It’s Time to Take Data Privacy Seriously in Singapore

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Observe and enforce.*** In April 2016, Singapore revised its Personal Data Protection Act (PDPA) to provide a broader spectrum of powers for regulators to investigate data privacy violations.
- ***Regional reputation.*** While the size of the fines for non-compliance is relatively tame in comparison to countries in the European Union or the United States, the real cost of an investigation comes in the form of highly negative publicity in the region.
- ***Avoid being a target.*** Organizations operating in Singapore should conduct regular privacy and security assessments to ensure they are in compliance with data privacy regulations.
- ***Teach to triage.*** Training employees to detect issues and prevent serious security incidents is an effective way to mitigate the risk of a data security violation.

Over the past decade, there has been an explosion of new data privacy laws in Asia. While certain countries like Malaysia do not actively police their own privacy laws, a number of others, including Singapore, have substantially increased enforcement actions.

Even though the city-state of Singapore is only 720 square kilometers in size, it is beginning to play an integral role in the world economy. Singapore, along with Hong Kong, has often been called the "business nexus of the East." In fact, a recent study conducted by Tower Watson states that Singapore is home to roughly 41 percent of the Asia Pacific headquarters for Fortune 500 companies, compared to 34 percent for Hong Kong and 16 percent for Mainland China.

n 2012, Singapore passed the Personal Data Protection Act (PDPA), which established a general data protection law in Singapore. Among other things, the PDPA governs the collection, use, disclosure, and protection of individuals' personal data by organizations. The main enforcement agency in charge of enforcing the PDPA is the Personal Data Protection Commission (PDPC). The PDPA provides the PDPC powers to: (1) investigate organizations' data protection practices; (2) obligate organizations to cease activities which are in violation of PDPA; (3) obligate organizations to destroy personal data collected in contravention of PDPA; (4) obligate organizations to comply with any other orders by PDPC; and, (5) obligate organizations to pay a fine which may not exceed US$1 million.

PDPA guidance on enforcement actions

On April 21, 2016, the PDPC revised the Advisory Guidelines on the Enforcement of the Personal Data Protection Act (Enforcement Guidelines). While the Enforcement Guidelines are not legally binding, they provide an understanding of how the PDPC decides which organizations to target for an investigation and what fines to seek.

The Enforcement Guidelines state that the PDPC may commence an investigation into any organization that the PDPC considers to be warranted based on the information that it obtained — whether from a complaint or otherwise. Among other things, the PDPC reviews the following factors to decide whether to investigate and/or whether financial penalties may be assessed: if the organization failed to comply with the PDPA, if the organization has systematically failed to comply with the PDPA, or if there is potential harm and severity in the misconduct.

Enforcement actions

In the past, the PDPC published enforcement actions related to "do-not- call" rules, which are a set of regulations loosely similar to the US Do-Not-Call rules. However, only recently has Singapore actively enforced and provided guidance on how the PDPC will approach enforcement of other parts of the PDPA.

First shots fired

On April 21, 2016, Singapore's PDPC published its first set of 11 enforcement actions. The organizations involved range from small businesses to multinationals such as China's Xiaomi subsidiary. Of the 11 enforcement actions, four organizations were fined for violations of the PDPA and six other organizations were issued warnings. Eight out of the 11 actions were based on a breach of Section 24 of the PDPA (Section 24) for failing to implement proper and adequate protective measures, which resulted in the unauthorized disclosure of personal data. Section 24

provides that an organization shall protect personal data in its possession or under its control by making reasonable security arrangements in order to prevent against unauthorized data access, collection, use, disclosure, copying, modification, disposal, or similar risks.

The largest assessed fine by the PDPC was to K-Box Entertainment Group Pte Ltd for S$50,000. In 2014, it was published that over 300,000 K-Box members' information had been leaked and uploaded online. The breach impacted the following types of data: names, contact numbers, and residential addresses. K-Box was found by the PDPC to have failed to input adequate security measures to protect personal data in its possession. Among other things, K-Box allegedly failed to enforce a password policy, provide reasonable controls over unused accounts, utilize a new version of software, or conduct security audits.

The PDPC also assessed a fine to Finantech Holding, K-Box's IT service provider. Finantech was in charge of developing, hosting, and managing K-Box's Content Management System (CMS). As a data intermediary, Finantech allegedly did not implement adequate data security measures for the CMS, such as patching security vulnerabilities or using a complex password for an administrative account.

Continued enforcement of data privacy laws

Since April, Singapore has increased its rate of enforcement actions. The PDPC released details of 11 more enforcement actions. Of the 11 new enforcement actions, seven companies received fines ranging from S$500 to S$25,000, and four companies received warnings. Similar to the first set of enforcement actions released on April 21, the majority (eight out of 11) relate to a breach of Section 24 for allegedly failing to implement proper and adequate protection measures.

Among the most recent enforcement actions, the PDPC fined Toh-Shi Printing (Toh-Shi) on two separate occasions for failing to implement proper and adequate protection measures. Toh-Shi was a service provider in charge of printing and sending paper notices on behalf of consumers. In both cases, Toh-Shi accidently sent sensitive financial information to the wrong customers. The PDPC fined Toh-Shi for allegedly failing to provide adequate quality controls and employee training. The events at Toh-Shi suggest that enforcement of Section 24 is not limited to IT security related measures, but also includes non-technical measures of quality control and employee training.

Perhaps the most interesting aspect of the Toh-Shi enforcement actions is that the two different companies that hired Toh-Shi as a service provider were not fined or found to be in violation of Section 24. This serves as a stark contrast from the severity of the enforcement action against K-Box. Even though Finantech managed part of K-Box's IT operations, K-Box was still fined for a breach of the PDPA.

The K-Box scenario, however, differs from the Toh-Shi incidents in two distinct ways. First, while Finantech was responsible for handling some of K-Box's IT operations, it was not primarily responsible. K-Box still maintained some IT-related authority, ultimately contributing to the breach of over 300,000 customer records. Alternatively, under the Toh-Shi enforcement actions, the company outsourced all parts of the printing operation, from the initial printing to the mailing of financial records. This suggests that there may be less privacy risk if the service provider completed all aspects of a process. Unlike K-Box, which did not have any data protection provisions in its contract with Finantech, Toh-Shi's customers contractually required the company to put adequate security policies, procedures, and controls into place. In other words, the PDPC's actions suggest that imposing contractual requirements on a vendor may discharge a company's obligations to take

“reasonable and appropriate” steps to secure information.

The Toh-Shi enforcement actions also show how a systematic and continuous disregard to adequate security measures may increase the magnitude of fines. Because Toh-Shi continued to reject security measures, the company’s second fine was increased from S$5,000 to S$25,000.

While the size of the fines levied by the PDPC for non-compliance of the PDPA have been relatively modest as compared to the million dollar fines issued by EU countries or by the United States, the real cost of an investigation by the PDPC comes in the form of highly negative publicity and the expenditure of legal fees and human capital.

Future considerations

As Singapore’s PDPC gains more experience and refines its interpretation of the PDPA, we expect to see more enforcement actions in Singapore. According to Singapore’s government directory, there are 18 individuals who work in the Personal Data Protection Commission. Of those 18 employees, roughly a third have been employed at the PDPC for less than 18 months.* Unfortunately, a detailed breakdown of headcount is not available from the Singapore government, but we speculate that as these new employees become more experienced and fully integrated with the PDPC, more enforcement actions will likely occur.

* Of the 18 individuals listed on the Singapore Government Directory, we found 13 of the individuals on LinkedIn. The information was based on a review of their LinkedIn profiles on November 18, 2016.

We understand that the PDPC is actively working with entities in Singapore by putting together data protection and security related training and educational sessions. However, the current list of enforcement actions shows that Singapore is also serious about its enforcement of the PDPA. Of the 22 enforcement actions, a sizeable majority of companies may be deemed to be either small- or medium-sized. We speculate that this may be due to the fact that the PDPC is still a relatively new government organization and that it may want to pick relatively easy targets with either egregious security practices or a lack of resources to challenge the PDPC in court. The PDPC may also be following an old Chinese idiom of (????) — or kill the weak to scare the strong. Picking relatively small companies with egregious security practices to fine may be a method for the PDPC to show the general public that they are serious about enforcement and are intent on setting an example in order to scare larger companies who may not be taking data protection seriously. As the PDPC becomes more experienced, we expect larger organizations to be targeted and higher fines to be assessed.

Lastly, since data breaches are now high profile events and often create rapid and widespread media attention, we expect Singapore to focus heavily on implementing proper and adequate protective measures on personal data through Section 24 of the PDPA. Sixteen of the 22 enforcement actions involved a failure for entities to maintain such measures.

Considerations for entities operating in Singapore

Recent enforcement actions have showed a propensity for the PDPC to focus heavily on implementing proper and adequate protective measures for personal data. The PDPC recently released the Advisory Guidelines on Key Concepts In the Personal Data Protection Act (Guidelines). Similar to the “I’ll know it when I see it” standard for obscenity in the United States, the Guidelines

do not provide a binary list of what an organization must do in order to be compliant under Section 24. Instead, the Guidelines state that there is no one-size-fits-all solution for data security. Rather, security obligations depend on the nature of the information, the form of the information, and the possible impact of the unauthorized disclosure of the information. Among other things, we recommend companies consider the following measures:

Conduct a privacy and security assessment of policies and procedures. Conducting a data privacy and security assessment allows an organization to review current policies to determine whether (1) the policies and procedures need to be updated and (2) the company actually follows the stated policies and procedures. It is also important to remember that going through the motions of a security assessment is not enough. For example, the PDPC issued a warning to Metro Pte Ltd for not addressing SQL injection vulnerabilities that were discovered in earlier IT security audits. To effectively lower risk, an organization needs to address issues found through security assessments and audits. In order to have an unbiased and truthful opinion of an organization's security measures, an organization should consider using a third-party vendor.

Organizations should consider, at a minimum, implementing and acquiring the following policies and procedures:

- Incident response plan;
- Mobile IT policy;
- Record retention policy;
- Password management policy;
- User access and management policy; and,
- IT vendor management process.

Conduct an internal data inventory. Knowing the type of data collected and held allows an organization to review the sensitivity and determine whether current security measures are appropriate and reasonable.

Organizations should consider the following when conducting a data inventory:

- The types of data collected;
- Where the data is physically housed (e.g., the building or location);
- Where the data is logically housed (e.g., the electronic location within a server);
- Whether encryption is applied to the data in transit (i.e., when it is moving). If it is, consider what encryption standard is being used;
- Whether encryption is applied to the data at rest (i.e., when it is being stored). If it is, consider what encryption standard is being used;
- The custodian of the data (i.e., who is responsible for it);
- Who has access within the organization to the data;
- Who has access outside of the organization to the data;
- Whether the data crosses national boundaries; and,
- The retention schedule (if any) applied to the data.

Review IT service provider contracts for adequate data protection provisions. The Toh-Shi enforcement actions suggest that one way an organization can protect itself against a possible enforcement action is to include adequate data protection measures in service provider contracts.

Consider adding the following provisions:

- Limitations to the use of personal data;
- Breach notification requirements;
- Representations, warranties, and covenants relating to data privacy and security;
- Indemnification obligations;
- Compliance with applicable data protection laws;
- Data transfer limitations;
- Audit or monitoring rights;
- List of certain IT technical safeguards (i.e., encryption standard, access control); and,
- Data maintenance/deletion obligations.

Request IT service provider complete a security questionnaire. Taking a proactive approach by requesting that a service provider complete a security questionnaire may avoid the headache of selecting a service provider that does not have adequate security procedures. This will lower the risk of a potential data breach. When drafting a security questionnaire, consider the following:

- The designated employee responsible for overseeing security program;
- Procedures for appropriately destroying documents with sensitive information;
- Encryption standards for mobile devices;
- Encryption standards for transmitting sensitive information;
- Employee training;
- Data breach incident response;
- Vendor management process;
- Process for provisioning user access;
- Process for de-provisioning user access; and,
- Disciplinary measures for security violations.

Conduct data security/privacy training for employees. Conducting data security/privacy training for employees may prevent potential security incidents. This preventive measure allows employees to detect issues earlier and may prevent more serious security incidents in the future.

For good reason, Singapore is one of the most popular places for multinational companies to establish their APAC company headquarters. With a strong rule of law, Singapore takes enforcement of its laws seriously and the PDPA is no exception. The increase in the number of PDPC enforcement actions shows the country's growing intention to ensure the protection of personal data through the enforcement of the PDPA. While the size of the fines levied by the PDPC for non-compliance has been relatively modest, it does not take into account the time and reputational costs associated with a PDPC investigation. Entities that operate in Singapore would be wise to conform their compliance to the PDPA and to pay attention to the PDPA's actions and public statements.

Further Reading

PriceWaterhouseCooper, The Preferred Asian HQ Location, (January 28, 2015).

Personal Data Protection Act of 2012, Section 28-30.

Personal Data Protection Commission, Advisory Guidelines on Enforcement of the Data Protection Provisions, (April 21, 2016).

Id. at Section 2.

Id. at Sections 15.3 and 25.

Government of Singapore, *PDPC Takes Action Against 11 Organizations for Breaching Data Protection Obligations*, April 21, 2016.

Section 24 of the PDPA.

Decision of the Personal Data Protection Commission, K Box Entertainment Group PTE. LTD., Finantech Holdings PTE. LTD., [2016] SGPDPC 1, Section 44 (April 20, 2016).

Id. at Section 2.

Id. at Section 3.

Id. at Section 30.

Id. at Sections 26 to 29.

Id. at Section at 5.

Id. at Section 39.

See Personal Data Protection Commission list of data protection enforcement cases; as of November 18, 2016.

See Decision of the Personal Data Protection Commission, Aviva Ltd. and Toh-Shi Printing Singapore Pte. Ltd., [2016] SGPDPC 15, (September 21, 2016). Decision of the Personal Data Protection Commission, Central Depository (PTE) Limited and Toh-Shi Printing Singapore Pte. Ltd., [2016] SGPDPC 11, (July 21, 2016).

[2016] SGPDPC 15 at Section 4; [2016] SGPDPC 11 at Section 3.

[2016] SGPDPC 15 at Section 8; [2016] SGPDPC 11 at Section 7.

[2016] SGPDPC 15 at Section 34.

[2016] SGPDPC 15 at Section 28; [2016] SGPDPC 11 at Section 18.

[2016] SGPDPC 1, at Section 39.

See generally, [2016] SGPDPC 1.

Id. at Sections 9 to 12.

[2016] SGPDPC 15 at Section 4; [2016] SGPDPC 11 at Section 3.

See [2016] SGPDPC 1 at Section 12; see also SGPDPC 15 at Section 27 and [2016] SGPDPC 11 at Section 17.

[2016] SGPDPC 15 at Section 38.

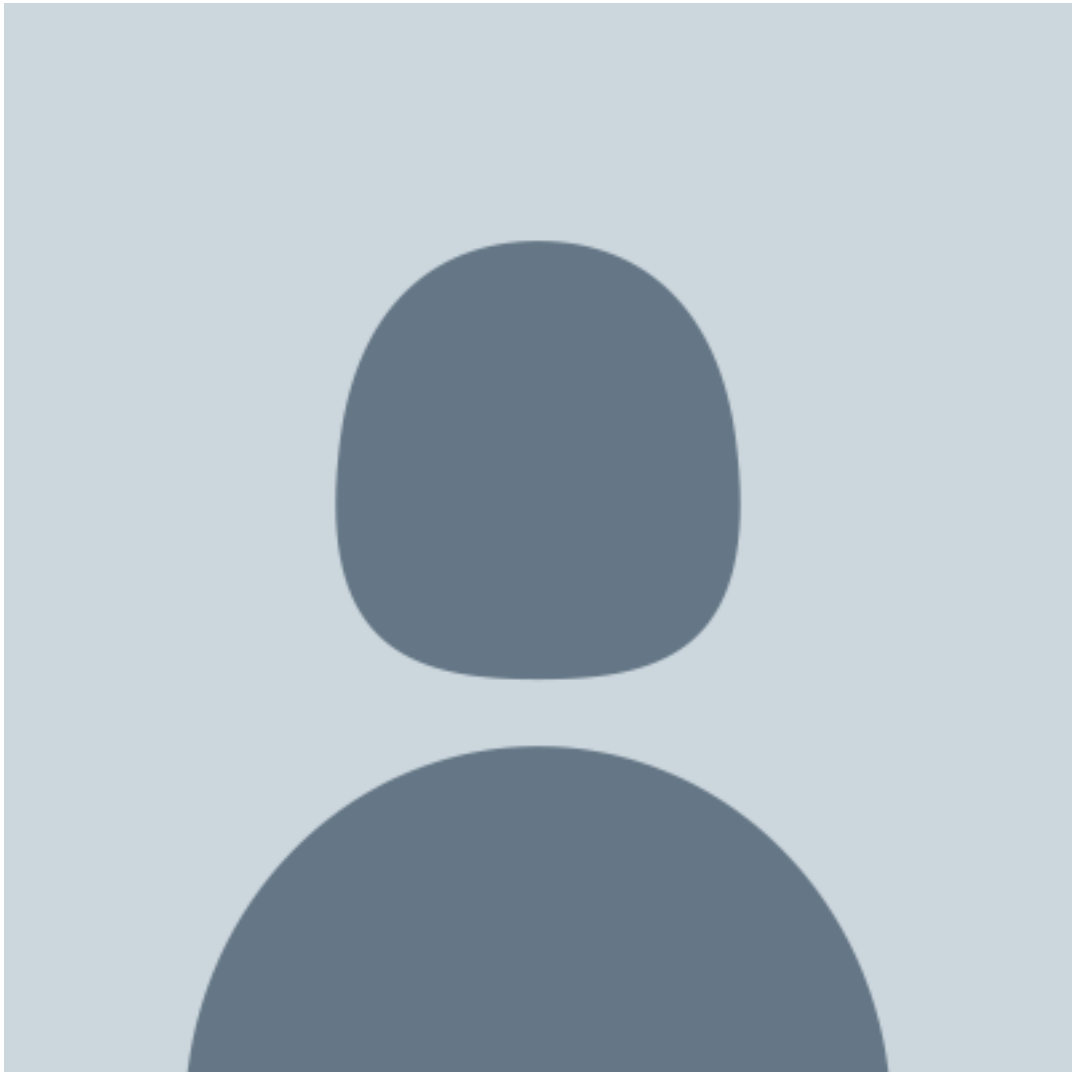
See Singapore Government Directory for a list of Personal Data Protection Commission employees.

Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (July 15, 2016).

Decision of the Personal Data Protection Commission, Metro Pte Ltd., [2016] SGPDPC 7, (April 20, 2016).

Zetoony, David, *Data Privacy and Security: A Practical Guide for In-House Counsel*, Pg. 2-3, May 2016.

Daniel Wang

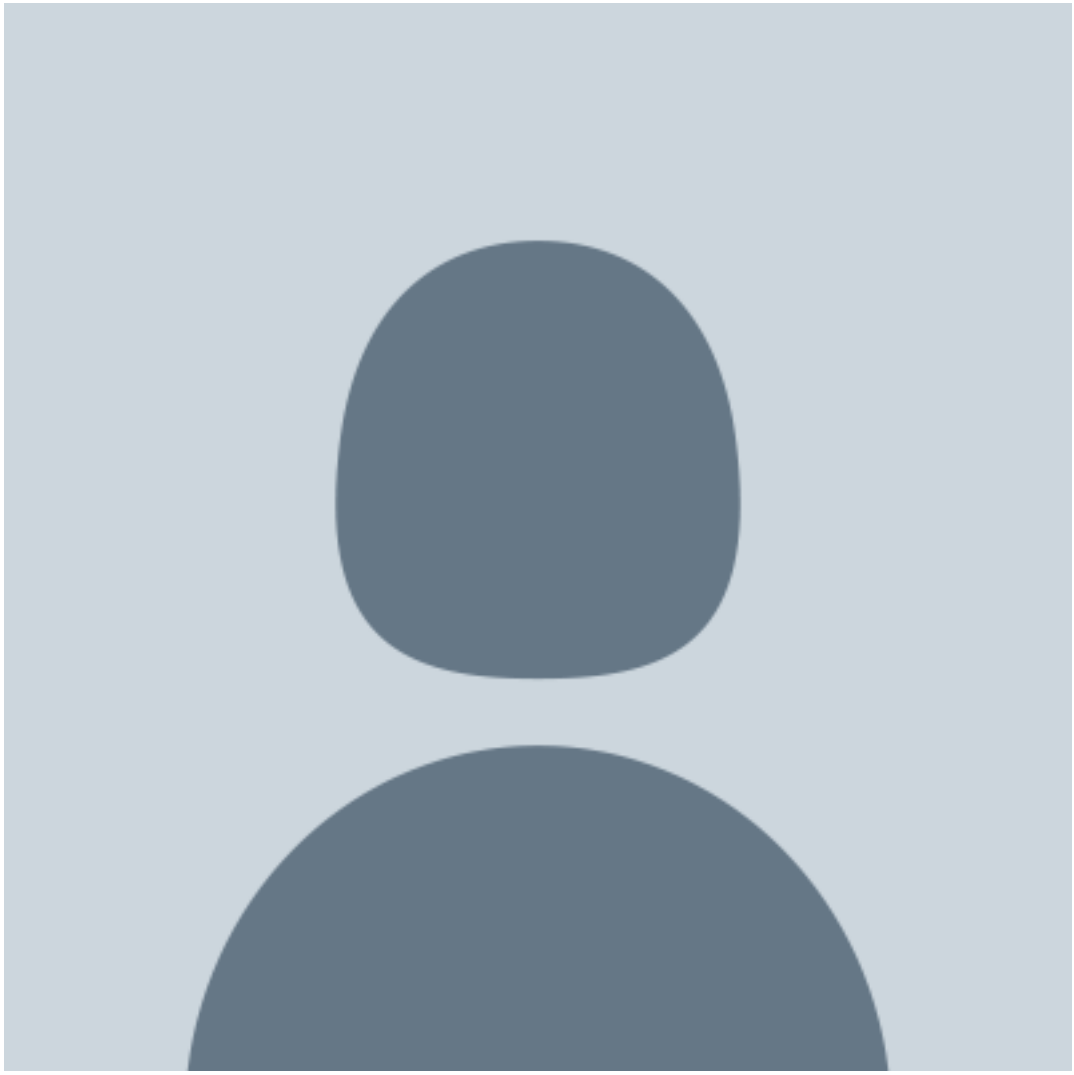


Corporate Legal Counsel

Beyondsoft

He works at their US office in Bellevue, Washington. Beyondsoft is a US$1 billion market cap public listed IT consulting and outsourcing company.

David Chen



Associate

the Boulder, Colorado office of Bryan Cave

He practices with the firm’s technology, entrepreneurial, and commercial practice client service group, where he focuses on technology transactions, data privacy, and security matters.