally prohibits the taking, sending, or removal from Philippine territory of documents and information related to any business carried on in the Philippines, unless such constitutes regular practice, relates to business transactions, is required to comply with an international agreement to which the Philippines is a party, or is pursuant to an authority granted by the designated representative of the President. However, in practice this lacks an effective enforcement mechanism.

Chapter VI (Accountability for Transfer of Personal Information) of the Data Privacy Act of 2012 sets out principles for the transfer of personal information. Firstly, each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. Secondly, the personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. Lastly, the personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

While there are no additional requirements for foreign Cloud service providers (compared to local ones) under existing laws and regulations, foreign Cloud service providers, if they solicit contracts from local residents or engage in business in the Philippines, would have to establish a legal presence in the Philippines..

### 2.9.1.5. Regulatory stability & enforcement

New laws are typically introduced in a transparent manner with public input as the Philippine Congress conducts hearings and debates on proposed bills that are open to the public.

The Corporation Code contains principles on the establishment and operations of stock and non-stock corporations, which includes the requirement on every corporation to keep at its principal office a record of all business transactions and minutes of all meetings of stockholders or members, or of the board of directors or trustees. Foreign companies doing business in the Philippines must establish a local presence.

The Central Bank regulations require banks to have business continuity and contingency planning, and have the ability to deliver e-banking services to all end-users and be able to maintain such availability in all circumstances (e.g., 24/7 availability). A business continuity planning process and manual, with a section on electronic banking channels and systems, is required of banks that provide electronic banking services. A bank intending to outsource information technology systems and processes is also required to submit the proposed contract between the bank and the service provider, which must provide for disaster recovery/business continuity contingency plans and procedures.

While there are no legal terms and conditions that a cloud computing service provider is required or recommended to incorporate into its cloud service agreements, if the agreement includes the assignment or licensing of intellectual property rights, such as software, the agreement may be considered as "technology transfer arrangements". In such a case, the Intellectual Property Code requires the agreement to include certain mandatory provisions and exclude certain prohibited clauses.

The Data Privacy Act allows a personal information controller to subcontract the processing of personal information: "provided, that the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information." The outsourcing of the operation of information technology systems for banks requires prior regulatory approval.

The Manual of Regulation for Banks require the prior approval of the Monetary Board for a bank to outsource "all information technology systems and processes except for certain functions affecting the ability of the bank to ensure the fit of technology services deployed to meet its strategic and business objectives and to comply with all pertinent banking laws and regulations." Banks may "enter into outsourcing contracts only with service providers with demonstrable technical and financial capability commensurate to the services to be rendered." Banks may outsource, among others, (1) data imaging, storage, retrieval and other related systems; (2) offsite records storage services, and; (3) back-up and data recovery operations.

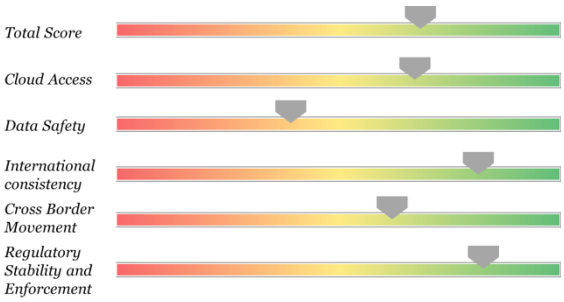
The provision of cloud computing services to local residents requires the provider to obtain a license to do business in the Philippines from the Securities and Exchange Commission (SEC) and register with the National Telecommunications Commission (NTC) as a value-added services provider.

## 2.9.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Data Privacy Act of 2012** | Personal information | Contains principles governing the processing (including collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data) of personal information. | Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. |
| **E-Commerce Act** | Electronic data | Providing for the recognition and use of electronic commercial and non -commercial transactions and documents, penalties for unlawful use thereof and for other purposes. | Service providers are obliged to abide by the rules and regulations as stated in Section 30 - Extent of Liability of a Service Provider. |
| **Presidential Decree No. 1718** | Documents and information | Contains principles regarding taking, sending, or removal of documents and information from The Philippines. | Generally prohibits the taking, sending, or removal from Philippine territory of documents and information related to any business carried on in the Philippines, unless such constitutes regular practice, relates to business transactions, is required to comply with an international agreement to which the Philippines is a party, or is pursuant |

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| | | | to an authority granted by the designated representative of the President. |
| **Cybercrime Prevention Act** | Internet traffic data and subscriber information | Contains principles to address legal issues concerning online interactions and the Internet in the Philippines | Law enforcement authorities, with due cause, can collect or record traffic data associated with specific communications transmitted by means of a computer system, even without a warrant.<br><br>Requires "the integrity of traffic data and subscriber information relating to communication services provided by a service provider" to be preserved for a minimum period of six months from the date of the transaction. |

# 2.10. Singapore




Singapore is a strong proponent of cloud computing. The Infocomm Development Authority of Singapore is investing in cloud providers and developing cloud standards to encourage adoption. Local, regional, and global cloud service providers are well represented and used by Singapore businesses. To encourage adoption of technologies including cloud computing, the government offers Productivity and Innovation Credit (PIC) Scheme as an incentive. Cloud computing is not widespread within the financial services industry due to Monetary Authority of Singapore regulations and guidelines.

In 2012, Singapore passed comprehensive Data Protection legislation, the Personal Data Protection Act (PDPA). This law took effect January 2013; however, enforcement will not start until after 12-18 month sunrise period for the various components. Under the law, cloud providers may be considered data intermediaries. As such, they are responsible for a subset of the requirements. Data transfers require appropriate contractual clauses to be in-place.

Singapore has a stable legal environment based on common law. Laws are typically introduced for public comment prior to enactment. There are no specific rules or laws pertaining to the usage of cloud computing. In addition, there is no legal bias towards local cloud computing companies.

## 2.10.1. Details on factors affecting cloud computing

**International implications**

Singapore is an active member of global initiatives including WTO TBT Code of Good Practice for the Preparation, Adoption and Application of Standards, UN Convention on Electronic Contracting, 18 regional and bilateral Free Trade Agreements with 24 trading partners, and APEC Cross Border Privacy Rules and APEC Cross-border Privacy Enforcement Arrangement.

### 2.10.1.1. Cloud access

Singapore recently passed comprehensive Data Protection legislation covering all types of personal data. The Personal Data Protection Act (PDPA) covers key principles including consent, access, disclosure, security, and transfer. The PDPA will typically apply to cloud providers as “data intermediaries” who will need to comply with a subset of the law. Relevant portions include the data protection and retention requirements. In addition, cloud providers may be required to amend or delete data as requested by the data controller to satisfy requests from data owners. In addition to the PDPA, data stored in Singapore is required to comply with 160 disparate, sector specific statutes that regulate the use and disclosure of data management in Singapore including in relation to consumer protection laws, employment laws, ecommerce, telecommunication and sector specific laws in healthcare, banking and insurance.

In legal proceedings, computer output is subject to the Evidence Act of Singapore which specifies protections required for admissibility of data. In addition, Section 199 of the Companies Act, Section 67 of the Income Tax Act, and Section 46 of the Goods and Services Tax Act which require various documents and records to be retained for seven years. Section 96 of the Employment Act also requires employer must keep records pertaining to payments made to each employee.

Cloud computing is not defined in any broad legislation and there are no laws or rules specific to cloud computing usage or providers. However, there may be other legislation which invariably impacts such services. For example, pursuant to Section 20 of the Second Schedule of the Broadcasting Act (Cap. 28) (‘Broadcasting Act’), “computer on-line services”, which arguably covers cloud computing services, is a licensable broadcasting service. As such, it is more likely than not that cloud computing service providers will be viewed as an Internet Content Provider (‘ICP’) pursuant to the Broadcasting (Class License)

Notification ('Notification') issued pursuant to the Broadcasting Act and will be required to comply with the Notification where applicable as well as the Internet Code of Practice.

There are no prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data in general. The MAS Technology Risk Management Guidelines (MAS TRMG) requires financial institutions to protect "Sensitive data". This includes information, such as customer data, computer files, records, object programs, source codes, passwords, authentication credentials, payment card data etc. For government agencies, the Government IM8 would apply.

Singapore currently offers an incentive for productivity improvements; which can include the usage of cloud computing. This offers companies a 400% tax deduction for up to the first $400,000 spent.

### 2.10.1.2. Data safety

The PDPA has a potential extraterritorial effect since it applies not only to personal data in Singapore, but companies that have personal data on Singaporeans. In addition, foreign judgments from superior courts of law of gazette countries may be registered in Singapore to be enforced. This applies to only those jurisdictions that have been registered under RECJA or REFJA.

Singapore law grants wide reaching powers of investigation to compel the disclosure of data including encrypted data to government bodies and law enforcement agencies for the purpose of criminal enquiries as well as when there is a matter of national security or public interest at issue. Outside of PDPA a warrant is typically required for investigations; however, the Computer Misuse (Amendment) Act (CMA) provides for exemptions.

Overseas governments or authorities are not allowed to access data that is hosted within Singapore territories.

### 2.10.1.3. International consistency

The effective regulator in Singapore is the Personal Data Protection Commission which can investigate complaints and enforce penalties and remediation programs. Generally, laws tend to be fairly and consistently applied to both local and international companies. PDPA is the first overarching law addressing data protection in Singapore. However, it is planned for the main data protection rules to come into force in 2014.

There are several key acts and legislations in Singapore. While individual regulators may overlap, this does not cause an undue burden on companies in general.

### 2.10.1.4. Cross border movement

The PDPA is very flexible on data transfers outside of Singapore. Not only is there no requirement to register, the PDPA does not specify a prescriptive approach for transferring data to countries with an adequate level of data protection. Instead, the PDPA adopts a "principle-based" approach, where the organization in Singapore has to put in place measures to ensure a comparable standard of protection over the personal data transferred overseas which can often be achieved through contractual arrangements. It should be noted, consent is required from the data owner prior to transfer unless it is obvious.

Singapore is an open market with non-discriminatory practices. Singapore is a member of the WTO plurilateral Agreement on Government Procurement, which includes rules guaranteeing fair and non-discriminatory conditions of international competition. In addition, Singapore is party to a number of Free Trade Agreements which provide additional market access concessions.

### 2.10.1.5. Regulatory stability & enforcement

Although there are no specific laws / regulations rafted for cloud computing in Singapore, the Government has been pro-actively supporting the adoption and promoting growth of cloud computing in Singapore.

New regulations in Singapore typically go through a 60 day public notice period prior to initial reading in parliament.

There are no specific security requirements or certifications required for cloud providers. However, Singapore is publishing a new Cloud Security Standard that will be optional for cloud providers to adopt. In addition, cloud providers may fall within the definition of Internet Content Providers (ICPs). As such, they may be subject to regulation by the Media Development Authority (MDA).

The PDPA provides for criminal and civil penalties for non-compliance. Enforcement comes from the Personal Data Protection Commission which can investigate complaints and enforce penalties and remediation programs. At this point, only compliant-based investigations are foreseen. While PDPA is not currently enforced, other laws tend to be fairly and consistently enforced by regulators. This applies to both local and foreign companies.

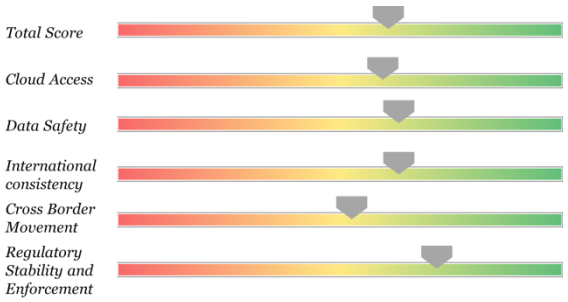
Contracting tends to follow standard practices. There are no legal terms and conditions that a cloud computing service provider is required or recommended to incorporate into its cloud service agreements. There are no legal restrictions on the exclusion of warranties (both statutory implied warranties and express warranties) in a cloud computing services contract. However, under the Unfair Contract Terms Act (Cap. 396) ('UCTA'), limitation of liability clauses in cloud computing contracts are either rendered wholly ineffective, or are ineffective unless shown to satisfy the requirement of reasonableness.

There are no taxes specific to cloud computing in Singapore; general tax principles apply. Guidance from Singapore Tax Authorities on e-commerce transactions indicates that mere presence of server in Singapore is not sufficient determine if income is taxable in Singapore. The business model and extent of operations should also be examined before determining tax liabilities. Hosting a transactional website on a server located in Singapore will result in Singapore income tax liability if the hosting arrangements amount to "substantial business activities" which create a source of income in Singapore. What constitutes "substantial business activities" is decided on a case – to –case basis. Payments for cloud computing are subject to GST if there is a Singapore affiliate or the principle has a branch / agency in Singapore.

## 2.10.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Personal Data Protection Act (PDPA)** | Data protection | Covers key principles including consent, access, disclosure, security, and transfer. | The PDPA requires consent from individuals prior to transferring their data. The type of consent is relative to the usage of the data and how "apparent" it is for the data provider. In addition, the receiving party must protect in-line with PDPA requirements. This can be done through binding corporate rules, written contracts and other mechanisms. |
| **Computer Misuse Act** | Computer security | The Act was updated in 2013 to require organizations to comply with directives to prevent or mitigate a cyber-attack from occurring. | Must be able to respond to requests from the Minister of Home Affairs. Failure to comply is a criminal offense. The government has extensive powers under the Internal Security Act and other acts to monitor anything that is considered a threat to "national security." |
| **Evidence Act of Singapore** | Forensics | In legal proceedings, computer output is subject to the Evidence Act of Singapore which specifies protections required for admissibility of data. | Presumption of reliability and accuracy of records means a wider variety of computer records are admissible. |

# 2.11. South Korea




Gartner has calculated the value of the public cloud services market in Korea in 2011 to be US$1.59 billion. This is a 23% increase from 2010 and ranks Korea 9 (out of 20 countries) in the forecast. Gartner has projected the five-year compound annual growth rate (CAGR) to 2016 to be 15.6% and this ranks Korea 13 (out of 20 countries) for growth in the value of the market for public cloud services to 2016.

Two of the main concerns that have been inhibiting cloud adoption are security and trust.

In South Korea, the Personal Information Protection Act ("PIPA") regulates the general collection, use and processing of personal information in both the public and private sectors. Collection of customer's personal information via online methods and overseas transfer of such information is governed by the Act on Promotion of Information and Communication Network Utilization and Information Protection ("Network Act").

## 2.11.1. Details on factors affecting cloud computing

**Regulatory environment**

There are currently no specific laws and regulations that govern cloud computing. However, the Korea Communications Commission ("KCC") announced the proposed Act on Cloud Computing Promotion and User Protection (the "Proposed Act") on July 10, 2012, which aims to comprehensively regulate cloud computing service providers. Although the language of the Proposed Act has not been finalized, draft language was made available in late summer 2012.

### 2.11.1.1. Cloud access

Among other requirements, the Proposed Act requires cloud computing service providers to comply with reporting requirements, notification to users and consent for transfer of information to third parties outside the scope of the service. In addition, the collection and use of personal information (as well as transferring such information to third parties) requires compliance with the privacy related laws of Korea, (PIPA, the Network Act and the Credit Information Act). Among other things, the privacy related laws require specific notice and consent and technical security measures.

The Proposed Act prohibits the provision of information to third parties without user consent (except when there are special provisions provided in other laws). Based on the relevant authority's interpretation of other existing laws, we anticipate third parties will likely include affiliates. On the contrary, there are no prohibitions on the use of cloud computing services in relation to particular functions or types of data. However, in practice, it is difficult for financial institutions to transfer data overseas, and therefore may be restricted from using cloud computing services.

The Use and Protection of Credit Information Act govern specifically the finance sector while the Network Act regulate the telecommunications and IT service providers.

From December 4, 2012, foreign direct investment (FDI) in high-tech businesses and related services has been granted corporate, income and acquisition tax incentives. Such investment will obtain a tax exemption from those taxes for the first five years, and a 50% reduction for the two years thereafter. The revision includes offers of incentives for FDI in an additional new technologies, such as cloud computing.

### 2.11.1.2. Data safety

In principle, a warrant is required when accessing data pursuant to a recent court decision which held a portal site civilly liable for providing a certain user's information to the police without valid warrant. However, in certain dawn raid type situations, the investigative authority may request that the company 'voluntarily' submit the data relevant to the particular investigation.

The Communications Secrecy Act prohibits the surveillance or "tapping" of any communications which are in the course of being transmitted. However, for certain types of crimes listed under the Communication Secrecy Act, these measures can be allowed by the relevant court under exceptional circumstances.

If information collected from South Korean users is stored overseas, even by a Foreign Service provider, such service would be sufficient to subject the Foreign Service provider to the laws and regulations of South Korea. According to Article 6 of the Criminal Code, criminal sanctions shall apply to aliens who commit crimes against South Korea or South Korean nationals outside the territory of Korea provided that the country where the crime was committed also constitute such acts as a crime.

#### 2.11.1.3. International consistency

Korea is a member of the WTO plurilateral Agreement on Government Procurement (GPA), which includes rules guaranteeing fair and non-discriminatory conditions of international competition. These rules cover most large contracts.

Before the PIPA, there are several personal data protection laws under different industry sector. Since 2011, the PIPA absorbed and unified all related laws, which means the law applied fairly and consistently.

Currently, it is contemplated that the KCC will play the primary enforcement role, in conjunction with the police and prosecutor's office in the case of criminal enforcement. However, the competent authority has been changed to the MSIP. The MSIP has broad authority to investigate any incident involving cloud computing service providers within the scope of the Proposed Act.

The KCC will continue to be the competent authority in the case of any incidents involving the leakage of personal information under the Network Act. The KCC has the authority to impose administrative sanctions and penalties, and can further recommend further criminal investigation to the prosecutor's office upon the conclusion of its own investigation. There are also penalties imposed in case of non-compliance as stated in Electronic Financial Transaction Act

#### 2.11.1.4. Cross border movement

General data has been not allowed to transfer outside of Korea under Electronic Financial Transaction Act. Though recently some of IT facilities and services are allowed to locate/to outsource outside of South Korea, financial transaction data still are not allowed. In addition to Electronic Financial Transaction Act, there are several laws for transfer of data outside of the jurisdiction and differences exist among these laws according to types of data and owner.

Article 25 of the Proposed Act prohibits the provision of information to 3rd parties, unless consent is obtained and Article 27 of the Proposed Act requires the service provider to disclose when information is stored overseas. Similar to the Proposed Act, the PIPA allows the transfer of personal data outside of Korea through obtaining consent from the individuals. Under PIPA, if the personal information were transferred to an overseas 3rd party, the following items must be disclosed and prior user's consent must be obtained: identity and country of the third party to which the personal information is to be provided; purpose behind the use of the personal information by the third party; specific items of personal information to be provided; time period of retention and use by the third party; and right to refuse and any disadvantages from refusal.

Under the Network Act, if the personal information were transferred to an overseas entity, some items must be disclosed prior to user's consent. These items include the specific information to be transferred overseas; the destination country; the date, time and method of transmission; the name of the transferee and the contact information of the person in charge of the personal information within the transferee; and the purpose of use of the personal information by the transferee and the period of retention and usage.

The transferor must also take certain protective measures to protect the personal information, and establish procedures to resolve users' claims. Further, these matters should be reflected in the agreement, etc. entered into between the transferor and the overseas transferee.

While there is no "mandatory data transfer agreement", Article 17 (3) of PIPA provides that overseas information transfer agreements cannot violate the articles of PIPA. Also, while there is no registration requirement with the authorities, Proposed Act states that all cloud computing service providers are required to file a report to the relevant authority under Article 14, regardless of whether domestic or overseas data transfers are involved.

### 2.11.1.5. Regulatory stability & enforcement

While there may be areas not specifically covered by any laws / regulations, the regulations of PIPA generally applies to all areas or services. Before the PIPA, there are several personal data protection laws under different industry sector. Since 2011, the PIPA has absorbed and unified all related laws, implying the fairly and consistently application of the regulation.

The Proposed Act has gone through public notice and comment procedures and the Korea Communications Commission (KCC) has received and considered public opinion as it currently revises the language of the Proposed Act.

While the Proposed Act generally encourages mutual interoperability of computing systems, it does not prescribe certain products, services, standards or technologies. However, PIPA provides for certain standards relating to the encryption for storage of unique identifying information, passwords and biometric information which have been collected from offline sources. Similarly, the Network Act has encryption standards specified for various types of information.

Article 23 of the Proposed Act requires the cloud computing service provider to report serious service disruptions or leakage to users, and depending on the scale of the incident, to the relevant authority without delay. Article 31 of the Proposed Act also addresses unexpected instances of business suspension and requires service providers to obtain guarantee insurance and temporary administration ability for any unexpected service outages.

The Network Act and PIPA also require similar notification requirements to the affected individuals and KCC and/or Minister of Public Administration and Security (MOPAS) in the case of leakage of personal information. In addition, the Network Act requires delegation arrangements to be notified and consented to by the users. Under PIPA, delegation does not require specific consent, but must be notified to the users and the service provider and principal company must have a written delegation agreement in place containing certain details.

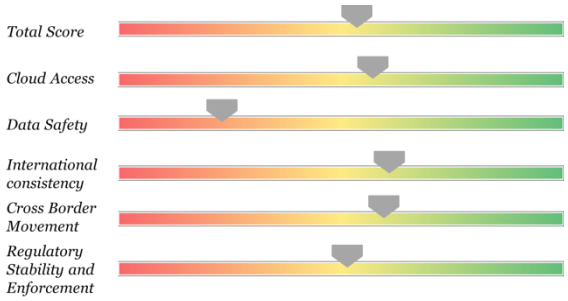
Article 22 of the Proposed Act contemplates the use of a standardized contract to be developed by cloud computing service provider groups, with prior review by the relevant authorities. Article 25 of the Proposed Act prohibits the provision of information to 3rd parties, unless consent is obtained. In addition, in the case of personal information, the privacy laws distinguish delegation arrangements from 3rd party provision, with different requirements for each. The specific details of the "subcontracting arrangement" must be reviewed in order to determine whether it would constitute a delegation or third party provision in order to provide the specific requirements under the laws.

Article 32 of the Proposed Act provides that users who have sustained damages from the cloud computing service provider may demand compensation for damages, and if not resolved, may submit the dispute to the relevant authority. It is possible that the court and/or relevant authority may deem provisions which excessively limit liability of the cloud computing service provider void, according to the Standardized Contract Regulations Act (SCRA).

## 2.11.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Personal Information Protection Act ("PIPA")** | Personal data | Contains principles regulating the general collection, use and processing of personal information in both the public and private sectors | For delegation of processing, PIPA requires that a written outsourcing agreement be in place containing the details of the arrangement such as delegated work scope, restriction on sub-delegation, security measures for protection of personal information, damage compensation in case delegate breaches its duties, etc.<br><br>Personal information may be retained until the stated period or the purpose has been fulfilled, whichever occurs earlier, at which time, the personal information must be irrevocably deleted or destroyed without delay.<br><br>Requires the cloud computing service provider to report serious service disruptions or leakage to users, and depending on the scale of the incident, to the relevant authority without delay. |
| **Act on Cloud Computing Promotion and User Protection (the "Proposed Act")** | Cloud computing | Contains principles regulating cloud providers such as requiring them to comply with reporting requirements, notification to users and consent for transfer of information to third parties outside the scope of the service. | Prohibits the provision of information to 3rd parties without user consent (except when there are special provisions provided in other laws).<br><br>Requires the cloud computing service provider to report serious service disruptions or leakage to users, and depending on the scale of the incident, to the relevant authority without delay.<br><br>Requires service providers to obtain guarantee insurance and temporary administration ability for any unexpected service outages.<br><br>Contemplates the use of a standardized contract to be developed by cloud computing service provider groups, with prior review by the relevant authorities.<br><br>Provides that users who have sustained damages from the cloud computing service provider may demand compensation for damages, and if not resolved, may submit the dispute to the relevant authority.<br><br>Any amendment to important portions of the report must be reported to the relevant authority. |

# 2.12. Taiwan




The ACCA Index shows that Taiwan is one of the top five (5) countries in Asia that is ready for cloud computing adoption due to its excellent connectivity and freedom of information. Taiwan is vigorously accelerating its efforts to be a critical supplier in the global cloud computing industry. "Taiwan Cloud Valley", initiated and promoted by Cloud Computing Association in Taiwan (TWCLOUD), aims to cluster Taiwan's complete supply chain and functions as a window of Taiwan and international cloud computing suppliers.

Also, tax incentives are available under the new Statute for Industry Innovation (SII), enterprises may claim up to 15% of their R&D expenditures as a credit to offset against their corporate income tax payable in the current year only, with a maximum credit of 30% of the tax payable.

However, under the Company Act, foreign companies are required to establish a local branch or a subsidiary if it intends to conduct business in Taiwan.

## 2.12.1. Details on factors affecting cloud computing

**Regulatory environment**

Personal Data Protection Act (PDPA) covers the protection of personal data. Set forth below is the key principles of the PDPA:

1. Adequate Notice in Advance: To comply with the PDPA, the data subject must be provided with adequate notice before the business entity first collects personal data from him/her.

2. Specific Business Purpose: The collection and processing of personal data must be for specific purpose(s) and meet one of the conditions listed in the PDPA.

3. Termination or Deletion of the Personal Data: A business entity should, on its own initiative or upon a data subject's request, delete or stop processing or using the data collected when the originally intended purpose no longer exists, unless a business entity has to keep the personal data to fulfil its legal obligation or it is otherwise agreed to by the data subject in writing.

4. Proper Security Measures: Article 27 of The PDPA requires that any business entity keeping personal data files should adopt proper security measures to prevent them from being stolen, altered, damaged, destroyed or disclosed.

### 2.12.1.1. Cloud access

While Taiwan has no specific law or regulation that governs cloud computing, they have the Personal Data Protection Act (PDPA) that covers the protection of personal data. Some key principles of the PDPA are: providing adequate notice in advance for collection of data; having a specific business purpose for that data; providing procedures in place for the termination or deletion of the personal data; and having proper security measures in place.

### 2.12.1.2. Data safety

Taiwan law grants wide reaching powers of investigation to compel the disclosure of data including encrypted data to government bodies and law enforcement agencies for the purpose of criminal enquiries as well as when there is a matter of national security or public interest at issue. The Communications Protection and Surveillance Act allows official authorities to intercept/ access or conduct surveillance on data under certain conditions. The Communications Protection and Surveillance Act also provides exceptions where warrants are not necessary.

The Communications Protection and Surveillance Act, which came into effect in Taiwan on July 16, 1999, provides that the monitoring of communications may only be implemented when it is deemed necessary to protect national security or to maintain social order. Warrants for such surveillance may only be issued if the content of the communications is related to a threat to national security or to the maintenance of social order. Furthermore, the crime in question must be a serious one. In principle, the period for which surveillance is implemented should not exceed 30 days. These restrictions reflect the government's determination to ensure that citizens' right to privacy is protected.

Generally a final and binding civil judgment rendered by a foreign court would be recognised in Taiwan if the requirements set forth in the Civil Procedure Code are met. In addition, the PDPA has an extraterritorial effect.

### 2.12.1.3. International consistency

With regards to personal data, the Ministry of Justice (MOJ) has been the primary regulator of PDPA and it is in charge of all matters in relation to the PDPA. The competent authorities for each industrial sectors are authorized under the PDPA to enforce certain matters, such as conducting on-site check on non-public organs, imposes penalties on non-public organs that do not comply with PDPA, issue order restricting international transfer of personal data, etc., for the their respective industry sectors. In general, laws tend to be fairly and consistently applied to local and international companies. There are no laws and regulations governing cloud computing services yet as there are no competent authorities taking in charge of computing service matters.

### 2.12.1.4. Cross border movement

While there are no regulations on international transfer and storage of general data, Article 24 of the PDPA provides that the competent authority may prohibit a business entity's international transmission of personal data if (A) it will prejudice any material national interest, (B) it is prohibited or restricted under an international treaty or agreement, (C) the country to which the personal data is to be transmitted does not afford sound legal protection of personal data, thereby affecting the rights or interest of the data subject(s), or (D) the purpose of transmitting personal data is to evade restrictions prescribed under the PDPA. As of today, only the National Communications Commission, Taiwan's communications and media regulator, has imposed a directive on telecom and media operators to prohibit them from conducting international transmission of personal data to the PRC.

With regard to personal data, if the data subject has entered into a contract or is preparing to enter into a contract with the business entity, and such an international data transfer is within the purpose of performing the contract, then his/her consent is not required. As for the circumstance that the consent is required, the consent should either be in a written form or be in accordance with the requirement under the Electronic Signatures Act. In addition, insurance companies would be required to obtain customer's consent for its offshore outsourcing activities.

There is no mandatory data transfer agreement required for the transfer of data to an overseas location. Also, registration for data controllers sending data overseas is not required.

### 2.12.1.5. Regulatory stability & enforcement

The PDPA imposes penalties in case of non-compliances. Failure to comply with the PDPA subjects the infringing party to civil liabilities, administrative penalties and criminal liabilities. Also, the application of the laws tends to be consistent. New laws in Taiwan are also typically introduced in a transparent manner with public input.

While there are no legal terms and conditions that a cloud computing service provider is required or recommended to incorporate into its cloud service agreements, Article 8 of the Enforcement Rules of the PDPA set forth certain guidance on subcontracting arrangements.

Taiwan has no specific legal restrictions on the exclusion of warranties (both statutory implied warranties and express warranties) in a cloud computing services contract. Also, there are no specific laws governing

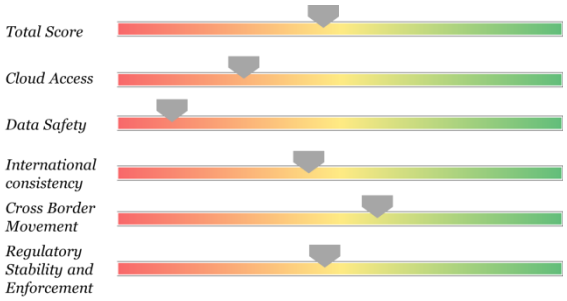
restrictions on the limitation of liability in a cloud computing services contract. The general principles in the Civil Code and other regulation, such as Consumer Protection Act, if applicable, shall govern.

Cloud providers are likely to be considered Internet service providers under Taiwan law. Such being the case, cloud providers may be exempt from obligations of filtering content provided that certain conditions under the respective legislation are met.

## 2.12.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Personal Data Protection Act (PDPA)** | Personal data | Contains principles governing the collection, processing, usage and storage of data. | The competent authority may prohibit a business entity's international transmission of personal data if (A) it will prejudice any material national interest, (B) it is prohibited or restricted under an international treaty or agreement, (C) the country to which the personal data is to be transmitted does not afford sound legal protection of personal data, thereby affecting the rights or interest of the data subject(s), or (D) the purpose of transmitting personal data is to evade restrictions. |
| **Electronic Signatures Act** | Electronic transactions | Contains principles governing the use and security of electronic transactions, and facilitate the development of electronic government and commerce. | As for the circumstance that the consent is required, the consent should either be in a written form or be in accordance with the requirement under the Electronic Signatures Act. |

# 2.13. Thailand




At present, Thailand does not have any general statutory law governing data protection or privacy. Principles of data protection and privacy law are embodied in the existing general laws (e.g., the Constitution of the Kingdom of Thailand, Civil and Commercial Code, Penal Code and other specific laws such as Financial Institution Business Act or the Operation of Telecommunications Business Act ("TBA"). Having no privacy laws is a major weakness for Thailand as privacy laws provides underlying principles to any possible cloud computing regulations.

While there was an initiative to launch Thailand Government Cloud in May 2012 by the Electronic government Agency (EGA) and another by Software Park, a government agency under the National Science and Technology Development Agency, to encourage local software companies to go on cloud and innovate local cloud platform, concerns that hinder adoption of cloud services still exist. These concerns include data privacy, residency, or 'loss of control'; cost; and availability or performance.

## 2.13.1. Details on factors affecting cloud computing

**Regulatory environment**

The conduct of cloud computing services is likely to be considered as the conduct of telecommunications and/or internet service provider business, which requires the provider to obtain the relevant telecommunications and/or internet service provider licence under the TBA. The telecommunications and/or internet service provider will be required to comply with the obligations and requirements under the TBA. Therefore, the TBA contains the general regulations governing the cloud computing services in Thailand.

### 2.13.1.1. Cloud access

As cloud computing services is likely to be considered as the conduct of telecommunications and/or internet service provider business, the provider would be required to obtain the relevant telecommunications and/or internet service provider licence under the TBA. The telecommunications and/or internet service provider will be required to comply with the obligations and requirements under the TBA. The TBA requires the telecommunications and internet service provider to protect personal data. In addition, the Financial Institutions Act requires financial institutions to protect sensitive data.

While there is no specific regulation governing cloud computing, there are also no prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data in general.

Various laws and regulations specify some data storage requirements for corporate records. These include Section 14 of the Accounting Act, Section 87/3 of the Revenue Code and Section 115 of the Labour Protection Act.

### 2.13.1.2. Data safety

While a warrant is required prior to accessing data held or transmitted by data hosting providers, carriers or other service providers, the Computer Crime Act provides some exceptions. Thai law grants wide reaching powers of investigation to compel the disclosure of data including encrypted data to government bodies and law enforcement agencies for the purpose of criminal enquiries as well as when there is a matter of national security or public interest at issue.

The Computer Crime Act, the Electronic Transactions Act and the TBA have provisions that allow official authorities to intercept/ access or conduct surveillance on data.

Although Thai criminal laws can be applied to persons both inside and outside of Thailand, if the person/entity is not present in Thailand, these laws cannot be enforced against them. In addition, a final judgment of any court of competent jurisdiction outside Thailand would not itself be automatically enforced in Thailand as a new legal proceeding in Thailand is required and such judgment would be admissible only as evidence in such Thai proceedings in Thailand.

### 2.13.1.3. International consistency

Currently, since Thailand has no specific law regulating data protection or privacy, there is no principal regulator responsible for the enforcement of regulations for data storage and transfer. However, regarding the telecommunications business, the TBA grants authority to the National Broadcasting and Telecommunications Commission (NBTC) to investigate relevant complaints and to enforce penalties against the offender e.g. through a fine, suspension or revocation of the licence.

Although it is possible that order or direction of regulators may overlap, it is unlikely to cause an undue burden on companies. Generally, laws tend to be fairly and consistently applied in Thailand although there is no system of binding precedence in Thailand.

### 2.13.1.4. Cross border movement

While there is no restriction for storage/transfer of general data outside of Thailand, specific businesses such as telecommunications or internet service providers have requirements, including personal data protection by the licensed business operator, under the TBA. The TBA also requires the business operator to obtain an individual's consent before his personal data is transferred to an overseas location.

Though regulations tend to be consistently applied to local and international companies, there are some additional requirements that apply to foreign companies or companies which have foreigners as majority shareholders such as the requirement to obtain a Foreign Business License (FBL) prior to commencing certain types of businesses in which foreign participation restrictions exist.

### 2.13.1.5. Regulatory stability & enforcement

While there is no general security audit requirement for hosting digital data in Thailand, the NBTC has the authority to specify the security and audit requirements as an attachment to the telecommunications licence and/or internet service provider licence. The relevant material obligations of the licensed telecommunications provider and internet service provider will also be provided by NBTC in the attachments of the telecommunications provider and internet service provider licence.

The telecommunications licence and internet service provider licence would also require the licensed business operator (i.e. cloud computing service provider) to comply with the NBTC's requirements regarding disaster recovery and business continuity.

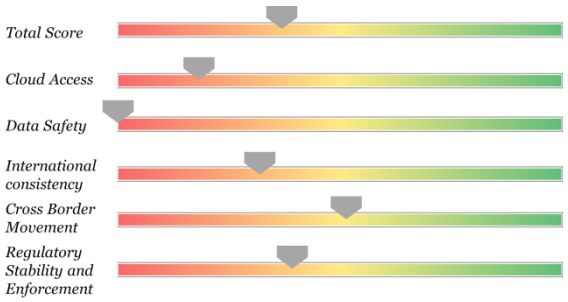
In addition, the TBA generally requires the holder of telecommunications and internet service provider licence to prepare the network security plan as the minimum requirement specified in the relevant licence. The TBA also grants authority to the NBTC to investigate relevant complaints and to enforce penalties against the offender (e.g., through a fine, suspension or revocation of the licence).

The TBA requires the relevant service contract between the telecommunications or internet service provider and its customer to have minimum legal terms and conditions as set out in the standard form provided by the NBTC. The service provider is also required to submit its contract to the NBTC for approval prior to using the contract with its customer. In additional, the Unfair Contract Terms Act provides that any provisions in an agreement (including the exclusion of warranties) which give one party inappropriate advantage over the other party may be regarded by the Courts of Thailand as unfair provisions and may result in such court ordering that only the provisions that are fair and appropriate are enforceable.

## 2.13.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Telecommunications Business Act ("TBA")** | Personal data | Contains principles pertaining to personal data, right of privacy and freedom to communicate by means of telecommunication. | Requires the business operator to obtain an individual's consent before his personal data is transferred to an overseas location. However, there is no specific form of consent required.<br><br>Requires the relevant service contract between the telecommunications or internet service provider and its customer to have minimum legal terms and conditions as set out in the standard form provided by the NBTC. |
| **Personal Information Protection Act ("Draft")** | Personal data | Contains principles providing protection for personal data by restricting the gathering, using, disclosing and altering of any personal data. | The Personal Information Protection Act ("Draft") is being reviewed and analysed to include practical issues on applying the law and how the Data Protection Committee should be formed.<br><br>The Draft is being reviewed by the Office of the Public Sector Development Commission and will subsequently be submitted to the Cabinet for approval |

# 2.14. Vietnam




While Vietnam continues to develop relevant cyber laws that will enhance confidence in the digital economy and facilitate cloud computing, gaps still exist in key areas. Modern laws are in place for electronic commerce, electronic signatures, and intellectual property but only very limited laws are in place for cybercrime and privacy, and these would require significant expansion to align Vietnam with international models.

Though Vietnam does not have comprehensive privacy legislation, it does have a short privacy section in its Law on E-Transactions 2005 that could serve as a foundation for more detailed legislation in the future.

## 2.14.1. Details on factors affecting cloud computing

**Regulatory environment**

Organizations and individuals shall be responsible to ensure the safety of the information infrastructure under their management. Accordingly, collection, use, transfer, storage, etc. of data must comply with the rules stipulated in the Regulations on applying standards and technical specifications for data centres.

In Vietnam, there is no unified regulation clearly classifies types of data to be protected. However, data relating to certain issues/matters shall be regulated and protected under relevant specific regulations.

### 2.14.1.1. Cloud access

Vietnam does not have comprehensive privacy legislation, but it does have a short privacy section in its Law on E-Transactions 2005. Article 46 of the law covers information confidentiality in e-transactions while Articles 21 and 22 of the Law on Information Technology stipulates that more detailed regulations regarding information protection in the environment such as regulations on collection, process, use, storage, and provision of personal information, may be developed in the future.

Other than the E-Transactions and Information Technology laws, the Law on Telecommunications, Law on Intellectual Property, Law on Publishing and the Press Law contain varying principles around data protection and privacy.

In addition, Article 12 of Law on Information and Technology states that the supplying, exchanging, transmitting, storing or using digital information for the following purposes shall be prohibited: opposing the State; exciting violence, propagating wars of aggression; revealing state secrets, military, security, economic, external relation or other secrets; distorting, slandering; advertising for or propagating goods or services banned by law.

### 2.14.1.2. Data safety

Article 20 of the Law on Information Technology states that competent state agencies shall monitor and supervise digital information; investigate law violations committed in the course of transmitting or storing digital information.

Under the Law on National Security, the state agency in charge of the protection of national security has the right to examine communication equipment or computers and computer networks and materials of individuals and organizations if there is any reasonable suspicion of a breach of national security. It is therefore very likely that this security agency shall have the right to access all information, including encrypted data, in case of a suspected violation of national security. In addition, Decree 55 and Decision 71 require Internet service suppliers to arrange necessary technical and material facilities for the relevant state authorities to take measures to protect national security as well as to protect information and network security.

The Law on National Security provides that any foreign individual who violates the national security of Vietnam outside the territory of Vietnam shall be penalized in accordance with the laws of Vietnam, if this is stipulated in an international treaty to which Vietnam has acceded or is a participant. According to Article 30.1 of the Civil Procedure Code, Vietnam recognises and enforces in Vietnam foreign courts' judgments or decision on business or commercial matters.

### 2.14.1.3. International consistency

Based on local laws and WTO commitments, laws of Vietnam tend to be consistently applied between local and international companies.

There is no dedicated privacy agency, although the Ministry of Information and Communications has broad responsibility for e-commerce law and regulation.

### 2.14.1.4. Cross border movement

Article 12 of Law on Information Technology and Article 10 of the Law on Media state that the supply, exchange, transmitting, storage or usage of digital information outside of Vietnam for the following purposes shall be prohibited: opposing the State; exciting violence, propagating wars of aggression; revealing state secrets, military, security, economic, external relation or other secrets; distorting, slandering; advertising for or propagating goods or services banned by law.

According to Articles 21.1 and 21.2 of the Law on Information Technology, organisations and individuals collecting, processing and using personal information of another person in the network environment must obtain consent from such person, unless otherwise stipulated by law. The consent form must be in writing or data messages. They shall also have the responsibilities to ensure such information to be secure and confidential.

### 2.14.1.5. Regulatory stability & enforcement

The permissibility, adoption for areas/services which are not specifically governed by any laws or regulations shall be subject to the sole discretion of the authorities of Vietnam.

While there are no laws or regulations similar to Sarbanes-Oxley Act in Vietnam, companies are subject to the specific control requirements stipulated in various laws (e.g., Law on enterprise, Law on accounting, etc.). Article 7.1 of the Prevention of Money Laundering Law, the collection, storage, transfer, access or retention of data for the purpose of creating conditions to carry out the act of money laundering shall be considered as a prohibited act.

In 2009 the Vietnam Minister of Information and Communications announced that it was mandatory that 100% of clients of IT divisions of government agencies must be installed with open source software while a lower limit of 70% applied to non-IT agencies. The announcement by the Minister includes mandatory requirements for the selection of open source software.

The material obligations of cloud computing service providers are stipulated in the Regulations (Circular 03/2013/TT-BTTTT) on applying standards and technical specifications for data centres.

Article 41 of the Law on Information Technology states that organisations and individuals that transmit digital information of other organizations and individuals shall be liable for the contents of that information under the following circumstances: they themselves start the transmission of information; they select recipients of transmitted information; and they select and modify the contents of transmitted information.

According to Article 302 of the Civil Code, limitation of liability shall be applied under the circumstances of force majeure event and proof that failure to perform the obligations is due entirely to the faults of the other party of the service contract.

According to Article 41 of Law on information technology and Circular 03/2013/TT-BTTTT, cloud computing services shall obtain or comply with (i) the Standardization and quality control in information

technology application and development activities and (ii) the rules stipulated in the Regulations on applying standards and technical specifications for data centres.

## 2.14.2. Summary of key regulations affecting cloud computing

| Law / Regulation | Area | Summary | Impact |
|---|---|---|---|
| **Law on E-Transactions 2005** | Electronic transactions | Contains principles regulating electronic transactions and information involved in the transactions. | Vietnam does not have comprehensive privacy legislation, but it does have a short privacy section in its Law on E-Transactions 2005 that could serve as a foundation for more detailed legislation in the future. |
| **Law on Information Technology** | General data | Contains principles governing the collection, use, transfer, storage, etc. of data. | Competent state agencies shall monitor and supervise digital information; investigate law violations committed in the course of transmitting or storing digital information. |
| **Civil Code** | Personal information | Contains the legal standards for the rights and obligations of subjects regarding personal identities, and property in business, trade, labor relations and other related areas | There is no unified regulation that clearly classifies types of data to be protected. Personal data is mainly regulated by the Civil Code.<br><br>Foreign courts' judgments or decision on business or commercial matters is recognized.<br><br>Limitation of liability shall be applied under these circumstances: (1) Force majeure event; and (2) Proof that failure to perform obligations is due entirely to the faults of other parties. |
| **Ordinance on Protection of State's Secret** | State/ Government data | Contains specifics of the task of protecting the State secrets; which mean information in the fields of external affairs, economy, science, technology and other fields that are sensitive and confidential to the country. | While personal information is regulated by the Civil Code, Data relating to State/Government shall be regulated by the Ordinance on Protection of State's Secret |

# 3. Conclusion

No country completely meets the ideal country definition. While some are close, none achieved more than 80% of the possible points. Every country has room for improvement to address the deficiencies identified. Ultimately, knowing the weaknesses allow organizations to better plan and insights will help move closer to achieving the ideal.

## 3.1. Current challenges and opportunities

**Opportunities: Stable regulatory enforcement, and Incentives**

On a positive note, most countries are reasonably stable when it comes to regulatory enforcement. The legal environment is predictable, and laws are fairly and consistently enforced for both local and foreign companies. Additionally, most countries are aligned with some form of international regulations. International standards are general favoured over domestic standards, and many countries are party to international agreements such as the UN Convention on electronic contracting, WTO, APEC, EU and others regional privacy and data protection frameworks. All countries' scores on regulatory stability range from 57% - 85%.

As per the case with all businesses, the attraction to enter the market is driven largely by potential profits. Some countries such as South Korea, Singapore, Taiwan and India do offer some form of incentive and/or tax exemption to encourage growth in the cloud computing industry. While not all financial assistance directly correlate with the cloud computing industry; as some are focused on other areas such as R&D and IT, Cloud service providers should take the opportunity to be one of the pioneers in the industry within the region, and gain competitive advantage via these vehicles.

**The biggest hurdle: Data safety**

Across Asia, it is observed that one of the key challenges in promoting cloud computing as an industry is the data safety. Specific pain points for most countries are: (1) data access and security, and (2) the lack of clarity with regard to regulations restricting access of data flowing across borders.

The findings gathered for fundamental data safety areas; particularly on regulatory matters, are among the areas that require further attention by the local regulators and international bodies alike. Regulations on areas such as warrants, data access by law enforcement authorities and overseas governments, data surveillance, extraterritorial effect, law enforcement in a foreign country, and customs monitoring are not clear as to extraterritorial reach to data stored or processed in the cloud. Countries such as Vietnam, Indonesia, India, Philippines, Thailand and Taiwan scored the lowest on data safety.

## 3.2. Practical solutions and approaches

### 3.2.1. General

#### 3.2.1.1. Collaboration with regulators

With the technology landscape evolving quickly, regulators may obtain useful information from cloud users and providers as they develop regulations or guidelines. Cloud users and providers should work to educate one another on regulatory compliance issues, and with regulators with regard to the impact of potential regulations on cloud adoption; exploring alternative ways of achieving the same objectives without the unintended consequence of generally impairing cloud adoption in their country.

#### 3.2.1.2. Formation of regional agreements to facilitate data transfer

One of the greatest concerns for users interested in adopting cloud services is the challenge of meeting legal requirements across multiple jurisdictions. With the pace of regulation, it appears that there has been

little focus on aligning regulations from jurisdiction to jurisdiction. Inconsistent regulations between jurisdictions add complexity to cloud computing. Regional agreements like the APEC framework can facilitate transfer of information between jurisdictions in consistent manner. Such a regional approach could remove much of the uncertainty faced by organizations interested in leveraging cloud services.

#### 3.2.1.3. Leveraging technical solutions

There are several aspects to achieving regulatory goals that should be considered where business practices and technology intersect. Governments can achieve their goals with regard to cloud computing most efficiently if they consider the business models and practices, and technical infrastructure associated with cloud computing. When organizations understand the intent behind regulations, they can explore with regulators how the government objectives could be met in alternative ways. One approach being used to satisfy regulatory requirements to protect data privacy is the encryption of data being sent to or stored with a cloud provider. With this method, data is encrypted with an encryption key controlled by the cloud user. Consequently, only the encrypted data is stored and processed by the cloud provider. While this may not address all regulatory concerns, it effectively ensures the control of, and access to, data remains within jurisdictional boundaries and is an example of a verifiable technical solution to a regulatory objective.

#### 3.2.1.4. Approach for cross border movements

Most data protection and privacy legislation restricts the movement of personal data to locations with equivalents protections. While certain countries have succeeded in obtaining reciprocal recognition of their regulatory environment, this is not widespread. As a result, cloud users and providers can pursue the following to facilitate cross border data movement:

- Binding corporate rules for processors: This is similar to the binding corporate rules that organizations may leverage for internal transfer. These are geared towards service providers like cloud providers to standardize transmission of information globally.

- Model contract clauses: Model contracts provide a simple mechanism for ensuring all concerns from the relevant data protection authorities are taken into account. They are only effective if they are leveraged in whole without any modifications. In addition, they are not available from every jurisdiction.

- Customised contract clauses: Without an umbrella mechanism providing for equivalent protection, cloud users and providers will need to agree on contractual clauses individually. This increases effort required by both parties and introduces challenges with the standard contracts used by many cloud providers.

### 3.2.2. Country Specific Recommendations

Based on the scorecard results, there are specific areas each country should address to bring them closer to the "ideal". We highlight a few for each country below. A careful review of our country analysis may reveal other issues which should be addressed in each country, as well.

#### 3.2.2.1. Australia

**Set up a transparent mechanism for data access:** Acts such as the Telecommunications (Interception and Access) Act 1978 can be amended to further promote data safety in cloud computing. A transparent mechanism can be achieved via the establishment of fundamental controls such as the issuance of warrants, and the ability for Cloud service providers to challenge the request for data access.

#### 3.2.2.2. China

- Regulation of data privacy should be addressed at the federal level and in a manner consistent with globally accepted regulatory norms. For example, currently Jiangsu and Shenzhen have either already passed or going to pass ordinances that prohibiting the transfer of personal data out

of the provinces without explicit legal authorization or regulatory approval. China may look to Hong Kong, which set up the Office of the Privacy Commissioner for Personal Data (PCPD) to manage the Personal Data (Privacy) Ordinance. In addition, China should clearly articulate what data categories are subject to cross border movement restrictions and prohibitions.

- China should also consider reviewing its practice in the following areas to move towards the "ideal":
    - The enactment of data privacy laws and regulations that are consistent with globally accepted standards and norms.
    - Removal of country specific certifications or standards requirements.
    - Aligning restrictions or prohibitions on cross border data movement with global norms and clarifying the classifications of data subject to restriction.
    - Laws to be fairly and consistently applied to local and international companies.
    - The establishment of a transparent mechanism for obtaining access to data via warrant or similar process and ability for Cloud service providers to challenge the request.
    - Removal of tariffs or trade barriers on downloading digital data from foreign Cloud service providers.

#### 3.2.2.3. Hong Kong

- **Enhance the current data access mechanism:** While the Interception of Communications and Surveillance Ordinance regulates the interception of communications by authorities, a more transparent mechanism can be achieved via the specification of detailed clauses in the ordinance to enable Cloud service providers to challenge the authorities' request for data access.

#### 3.2.2.4. India

- **Information Technology Act to be more supportive of cloud computing:** India should consider the cloud computing implications in the Information Technology Act, 2000. Several requirements that are currently included in the act are rather onerous and can be costly if legal proceedings are involved, for example, providers of sensitive information are currently required to verify the given information, and Cloud service providers can be held liable for the illegal data they may be hosting.

- India should also consider reviewing its practice in the following areas to move towards the "ideal":
    - The enactment of data privacy laws and regulations that comply with globally accepted standards and best practices.
    - Clearly define the classifications of data subject to government restriction.
    - The establishment of a national data protection authority.
    - Removal of country specific certifications or standards required.

#### 3.2.2.5. Indonesia

- **Newly defined Regulation 82 to consider cloud computing:** Indonesia should take into account the cloud computing perspective while formulating the Government Regulation 82 on the operation of electronic systems and transactions. Some key requirements of the Regulation 82 include registration of service providers, certification of software and locating data center and

disaster recovery center within the country, which will significantly determine the future of cloud computing industry in Indonesia as a whole.

- Indonesia should also consider reviewing its practice in the following areas to move towards the "ideal":
    - Loosen data residency policies such that information collected can be store overseas in an encrypted format.
    - The establishment of a transparent mechanism for obtaining access to data via warrant or similar process and ability for Cloud service providers to challenge the request.
    - Clearly defined liabilities on cloud service providers.
    - Laws to be fairly and consistently applied to local and international companies.
    - Overlapping regulations on cloud computing to be minimised and to be brought under single distinct authority.

### 3.2.2.6. Japan

- **Enhance the current data access mechanism:** Existing laws like the Act on Wiretapping for Criminal Investigation (Act No. 137 of 1999) currently allows the investigative authorities to intercept communications with a warrant to the extent necessary to investigate serious organized crimes such as drug crimes, crimes using firearms, etc**.** A more transparent mechanism can be achieved via the specification of detailed clauses in the ordinance to enable Cloud service providers to challenge the authorities' request for data access.

- Japan should also consider reviewing its practice in the following areas to move towards the "ideal":
    - Provision of incentives to be provided by government for companies to adopt cloud computing.

### 3.2.2.7. Malaysia

- **Enhance the current data access mechanism:** A more transparent mechanism can be achieved via the specification of detailed clauses in relevant regulations to enable Cloud service providers to challenge the authorities' request for data access given the necessary circumstances. These requirements can be included as potential amendments to the recently passed Personal Data Protection Act. Malaysia should increase the transparency around the PDPA to reduce uncertainty around the implementation.

- Malaysia should also consider reviewing its practice in the following areas to move towards the "ideal":
    - Laws to be introduced in a more transparent manner with public input.

### 3.2.2.8. New Zealand

- **Government-driven enforcement of regulation:** While it is an impressive progress in the country's cloud computing industry, the currently in place NZ Cloud Code is a code of practice that has been developed by the Institute of IT Professionals (formerly the NZ Computer Society) covering issues such as security and disclosure statements. It is a strictly voluntary code, not mandated by Government, and has had limited traction to date. Restrictions on export of data included and disclosure requirements in the voluntary cloud code of practise should be aligned with globally accepted standards.

### 3.2.2.9. Philippines

- **Set up a transparent mechanism for data access:** The Philippines should consider establishing a transparent mechanism for obtaining access to data, via warrant or similar process, and ability for Cloud service providers to challenge the request. Current requirements as stated in the Cybercrime Prevention Act allows law enforcement authorities, with due cause, can collect or record traffic data associated with specific communications transmitted by means of a computer system, even without a warrant.

- The Philippines should also consider reviewing its practice in the following areas to move towards the "ideal":

    - To define regulations on data storage requirements for corporate records.

    - To participate more in regional privacy/data protection framework.

    - Laws to be fairly and consistently applied to local and international companies.

    - Restrictions that prohibit foreign service providers from providing services in country to be relaxed.

    - Rules that apply to subcontracting arrangements under a cloud computing services contract should comport with globally accepted standards.

### 3.2.2.10. Singapore

- **Set up a transparent mechanism for data access:** Singapore should consider establishing a transparent mechanism for obtaining access to data, via warrant or similar process, and ability for Cloud service providers to challenge the request. Singapore law can compel the disclosure of data including encrypted data to government bodies and law enforcement agencies for the purpose of criminal enquiries as well as when there is a matter of national security or public interest at issue. While a warrant is typically required for investigations; however, the Computer Misuse (Amendment) Act (CMA) provides for exemptions.

- Singapore should also consider reviewing its practice in the following areas to move towards the "ideal":

    - Penalties enforced for non-compliance of laws / regulations for data storage and transfer to comport with globally accepted standards.

### 3.2.2.11. South Korea

- **The "Proposed Act" to be more supportive of cloud computing:** South Korea's Act on Cloud Computing Promotion and User Protection (the "Proposed Act") has been seen to gather mixed reactions. Several elements of the Act have been questioned as they place unnecessary burdens on the industry thereby limiting adoption of cloud servicing and hindering international trade such as prohibiting the provision of information to 3rd parties without user consent, and requiring Cloud service providers to report serious service disruptions or leakage to users, and depending on the scale of the incident, to the relevant authority without delay.

- South Korea should also consider reviewing its practice in the following areas to move towards the "ideal":

    - Revise data residency policies such that information collected can be stored overseas in an encrypted format.

    - Restrictions on business continuity or disaster recovery regulations that could affect cloud computing to comport with globally accepted standards.

### 3.2.2.12. Taiwan

- **PDPA to be more supportive of cloud computing:** According to the PDPA of Taiwan, cross-border transfer of personal data constitutes an "international transmission". The National Communications Commission, Taiwan's communications and media regulator, has imposed a directive on telecom and media operators to prohibit them from conducting international transmission of personal data to China.

- Taiwan should also consider reviewing its practice in the following areas to move towards the "ideal":

    - The establishment of a transparent mechanism for obtaining access to data via warrant or similar process and ability for Cloud service providers to challenge the request.

    - Rules that apply to subcontracting arrangements under a cloud computing services contract to comport with globally accepted standards.

### 3.2.2.13. Thailand

- **Telecommunications Business Act to be more supportive of cloud computing:** The Telecommunications Business Act ("TBA") states requirements that may result in onerous operations for the Cloud service providers. For example, TBA requires the relevant service contract between the telecommunications or internet service provider and its customer to have minimum legal terms and conditions as set out in the standard form provided by the NBTC, as well as, requires the business operator to obtain an individual's consent before his personal data is transferred to an overseas location.

- Thailand should also consider reviewing its practice in the following areas to move towards the "ideal":

    - To enact data privacy laws that comport with globally accepted standards and norms.

    - Legal uncertainties on data protection and cross border movement to be clarified.

    - Removal of censorship or liability for content.

### 3.2.2.14. Vietnam

- **Develop a privacy legislation based on the existing Law on E-Transactions 2005:** Vietnam was among the countries without comprehensive privacy legislation; however, it does have a short privacy section in its Law on E-Transactions 2005 that could serve as a foundation for more detailed legislation in the future.

- Vietnam should also consider reviewing its practice in the following areas to move towards the "ideal":

    - Data privacy laws and material obligations on cloud computing service providers to comport with globally accepted standards and best practices should be properly enacted.

    - Prohibitions on use of cloud computing services to be revised to comport with globally accepted standards.

    - The establishment of a transparent mechanism for obtaining access to data via warrant or similar process and ability for Cloud service providers to challenge the request

    - Laws to be fairly and consistently applied to local and international companies.

# *Appendix – Scorecard factors*

The following table lists the questions asked and criteria for scoring. In addition, the columns at right contain the score weightings for each factor: A: Cloud Access, B: Data Safety, C: International Consistency, D: Cross Border Movement, E: Regulatory Stability and Enforcement

| **Question** | **Definition for grading scale (1, 2,3,4,5) for each answer** | **Weighting by sub category** | | | | |
|---|---|---|---|---|---|---|
| | | **A** | **B** | **C** | **D** | **E** |
| Background Questions | | | | | | |
| Rate of cloud adoption in the country (overall) (rate on a scale of 1-5) [1: no adoption 5:widely adopted] | Not scored | 0 | 0 | 0 | 0 | 0 |
| Rate of cloud adoption for Software as a Service (SaaS) in the country (rate on a scale of 1-5) [1: no adoption 5:widely adopted] | Not scored | 0 | 0 | 0 | 0 | 0 |
| Rate of cloud adoption for Infrastructure as a Service (IaaS) in the country (rate on a scale of 1-5) [1: no adoption 5:widely adopted] | Not scored | 0 | 0 | 0 | 0 | 0 |
| Rate of cloud adoption for Platform as a Service (PaaS) in the country (rate on a scale of 1-5) [1: no adoption 5:widely adopted] | Not scored | 0 | 0 | 0 | 0 | 0 |
| Geographic distribution of cloud services being consumed in the country | Not scored | 0 | 0 | 0 | 0 | 0 |
| What are the main barriers for a cloud computing service provider to provide services in this country? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Are there any incentives provided by government for companies to adopt cloud computing in the country? | 5 = if high incentives<br>3 = if moderate level of incentives<br>1 = if no | 2 | 0 | 0 | 0 | 0 |
| Local Laws and Regulations | | | | | | |
| Regulatory Environment | | | | | | |
| Are there laws or regulations governing data protection in the country (including collection, use, transfer, storage, etc. of data)? If so, what are the key requirements? | 5=There are general data protection laws but they are most likely not prohibitive for usage of cloud services<br>3= There are only personal data protection laws but they may not be prohibitive for usage of cloud services<br>1= There are no data protection laws or any law section on data protection | 0 | 0 | 3 | 0 | 0 |
| What types of data are regulated? | 5= Clearly defined definition of personal data<br>3= moderate / acceptable (typically just personal data)<br>1= uncertainty regarding types of data regulated or large amount of types included | 1 | 0 | 2 | 0 | 0 |
| Are there data protection requirements assigned to third parties (i.e., cloud provider) that processes data on behalf of the data controller? | 5=only requirements are through contractual relationships<br>3- liable but not as much as data controller<br>1 =liability not clearly defined | 0 | 0 | 2 | 2 | 0 |
| Are there any regulations that govern cloud computing in general? | 5=No prohibitions for operations of cloud service provider<br>3= If no regulations specifically for cloud computing but other related area regulations may apply | 2 | 0 | 2 | 0 | 0 |

| Question | Definition for grading scale (1, 2,3,4,5) for each answer | Weighting by sub category | | | | |
|---|---|---|---|---|---|---|
| | | A | B | C | D | E |
| | 1= Highly regulated environment with restrictions on normal cloud computing service usage | | | | | |
| Are there any prohibitions against the use of cloud computing services or the use of cloud computing services in relation to particular functions or in relation to any particular types of data (e.g., Human Resources, Intellectual Property, and finance)? | 5= No prohibitions for operations of cloud service provider<br>3= Certain prohibitions<br>1= Moderate prohibitions / restrictions on normal cloud computing service usage | 3 | 0 | 0 | 0 | 0 |
| Is the definition of cloud computing clearly and coherently defined in relevant laws/ regulations? | 5= compliance needs are not onerous, clearly defined, not subject to frequent change and does not require modifications to standard offerings<br>3 = compliance needs are moderate and reasonable<br>1 = ambiguous and falls under broadly defined service category | 0 | 0 | 2 | 0 | 2 |
| Are there any laws or regulations for specific industry sectors? If yes, please list the name of sectors. | 5=No prohibitions for operations of cloud service provider<br>3= Primarily one or two industries<br>1= Moderate prohibitions | 3 | 0 | 0 | 0 | 0 |
| How are areas/services not specifically governed by any laws / regulations treated by authorities in the country in terms of permissibility, adoption etc.? | 5= if flexible / allowed<br>3= if likely to be allowed because government is proactively supporting the area / services<br>1= very prohibitive | 0 | 0 | 3 | 0 | 1 |
| Are there any laws or regulations that specify data storage requirements for corporate records including location, format, retention period, etc.? | 5= Minimal restrictions<br>3= moderate level (data storage requirements for data other than personal data)<br>1= Unique / ad-hoc / restrictive requirements | 2 | 0 | 2 | 0 | 0 |
| Are new laws typically introduced in a transparent manner with public input? | 5= public consultation/other forms of stakeholder engagement regularly organized<br>3= no consultation but notice provided when new laws are introduced<br>1= no consultation/no advance notice given before introduced | 0 | 0 | 2 | 0 | 3 |
| Are companies subject to laws (i.e., Sarbanes-Oxley) that require specific controls to be in-place? | 5=No prohibitions for operations of cloud service provider<br>3= Moderate prohibitions<br>1= Highly regulated environment with restrictions on normal cloud computing service usage | 0 | 0 | 1 | 0 | 0 |
| Are there any Anti-Money Laundering (AML) laws that could affect cloud computing usage? If yes, are there any requirements in these Anti Money Laundering Laws that are related to collection, storage, transfer, access or retention of data? | 5=No prohibitions for operations of cloud service provider<br>3= Moderate prohibitions<br>1= Highly regulated environment with restrictions on normal cloud computing service usage | 0 | 0 | 2 | 0 | 0 |
| Security | | | | | | |
| Are cloud service providers subject to mandatory filtering or censoring of content? | 5=If no<br>1= if yes | 0 | 2 | 2 | 0 | 0 |
| Are there any specific security and audit requirements for hosting digital data in the country? | 5=No country specific technical requirements that would require changes to the standard product (no specific security and audit requirements)<br>3= moderate level technical restrictions that may require minimal changes to standard product (moderate coverage in legislation)<br>1= High level of restrictions requiring major changes or workarounds to standard product (detailed legislation) | 0 | 0 | 3 | 0 | 3 |
| Are any security related certifications or standards required before using certain technology products in the country? | 5=No country specific technical requirements that would require changes to the standard product<br>3= moderate level technical restrictions that may require minimal changes to | 0 | 0 | 3 | 0 | 0 |

| Question | Definition for grading scale (1, 2,3,4,5) for each answer | Weighting by sub category | | | | |
|---|---|---|---|---|---|---|
| | | A | B | C | D | E |
| | standard product<br>1= High level of restrictions requiring major changes or workarounds to standard product | | | | | |
| Are there any business continuity or disaster recovery regulations that could affect cloud computing. | 5=No country specific technical requirements that would require changes to the standard product<br>3= moderate level technical restrictions that may require minimal changes to standard product<br>1= High level of restrictions requiring major changes or workarounds to standard product | 0 | 0 | 2 | 0 | 0 |
| Cross Border Data Movement | | | | | | |
| Are there any prohibitions / conditions for storage/transfer of general data outside of this jurisdiction? | 5= if no or minimal restrictions<br>3= if moderate / reasonable level of restrictions<br>1=if highly prohibitive | 0 | 0 | 0 | 4 | 0 |
| Are there restrictions or prohibitions on the export of personal (sensitive or non-sensitive) data from your jurisdiction to an overseas location? | 5= if no or minimal restrictions<br>3= if moderate / reasonable level of restrictions<br>1=if highly prohibitive | 0 | 0 | 0 | 3 | 0 |
| Is consent from an individual required before data is transferred to an overseas location? If so, what form of consent is required? | 5=if no consent<br>3= implied consent<br>1=explicit consent | 0 | 0 | 0 | 5 | 0 |
| Is there a mandatory data transfer agreement required by the national regulator for the transfer of data to an overseas location? | 5= if no<br>1=may be used | 0 | 0 | 2 | 5 | 0 |
| Are data controllers sending personal information overseas required register themselves with official authorities? | 5= if no<br>1=yes | 0 | 0 | 1 | 4 | 0 |
| Is the destination country restricted based on the type of data sent overseas? | 5= if no<br>1=yes | 0 | 0 | 2 | 4 | 0 |
| Have any standard forms or precedents for data transfer agreements been approved by national authorities? | 5= present and help facilitate cross-border movement<br>3= not present but do not hinder cross-border movement<br>1= cross-border movement hindered | 0 | 0 | 0 | 1 | 0 |
| Enforcement environment | | | | | | |
| Is there an effective agency (or regulator) responsible for the enforcement of regulations for data storage and transfer? If so, what enforcement powers do they have? | 5= regulator enforces impartial and fair manner<br>1= regulator enforced impartially but without moderating frequency of enforcement | 0 | 0 | 0 | 0 | 4 |
| Are there penalties enforced for non-compliance of laws / regulations for data storage and transfer? | 5= if no penalties<br>3= if there are penalties but the amount is moderate<br>1= if penalty amount is significantly high | 0 | 0 | 0 | 0 | 2 |
| Are there penalties enforced if companies are unable to produce records and documents in a timely manner? | 5= if no penalties<br>1= if there are penalties but the amount is moderate | 0 | 0 | 0 | 0 | 3 |
| Are laws fairly and consistently applied? | 5= if laws are applied fairly in a consistent manner<br>3= if laws are usually applied fairly but laws subject to frequent changes or revision<br>1=if laws are not applied fairly or application is inconsistent and not transparent | 0 | 0 | 2 | 0 | 5 |
| Are companies using or providing cloud computing subject to overlapping regulations, inter-ministry turf wars, ministries with differing interpretations of regulations, etc.? | 5= if no overlapping regulations, cloud computing falls under a single distinct regulatory authority<br>3= if more than one regulators are involved but there is no conflict/ difference | 0 | 0 | 0 | 0 | 3 |

| Question | Definition for grading scale (1, 2,3,4,5) for each answer | Weighting by sub category | | | | |
|---|---|---|---|---|---|---|
| | | A | B | C | D | E |
| | of opinion among the different regulators<br>1= if multiple regulators involved and conflict/difference of opinion is prevalent between the different regulators | | | | | |
| Are regulations consistently applied to local and international companies? | 5= regulator enforces impartial and fair manner<br>3= regulator enforced impartially but without moderating frequency of enforcement<br>1= enforced to letter of law without flexibility without regard to legislative intent of law | 0 | 0 | 3 | 0 | 5 |
| Is a warrant required prior to access data held or transmitted by data hosting providers, carriers or other service providers when required? | 5= if yes, there is a transparent mechanism for obtaining access to data via warrant or similar process that is based on proper due diligence, users are notified of the request and they have the ability to challenge the request<br><br>3= if no warrant required but there are other forms of notification / processes to be followed before access to data can be granted, there is a transparent mechanism for obtaining access to data via warrant or similar process that is based on proper due diligence, users are notified of the request and they have the ability to challenge the request<br><br>1= if no warrant is required, users are not notified about access of their data | 0 | 5 | 0 | 0 | 0 |
| Can law enforcement authorities obtain access to encrypted data held or transmitted by data hosting providers, carriers or other service providers when required? | 5=if no<br>1= if yes | 0 | 4 | 0 | 0 | 0 |
| Are there any laws or regulations that allow official authorities to intercept/ access or conduct surveillance on data? | 5=if no<br>1= if yes | 0 | 5 | 0 | 0 | 1 |
| Do the local country regulations have an extraterritorial effect? | 5 = if no<br>1= if yes | 0 | 0 | 1 | 0 | 2 |
| Can action be enforced on a cloud provider in the country by a foreign country? | 5=if no<br>1= if yes | 0 | 2 | 0 | 0 | 4 |
| Ease of conducting operations | | | | | | |
| Are there any laws or policies that mandate the use of /specify a preference for certain products (including, but not limited to types of software), services, standards or technologies? | 5=No country specific technical requirements that would require changes to the standard product<br>3= moderate level technical restrictions that may require minimal changes to standard product<br>1= High level of restrictions requiring major changes or workarounds to standard product | 0 | 0 | 4 | 0 | 0 |
| Are there any laws/regulations that discriminate based on the nationality of the vendor, developer or service provider? | 5= if no discrimination between local and foreign service provider<br>3= if foreign Cloud service providers are free to provide service in country but subject to additional requirements / restrictions than local providers<br>1 = if restrictions that prohibit foreign service providers from providing services in country | 0 | 0 | 3 | 0 | 0 |
| Are foreign companies subject to any localization requirements (e.g. required to have a local presence, must offer local language solutions)? | 5= if no discrimination between local and foreign service provider<br>3= if foreign Cloud service providers are free to provide service in country but subject to additional requirements / restrictions than local providers<br>1 = if restrictions that prohibit foreign service providers from providing services in country | 0 | 0 | 5 | 0 | 0 |

| Question | Definition for grading scale (1, 2,3,4,5) for each answer | Weighting by sub category | | | | |
|---|---|---|---|---|---|---|
| | | A | B | C | D | E |
| Are there any specific material obligations on cloud computing service providers such as data retention obligations, data security standards, duties to notify of security breaches and duties to disclose processed data to regulators or law enforcement officials? | 5=No obligations impacting operations of cloud service provider and incentives available for cloud adoption<br>3= Moderate level of obligation<br>1= Highly material obligations for cloud service providers | 0 | 0 | 0 | 0 | 2 |
| Are foreign cloud service providers (Cloud service providers) subject to additional requirements compared to local Cloud service providers? | 5= if no discrimination between local and foreign service provider<br>3= if foreign Cloud service providers are free to provide service in country but subject to additional requirements / restrictions than local providers<br>1 = if restrictions that prohibit foreign service providers from providing services in country | 0 | 0 | 2 | 0 | 3 |
| Is the cloud provider held liable for illegal content? | 5= if no under any circumstance<br>3=if held liable if showing complacency in providing assistance<br>1= if yes | 0 | 4 | 0 | 0 | 4 |
| Contracting considerations | | | | | | |
| Are there any legal terms and conditions that a cloud computing service provider is required or recommended to incorporate into its cloud service agreements. | 5= if no or minimal rules exist<br>3 = if moderate rules exist<br>1 = if highly restrictive rules exist | 0 | 0 | 0 | 0 | 3 |
| Are there any rules or regulations which apply to subcontracting arrangements under a cloud computing services contract? | 5 = if no or minimal rules exist<br>3 = if certain rules exist<br>1 = if moderate rules exist | 0 | 0 | 0 | 0 | 4 |
| Are there any legal restrictions on the exclusion of warranties (both statutory implied warranties and express warranties) in a cloud computing services contract? | 5= if no restrictions on exclusion of warranties<br>3 = if moderate level of restrictions<br>1 = if high level of restrictions | 0 | 0 | 0 | 0 | 3 |
| Are there any legal restrictions on the limitation of liability in a cloud computing services contract? | 5 = if no restriction<br>1 = if moderate level of restrictions exist | 0 | 0 | 2 | 0 | 2 |
| Are there any licenses, consent, approval, consultation or notification processes (such as material outsourcing regulation) which may be applicable to cloud computing services? | 5 = if no restriction<br>3 = if moderate level of restrictions exist<br>1 = if high level of restrictions exist | 0 | 0 | 3 | 0 | 4 |
| International Perspective | | | | | | |
| Are international standards favoured over domestic standards in the country? | 5 = if there is active adoption of international standards<br>3 = if international standards considered when drafting domestic standards<br>1 = if domestic standards are favoured and bear little resemblance to international standards | 0 | 0 | 4 | 0 | 2 |
| Is the country party to UN Convention on Electronic Contracting? | 5 = if yes<br>1 = if no | 0 | 0 | 0 | 0 | 5 |
| Is data flowing over borders subject to customs monitoring? | 5 = if no<br>1 = if yes<br>(no differentiation) | 0 | 0 | 0 | 0 | 0 |
| Are any tariffs or trade barriers imposed when downloading of applications or digital data from foreign cloud service providers? | 5 = if no tariffs or trade barriers<br>3 = if there are either tariffs or trade barriers but not of a high value<br>1 = if both tariffs and trade barriers exist | 0 | 0 | 0 | 1 | 1 |
| Are there any bilateral/international agreements that may impact cloud computing services in your jurisdiction? | 5 = if yes (TRIPS + FTA which include cloud computing services)<br>1 = if TRIPS but no additional FTAs<br><br>(focus on agreements that will be facilitative for cloud computing e.g. TRIPS. Negative aspects - For e.g. access to data - MLATs will be covered in 3.7 ) | 0 | 0 | 2 | 0 | 3 |

| Question | Definition for grading scale (1, 2,3,4,5) for each answer | Weighting by sub category | | | | |
|---|---|---|---|---|---|---|
| | | A | B | C | D | E |
| Is country party to any international trade agreements that mandate access to cloud services | 5 = if yes<br>3 = if not yet but planning to<br>1 = if no | 1 | 0 | 0 | 0 | 0 |
| Are overseas governments or authorities entitled to access data stored on the cloud platform? | 5=if yes but with restrictions<br>1 = if yes | 0 | 2 | 2 | 0 | 0 |
| Is the country a member of the World Trade Organization (WTO)? | 5 = if yes<br>1 = if no | 0 | 0 | 0 | 0 | 1 |
| Is the country a member of any regional privacy / data protection frameworks (i.e., APEC, EU)? | 5 =aligned with multiple frameworks<br>3 = not yet but planning to<br>1 = if no yet and no plans to join | 0 | 0 | 2 | 1 | 0 |
| Financial Considerations | | | | | | |
| Are there requirements covering the establishment of a taxable nexus on equipment/services that are involved in providing cloud computing services? | 5 = if no<br>1 = if yes | 0 | 0 | 1 | 0 | 9 |
| Are there any rules for characterizing income from cloud computing services for taxation purposes? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Are there specific taxes are levied on income from cloud computing? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Is cloud computing subject to withholding tax on payments? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Is cloud computing usage subject to taxes (e.g. VAT or GST)? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Are there tax benefits to encourage the use of cloud computing? | Not scored | 0 | 0 | 0 | 0 | 0 |
| Are there tax benefits that discourage the use of cloud computing (i.e., encourage internal IT resources)? | Not scored | 0 | 0 | 0 | 0 | 0 |
| | | | | | | |
| | **Maximum available points defining the ideal state for each criteria** | **70** | **120** | **360** | **150** | **420** |

About the Asia Cloud Computing Association: The ACCA is an industry trade association that represents the stakeholders of the cloud computing ecosystem in Asia, working to ensure that the interests of the cloud computing community are effectively represented in the public policy debate. We aim to promote the growth and development of cloud computing in Asia Pacific through dialogue, training, and public education. We also provide a platform for members to discuss implementation and growth strategies, share ideas, and establish policies and best practices relating to the cloud computing ecosystem. Visit http://www.asiacloudcomputing.org.