RHTLaw Asia

February 2023

Year-End Review for Data Protection and Cybersecurity Laws in Major Jurisdictions in Asia for 2022 (Part 1)

Introduction and Overview

It was another busy and hectic year for legislative developments in Data Protection in Asia. It was heartening to see so many countries in Asia, from Indonesia to China and Japan, step up their legislative efforts to enhance and improve their data protection standards.

Pertinently and unsurprisingly, cross-border data flows and data breach response took centre stage in most of the new developments in Asia. Some countries, like Singapore and Hong Kong, implemented measures to address more specific concerns, reflecting how sophisticated and mature their laws have since evolved.

In this year-end roundup, I will provide a snapshot in two parts. The first part will cover the significant developments in Singapore, and in the second part, we will look at how some of the major Asian countries are enhancing their data protection standards to address the growing threats in the region.

Singapore's Data Protection Regime : A year of Levelling Up to meet new challenges

Ever since 2013, when omnibus legislation on data protection was first introduced, Singapore has continuously enhanced and refined its provisions to cater to the ever-changing landscape threatening the protection and security of personal data. Amongst other things, -

- The Personal Data Protection Commission ("PDPC") continued its good work in policing the standards of protection of personal data, by setting standards in niche and nascent areas, including addressing concerns arising from A.I, blockchain and cloud security providers;
- The Cybersecurity Agency of Singapore also continued its efforts to enhance regional co-operation and enhance standards of protection for Critical Information Infrastructure ("CII"); and
- There was also a landmark Court decision, the first ever on the Personal Data Protection Act ("PDPA").

The PDPC has had a Busy Year

In 2022, the PDPC set out a plethora of guidelines, most of which were catered towards very specific situations. In 2022, the PDPC published or released the following: -

- The PDPC on 31 March 2022 published a new Guide on Basic Anonymisation to provide more practical guidance for businesses on how to appropriately perform basic anonymisation and de-identification of various datasets through a simple 5 step anonymisation process
- On 4 April 2022, the PDPC and Info-Communications Media Development Authority (IMDA) offered the Data Protection Essentials (DPE) programme, which supports Small and Medium Enterprises (SMEs) in acquiring a basic level of data protection and security practices to protect their customers' personal data and recover quickly in the event of a data breach
- On 17 May 2022, the PDPC published a new Guide on the Responsible Use of Biometric Data in Security Applications to help organisations such as Management Corporation Strata Title (MCSTs), building/premise owners and security services companies, to ensure responsible use of security cameras and biometric recognition systems to safeguard individuals' biometric data where it is collected, used or disclosed
- On 25 May 2022, the IMDA and the PDPC launched A.I. Verify - the world's first AI Governance Testing Framework and Toolkit for companies that wish to demonstrate responsible AI in an objective and verifiable manner. A.I. Verify aimed to promote transparency between companies and their stakeholders
- On 30 May 2022, the PDPC launched a free Data Anonymisation tool to help organisations transform simple datasets by applying basic anonymisation techniques. An infographic that provides guidance on how to use the tool was also included.
- On 18 July 2022, the PDPC launched a Guide on Personal Data Protection Considerations for Blockchain Design to help organisations with blockchain adoption by clarifying how to comply with the PDPA when deploying blockchain applications to ensure more accountable management of customers' personal data.
- Increasing digitalisation has also spurred more organisations to adopt cloud services and platforms. With the security features in-built by the cloud service providers (CSPs), cloud services and platforms are generally more secure than on-premises implementation. On 18 July 2022, the PDPC launched an infographic to help organisations start implementing good practices to secure personal data in the cloud platform.
- On 20 July 2022, the IMDA and the PDPC launched a Privacy Enhancing Technologies (PET) Sandbox to support businesses who wish to pilot PET projects that address common business challenges. PET allows the extraction and sharing of insights, while protecting personal data and commercially sensitive information.
- Finally, but most significantly, PDPC enacted amendments to the enforcement of the PDPA, effective from 1 October 2022.

  The power of the PDPC was enhanced to accept voluntary undertakings as part of its enforcement regime. Additionally, the financial penalty cap which may be imposed on organisations for breaches under the PDPA has increased from the previously fixed S$ 1 million, to 10% of the organisation's annual turnover in Singapore for organisations with annual local turnover exceeding S$10 million, whichever is higher.

  To help organisations with compliance, the PDPC also updated the Advisory Guidelines on Enforcement of Data Protection Provisions, and the Guide on Active Enforcement.

Cybersecurity Agency of Singapore ("CSA")

2022 was another busy year for the CSA, counting building up regional co-operation and strengthening capabilities amongst its achievements.

The CSA, in partnership with the Global Forum on Cyber Expertise (GFCE), officially announced the creation of a GFCE Southeast Asia Liaison position in October 2022 at the Singapore International Cyber Week 2022.

This Liaison will connect the region and the existing efforts of the ASEAN-Singapore Cybersecurity Centre for Excellence ("ASCCE") more closely with other GFCE member nations and organisations, including GFCE Liaisons and Hubs from other regions. This closer integration of the region and the GFCE through the Liaison is expected to facilitate exchange of best practices and foster a deeper understanding of the region's cyber capability gaps, as well as ensure better coordination of cyber capacity building efforts amongst the region's stakeholders and more efficient use of resources to close these gaps.

The CSA also upgraded the Cybersecurity Code of Practice ("The 2022 Code") for Critical Information Infrastructure ("CII"), effective from 4 July 2022, superseding previous versions of the Code.

This Code is intended to specify the minimum requirements that the Critical Information Instructure Owner ("CII Owner") shall implement to ensure the cybersecurity of its CII.

The CII Owner is expected to implement measures beyond those stipulated in this Code to further strengthen the cybersecurity of the CII based on the cybersecurity risk profile of the CII.

Of particular significance within this 2022 Code: -

- All owners of CII in Singapore must comply with this 2022 Code under the Cybersecurity Act of Singapore.
- Certain acts require to be performed on a recurring basis, that is to say, once is not enough.
- The CII Owner has very specific obligations in relation to assessment, detection, prevention and response to any cybersecurity threats.
- CII Owners who engage the services of Cloud Service Providers (CSP) shall remain responsible and accountable for maintaining oversight of the cybersecurity of the CII and for managing cybersecurity risks to the CII, even when the CII is wholly or partly implemented on cloud computing systems; and the CII Owner must ensure that the CSP appoints a person in Singapore to accept service of legal process.

Any onerous burden that is imposed onto owners of CII is essential and must be balanced against the fact that the cybersecurity has become one of the crucial pillars of the safe operation of CII.

First Court Decision on the PDPA

Finally, in a landmark decision, the Singapore Court of Appeal ("CA") provided some valued insight as to its approach on the interpretation of the provisions of the PDPA.

In the case of Michael Reed v Alex Bellingham (Attorney-General, Intervener) [2022] SGCA 60, they adopted a purposive approach to the construction of the term "loss or damage" under s 32(1) of the PDPA. Section 32(1) confers a right of private action on any person who suffers loss or damage directly because of the contravention of any provision in Part IV/V/VI of the PDPA.

In essence, the CA held that "loss or damage" under s 32(1) of the PDPA includes emotional distress but excludes loss of control of personal data. Some of the CA's key findings are summarized below:

- Section 4(1)(b) did not exempt the respondent, as an individual, from liability for breaching ss 13 and 18 of the PDPA. The CA held that individuals are subject to ss 13 and 18. To hold otherwise would be contrary to a stated aim of the PDPA, namely, to recognize the right of individuals to protect their personal data.
- Common law principles on vicarious liability should not be imported into s 4(1)(b) as the employer's liability under the PDPA.

Scope of "Loss or damage"

- The s32 action is a statutory tort and its scope is determined first and foremost by the principles of statutory construction.
- The general purpose of the PDPA was to provide robust protection for individuals' personal data. The specific purpose of s 32 is to create a statutory tort and to allow a right of private action on that basis.

- Interpreting "loss or damage" to include emotional distress ("Wide Interpretation") would not open the floodgates to frivolous claims for minor or technical breaches. One control mechanism is the requirement of a strict causal link in that the "loss or damage" must have directly resulted from the breach. Secondly, trivial annoyance or negative emotions which form part of the vicissitudes of life will not be actionable ("de minimis principle"). In addition, the CA envisaged that individuals will be discouraged from making frivolous claims for emotional distress through the development of case law under s 32(1) and the imposition of cost orders in the normal course of litigation.
- The Wide Interpretation should be preferred as it better promotes the general purpose of the PDPA and the specific purpose of s 32;
- Specific purpose of s 32: If s 32 was to be an effective means for individuals to enforce the right to protect their personal data, Parliament could not have intended s 32(1) to be "a dead letter" in many cases where no material damage is suffered.
- The test for determining whether an individual has suffered emotional distress cannot be fully objective, although greater weight will be attached to objective indicia of emotional distress. The inquiry must be anchored in whether the individual subjectively suffered emotional distress because remedies are awarded to compensate the person aggrieved or to ameliorate the injury.

"Loss of control"

- The CA agreed with the High Court that loss of control of personal data did not constitute "loss or damage" under s 32. Taking the opposite view would render the requirement of "loss or damage" in s 32(1) tautologous as the breach of any provision in Part IV to VI would inevitably give rise to cognizable "loss or damage".

Conclusion

Despite all the efforts to level up standards, to address data security concerns on new and specific issues like A.I. and blockchain, and even improving standards for the protection of CII, more still needs to be done to fight against all threats to data security.

The continued reports of data breaches are a testimony that the fight to protect data remains a constant need.

It is nonetheless reassuring to see that efforts in Singapore are being made to "level up" standards, whether to provide guidance to manage personal data in this era of new technologies and innovation, or to guard against specific and new types of threats.

As will also be seen by developments in major Asian countries, the improvements and enhancements can only make it easier for other countries to co-operate on joint enforcement efforts with Singapore for their data protection regimes.

About the Author

Wun Rizwi
Partner
RHTLaw Asia
rizwi.wun@rhtlawasia.com
+65 6381 6818

Rizwi is a founding member of RHTLaw Asia, and is the Acting Head of the firm's Intellectual Property and Technology Practice. He also heads the Firm's Consumer Brands Industry Group, with specific focus on Food & Beverage, Fashion & Luxury, and the Video and Computer Games industries.

About RHTLaw Asia

RHTLaw Asia offers a different perspective on client experience and commercial thinking. As a leading regional law firm headquartered in Singapore, clients can expect intelligent and innovative solutions from a team that is attuned to the nuances of doing business in Asia.

With access to our own ASEAN Plus Group, a network of leading firms comprising over 2,000 lawyers in 16 jurisdictions across Asia and beyond, as well as our membership with The Interlex Group, a global network of leading law firms and HLB a global advisory and accounting network, we help clients understand the local challenges, navigate the regional complexity to deliver the competitive advantage for their businesses in Asia.

In delivering innovative legal and commercial solutions, it collaborates with ONERHT through entities which are not affiliates, branches or subsidiaries of RHTLaw Asia LLP.