Cloud storage and the law

Changes to Asean data protection laws could affect cloud storage implementations

Unstructured data growth continues to present challenges – and opportunities

Shopping for storage? Prepare to be confused by the variety of options

Protecting data on mobile devices, from smartphones to tablets and phablets
DATA PROTECTION LAWS enforced in several Asean countries are putting renewed pressure on cloud storage users to ensure service providers have the appropriate technical and organizational procedures to protect personal data.

With respective personal data protection regulation put into effect last year in Singapore, Malaysia and the Philippines, cloud storage users with data residing in these countries are navigating uncharted waters to ensure compliance.

“The regulations have changed the way organizations engage with cloud services providers,” says Manatosh Das, senior analyst for security and risk at Forrester Research. “Now they are more concerned about security, privacy, compliance and legal issues while implementing cloud storage.”

The laws stipulate how personal data is collected, stored and transferred. They apply to companies that have control of the information, regardless of whether they have asked a third party to collect, process or – in the case of cloud storage providers – store data on their behalf.

This is a major challenge for the growing number of companies in Asia-Pacific moving to software-as-a-service (SaaS) models. “About 41% of Apac budget
decision-makers rate the need to recreate a comprehensive strategy and implementation plan for public cloud and other as-a-service offerings as a high or critical priority,” says Das.

CLOSER SCRUTINY

IT consultant Lito Averia of Rigeltech Information Technology Consultancy and president of the Philippine Computer Emergency Response Team (PHCERT) says cloud storage users have to better understand their providers.

“Potential users of cloud storage services need to assess the provider’s capability to protect data stored in their facilities,” he says.

This, according to Averia, covers an assessment of the provider’s operational processes, people skills and capabilities; the technologies used to protect the infrastructure; the data that resides in the facility; and data in transit between the provider’s facilities and the user’s equipment.

Averia says few people in the Philippines understand the cloud, and the country’s Data Privacy Act (DPA) of 2012 seeks to allay serious concerns raised by existing and potential cloud storage users about security and protection of data – whether they are in transit to and from the service provider’s facility or at rest in the provider’s storage.

As the DPA only provides general guidance, it is now up to companies to come up with a strategy to implement data security and protection that ensures compliance.

Averia stresses the importance of creating and implementing a set of policies that reflect the new law: “Put in place procedures, rules and guidelines that dictate how users across the organization can conduct their assigned roles and functions, especially defining their access rights to the data and how data will be processed and used.

“Cloud storage providers have control over the management, administration, operations and configurations of their infrastructure. In this sense, they may be regarded as a ‘personal information controller’ whose role, function and obligations are defined by law. As a consultant, I always suggest a user accountability framework is included in agreements or contracts between a company and a service provider.”

COMPLIANCE TIPS

Manatosh Das, senior analyst for security and risk at Forrester Research, shares best practices for ensuring that cloud storage implementations comply with local data protection laws:

- Gather legal and regulatory requirements for a feasibility assessment.
- Thoroughly vet your provider.
- Work guidelines and standards into the service level agreement (SLA).
- Seek ongoing assurance that your service providers are compliant.
- Use a third-party, unbiased cloud assessment service.
BESPOKE SERVICE CONTRACT

Gupinder Assi, counsel at the Singapore office of law firm Bryan Cave LLP, says companies should negotiate specific terms and conditions in cloud storage contracts that mirror the data controller’s obligation under the applicable data protection acts.

“They can also insist on audit rights so that companies – or a third-party auditor – can check that appropriate security safeguards are in place,” he adds. “Contractual provisions can also be included to control the countries in which data can be stored, rather than allowing the cloud provider to choose whichever destination they wish.”

Looking forward, Assi believes cloud storage contracts will be more tailored to match the companies’ obligations under data protection legislation. “This will have an impact on price, insurance, liability, etc,” he adds.

Moreover, Assi says companies may wish to treat sensitive personal data differently, “perhaps by ensuring they are stored within their jurisdiction, so that they do not have to comply with the provisions on cross-border transfers”. “Service providers may seek to include consents for

CONSIDERATIONS FOR SUPPLIER ACCOUNTABILITY

Gupinder Assi, counsel for the Singapore office of Bryan Cave LLP, shares best practices for implementing an accountability framework with your cloud service provider:

Data protection officer

- Certain jurisdictions now require the appointment of a data protection officer, or at least someone who is responsible for compliance with the data protection provisions. Even if the legislation does not require this, it is recommended that organizations with large amounts of personal data should nominate someone to ensure compliance with the relevant data protection acts.
- Any nominated individual should establish a team, including members from IT, legal, HR, sales and marketing.

Engage management

- The management should also be engaged in any data protection program and the company should ensure they understand the importance of data privacy.

continued on p5
cross-border transfer of data in their standard terms of conditions with clients and customers,” he adds.

With Asean countries now coming out with their own data protection laws, what is the best way for cloud storage users to deal with a situation where their customer data is located in multiple countries?

“Many data protection laws have a set of core principles central to their provisions, so these should be followed. These include concepts such as notice, purpose, security, transferability, retention and accessibility. These should be encompassed within a company’s data protection policies and practices,” says Assi.

---

**Put in place clear policies and procedures**

- There should be a clear record of what types of data are being stored in the cloud and companies should have a clear policy as to how this is processed. For clients and customers this should be available on a website. A data retention policy should also be in place to ensure data is not kept longer than is necessary and the cloud provider is able to delete such data entirely from its servers when the retention period expires.
- Privacy concerns should be considered at the outset in relation to any new project, product or service.
- It is also good practice to conduct a privacy impact assessment periodically to ensure that appropriate policies and practices are in place to protect personal data, and to refine them as necessary.

**Ensure internal security procedures are in place**

- There should be a system in place to regulate access by company users or subscribers to data stored in the cloud. This includes creating, amending and suspending access to such data by the company.

**Negotiate appropriate provisions in cloud contracts**

- As stated above, specific indemnities should be negotiated with the cloud storage provider.
- Audit rights could also be negotiated to ensure that personal data is being adequately protected.

**Be prepared for a data breach**

- Contracts should be entered into with lawyers, forensic analysts and a PR management company, and a list of hotline numbers of such advisors should be maintained, in preparation for any data breach.
He advises that the following provisions should be included in the cloud storage provider contract:
- The jurisdictions in which data may be stored;
- Provisions on security;
- Provisions on the retention of data;
- An indemnity of loss.

“Companies should be aware of the ability of the government authorities of some jurisdictions to access data held on servers in that jurisdiction and will need to assess whether they wish their data to be located in such jurisdiction,” says Assi.

The promulgation of data protection laws in Singapore, Malaysia and the Philippines not only affects local companies using cloud storage services in these countries, but also affects multinational firms with a presence in the region. Forrester’s Das says it is time for these global companies to take a closer look at local regulations.

“Global firms with a presence in Asia-Pacific generally do not take local regulations seriously enough. In fact, many tech management professionals are unfamiliar with local requirements and simply use the guidelines to comply with the EU Data Protection Directive.

“While this is a sensible foundation, local laws in Asia-Pacific are not aligned with the EU model, and penalties for non-compliance are growing. Recent amendments in existing privacy laws in Australia and Hong Kong, for example, allow the privacy commissioner to enforce significant penalties for data breaches,” Das says.

GIGI ONAG is a freelance journalist based in Hong Kong. She has 10 years’ experience of covering the technology industry across Asia-Pacific and beyond.