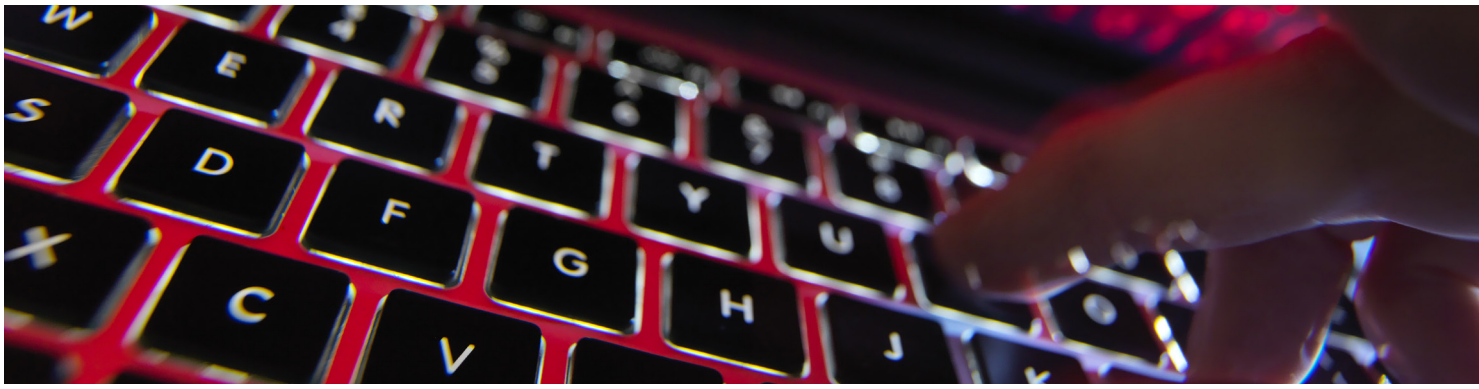
RPC PREMIER LAW

Data protection alert



Are you compliant with the new rules in Singapore? Asia? Beyond?

February 2020

With the implementation of the GDPR in Europe (2018) and the rise of serious cyber-attacks in Asia, many APAC countries are making major changes to their data privacy laws. Navigating the various regulatory regimes can be complex particularly for companies doing business across the region and beyond.

There is no overarching regulatory framework in Asia like the GDPR in Europe. Some countries have implemented strict data protection regulations (eg South Korea) and others have very few or no specific data privacy laws. Over the last 12 months there has been a significant increase and/or change in data protection legislation (or an announcement of the intention to make changes) across APAC. A few recent examples include:

South Korea

On 9 January 2020 the Korean National Assembly passed major amendments to the three main data privacy laws (ie Personal Information Protection Act (PIPA), Promotion of Information Communications Network Utilisation Act and Use and Protection of Credit Information Act).

In broad terms these changes have sought to minimise the burden of overlapping data privacy regulations and supervisory bodies while elevating and strengthening the Personal Data Protection Commission's status and powers. The PIPA has been amended to clarify the definition of 'personal data', and it has also introduced the concept of 'pseudonymised data' and defined how such data can be processed without the data subjects' consent.

Hong Kong

On 20 January 2020 the Legislative Council on Constitutional Affairs discussed possible changes to the Personal Data (Privacy) Order (PDPO) following a paper (LC Paper No. CB(2)512/19-20(03)) released by the Constitutional and Mainland Affairs Bureau which was aimed at strengthening data privacy laws in Hong Kong.

Proposed changes to the PDPO include (amongst others): (i) the introduction of a mandatory notification obligation for data breaches with "a real risk of significant harm"; (ii) broadening the definition of personal data; and (iii) increased administrative fines. One to watch in the coming months.

Thailand
The Thai Personal Data Protection Act was enacted in 2019 and is due to come into force on 27 May 2020.

Singapore
Over the last 12 months Singapore has made significant changes to its Personal Data Protection Act including the implementation of mandatory notification to the Personal Data Protection Commission (PDPC) in certain circumstances. There may soon be a mandatory notification of all data breaches. A comprehensive update regarding the new changes is set out below.

Malaysia and India have also recently announced their intentions to review and potentially revise their existing data privacy laws.

Staying on top of the changes to the data protection laws around the APAC region can be challenging. Please contact us if you would like specific advice or would like to have an informal chat. We have dedicated data protection specialists in our Singapore and Hong Kong offices and we work closely with our preferred cyber and data protection firms in 14 countries across the APAC region.

Updates to the Personal Data Protection Act (Singapore)

The note that follows is a non-exhaustive summary of some of the more recent guides issued by the Singapore Personal Data Protection Commission and its impact on the way an organisation is to "collect, use and/or disclose" Personal Data.

PDPA

Key changes – at a glance

- Prohibition of the collection of an individual's NRIC (or a copy) and the IC number for many companies.
- Mandatory reporting of data breaches if the breach is likely to result in significant harm or involves the data of 500 or more individuals.
- Individuals must be informed of a data breach if there is likely to be significant harm.
- Madatory notifications must be made to the PDPC within 72 hours.
- The rules may change soon to include mandatory notification of all data breaches.

The Personal Data Protection Act 2012 ("PDPA") was enacted in 2012. Its provisions came into force in stages such as the formation of the PDPC in 2013 and the Do Not Call Registry in early 2014.

It was only in the middle of 2014 that the main provisions of the PDPA came into force. This was to give organisations time to consider the provisions and implement practices and procedures to ensure that when the PDPA is fully in force, they would be able to comply with the terms.

Under the PDPA there is a requirement for an organisation to notify an individual of the purpose of collecting, using and/or disclosing the data ("Personal Data") of the individual and to obtain the consent of the individual before the Personal Data is collected.

Once the Personal Data is collected, there is a duty to ensure that it is accurately recorded and that it is retained in a secure manner.

Personal Data may be transferred out of Singapore but there are certain requirements to be met before it is transferred out.

Once the purpose for which the Personal Data was collected, used and/or disclosed is no longer necessary there is a duty on an organisation to not retain (ie dispose) the Personal Data in a secure manner.

Under the PDPA an individual can request an organisation to disclose the Personal Data that it has on that particular individual and if there is such a request, the organisation is required to furnish the relevant details.

An organisation that does not comply with the PDPA can be subjected to various directions by the PDPC including but not limited to a financial penalty not exceeding SGD 1 Million Dollars.

Guidelines

Under the PDPA, the PDPC may issue "written advisory guidelines" for the purposes of interpreting the provisions of the PDPA. As at the time of this note, there are about 34 guides comprising both written advisory guidelines as well as other general guides.

As it is not possible to discuss all the guides issued by the PDPC, this note will therefore focus on some of the more recent guides issued by the PDPC which are of general application.

NRIC

There are currently two guidelines issued by the PDPC on NRICs ("NRIC Guides"). The first guideline is a written advisory guideline on the use of NRIC numbers and the second guideline is a technical guide on using alternatives to NRIC numbers. They were both issued on 31 August 2018. The second guideline was revised and a revised version of the second guideline was issued on 26 August 2019.

The NRIC Guides generally prohibit the collection of an individual's physical NRIC (or a copy thereof) as well as the NRIC number of that individual.

The NRIC Guides encourage organisations to consider using alternatives to an individual's NRIC number such as the individual's phone number, residential address or email address.

Under the NRIC Guides, if there is a need to collect the NRIC number of an individual, it recommends the collection of "partial numbers" of an individual's NRIC such as the last 3 digits followed by the checksum. If a partial number is collected instead of the full NRIC number, the organisation is not subjected to the stringent requirements under the NRIC Guides. However, care must be taken to note that even if partial numbers are collected, the partial numbers are still Personal Data under the PDPA so the organisation is still required to comply with the PDPA.

If there is a requirement under the law to retain a person's physical NRIC or collect the full NRIC number, then the NRIC Guides do not apply. Mobile phone service providers, hospitals, clinics, hotels and massage establishments are required under the law to collect a person's full NRIC number.

Under the Second Schedule, Third Schedule and Fourth Schedule of the PDPA ("PDPA Schedules") an organisation may collect, use and/or disclose the NRIC number of an individual in certain circumstances. A selection of the circumstances is listed below:

- in the interest of the individual
- responding to an emergency that threatens the life, health or safety of the individual or another individual
- the Personal Data is publicly available
- national interest
- necessary for investigations or proceedings
- for evaluative purposes
- solely for artistic or literary purposes
- debt owed to or from the individual
- providing legal services
- creating a credit report
- creating a private trust
- providing domestic services
- person's employment or termination
- matters relating to a business asset transaction
- disclosed by a Public Agency
- research
- informing law enforcement agencies
- contacting next of kin

Under the NRIC Guides, if an organisation is not required under the law to collect the NRIC number of a person and if the exceptions under the Second, Third and Fourth Schedules of the PDPA do not apply, the organisation may still be able to collect the NRIC number of a person if it can show that the NRIC number is required for the purposes of "accurately establishing or verifying the identity of an individual to a high degree to fidelity".

The way to ascertain whether there is a need to "accurately establish or verify the identity of an individual to a high degree to fidelity" is to ask the following questions:

- would there be a significant risk to safety
- would there be a significant risk to security
- could there be significant impact or harm to organisation/individual?

Examples include the possibility of a significant risk to safety when a visitor is visiting a school for young people and the possibility of a fraudulent transaction in the healthcare, insurance or property sector.

Under the NRIC Guides, even if there is voluntary disclosure by an individual of his NRIC number, the organisation cannot collect the number unless there is a justification for doing so.

Care must be taken to ensure that even if an organisation is allowed to collect the NRIC number of an individual, that is not the end of the matter. Firstly an NRIC number is still Personal Data so the provisions of the PDPA will apply. Secondly and more importantly, given that NRIC numbers are sensitive and that there are serious consequences of a person's NRIC number ending up in the wrong hands, it would follow that if there was a data breach and if the data that was breached includes NRIC numbers the consequences of that breach would be more severe than a breach of other types of Personal Data that did not include NRIC numbers.

Data breaches

The PDPC issued a guide on 22 May 2019 dealing with data breaches ("Data Breach Guide").

When an organisation becomes aware of a data breach, it has to carry out and complete an assessment within 30 days starting from the time when the organisation first becomes aware of the data breach.

Currently there is mandatory reporting of data breaches only in the following circumstances:

- if the assessment reveals that the data breach is likely to result in significant harm or impact to the individuals whose data was compromised, the organisation must report the data breach to the PDPC within 72 hours of the conclusion of the assessment and also inform the individuals of the data breach as soon as practicable

- if the assessment reveals that the data breach is of a significant scale involving the data of 500 or more individuals but the assessment does not reveal any likelihood of any significant harm or impact to the individuals whose data was breached, the organisation is to report the data breach to the PDPC within 72 hours of the conclusion of the assessment but there is no need to inform any of the individuals.

Other than the above scenarios there is **for the moment** no mandatory reporting of data breaches. Care must be taken to note that the Data Breach Guide says that there will soon be a mandatory reporting for all data breaches.

Under the Data Breach Guide, all organisations are required to have a Data Breach Management Plan which is to include the following:

- a data breach management team with defined responsibilities
- a clear explanation of what constitutes a data breach
- how to report a data breach internally
- how to respond to a data breach

The Data Breach Guide also adopts a 4-step approach to responding to a data breach as follows:

- step 1 – contain the data breach to prevent further compromise
- step 2 – assess the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals
- step 3 – report the data breach to the PDPC and affected individuals
- step 4 – evaluate the organisation's response to the data breach incident and consider the actions which can be taken to prevent future data breaches.

Active enforcement

The PDPC has issued a guide on 22 May 2019 setting out a framework on how the PDPC will deal with data breaches ("Active Enforcement Guide").

When a report is received (which could be from the organisation or from the individual whose data has been compromised), the PDPC will decide whether to conduct an investigation. If there is no need to conduct an investigation it may either close the matter or it may refer the organisation and the individual to mediation.

If there is a need to investigate, the PDPC may nonetheless:

- suspend or discontinue the investigations
- accept an undertaking from the organisation in lieu of investigations
- issue an expedited decision without a full investigation.

The Active Enforcement Guide also addresses some of the powers that the PDPC has after carrying out an investigation and they are as follows:

- determine that there is no breach (after conducting the investigation)
- issue a warning
- issue directions
- impose financial penalties
- issue directions and impose financial penalties.

Accountability

The PDPC issued a guide on 15 July 2019 on accountability of organisations ("Accountability Guide") highlighting a shift from merely complying with the provisions of the PDPA to being accountable for ensuring that there is compliance with the provisions of the PDPA.

The Accountability Guide suggests "good practice" to consider and adopt data management practice in the areas of:

- policy
- people
- processes

Under "Policy" data protection is to be considered as part of a company's corporate governance policies and each organisation is to have a Data Protection Officer from the senior management of the company.

Under "People" all employees are to be involved in data protection and trained in data protection.

Under "Processes" all companies are to have effective processes dealing with the Personal Data from collection to disposal and how to ensure that Personal Data is not disclosed.

If there is a data breach, but if the organisation has adequate data management practices it is possible for the organisation to apply for an undertaking to be given or an expedited decision to be made instead of a full investigation. This would be a mitigating factor and is likely to result in lower penalties.

Notification

The PDPC issued a guide on 26 September 2019 on notification under the PDPA ("Notification Guide").

As stated earlier, under the PDPA there is a requirement to notify an individual of the purpose of collecting, using and/or disclosing the Personal Data and to obtain the consent of the individual before the Personal Data is collected.

Under the Notification Guide, an organisation is to give clear details to the individual about the organisation's purpose in the intended collection, use and/or disclosure of the Personal Data.

In addition to stating the purpose, an organisation is also to explain why it is necessary to collect, use and/or disclose the intended Personal Data.

If the Personal Data will be disclosed to third parties, the details of the Third Parties are to be given to the individual.

The individual is to be given an opportunity to actively give his consent and must also be notified that he may withdraw his consent at any time.

Under the Notification Guide, the individual is to be notified about the organisation's personal data protection policy and the names of persons in the organisation that would be able to address any queries about the policy.

Mitigation of cyber risk

The new rules will have an impact on most organisations in Singapore. Aside from the potential regulatory penalties imposed by the PDPC, a data breach can have serious financial consequences for businesses and cannot be ignored when implementing prudent risk management strategies.

There are a number of steps that organisations can take to mitigate their cyber risk. Many of these will be less expensive to implement than dealing with the potential fallout of a data breach. Examples of such measures include:

- ensuring that software is up to date on all computers
- training employees to recognise cyber risks
- limiting access to sensitive information
- restricting the use of personal emails and USB sticks
- securing the Wifi network
- preventing the use of unknown software
- monitoring for breaches of IT policy and potentially suspicious activity.

Cyber insurance is another key way that organisations can manage their risk. First party cyber insurance policies cover losses including business interruption, loss of data, theft and extortion. Third party cyber insurance policies cover the loss suffered by customers and third parties, as well as legal costs associated with defending claims. Many policies cover both types of losses.

Another potential risk mitigation strategy to consider is arranging access to a consolidated breach response service (such as RPC's ReSecure product). Following a breach, response services can provide professional support from forensic IT experts and specialist lawyers, limiting the potential consequences. These services are also offered as a benefit of certain cyber insurance policies. Please let us know if you would like further information regarding ReSecure or an introduction to cyber insurance brokers or insurers.

Contacts

Summer Montague
Senior Associate
+65 6422 3042
summer.montague@rpc.com.sg

Summer is a commercial disputes lawyer who focuses on insurance and reinsurance.

Summer specialises in resolving complex, cross-border insurance and reinsurance disputes arising from property, power generation, energy (onshore and offshore), mining and construction risks. She regularly advises in respect of Contractors All Risks, Erection All Risks and Delay in Start Up, PD/BI and construction professional indemnity policies.

She also has extensive experience advising on product recall policies and in handling product liability claims in Asia, Europe and the US, particularly in the technology, pharmaceutical and automotive industries. Summer advises on all aspects of claims, coverage issues and subrogated recoveries.

Summer has helped develop RPC's award-winning ReSecure cyber incident response service in Singapore and advise on legal issues arising from cyber security incidents, data privacy and complex IT claims (software and mobile technology) across the globe. More recently she has been working with several (re)insurers to help implement their cyber breach response offerings to clients and regularly advises on cyber policy coverage.

Summer is also experienced in International Arbitration and English High Court / Court of Appeal litigation and regularly monitors proceedings in multiple jurisdictions across Asia. She is a qualified mediator with the Singapore Mediation Centre.

Prakash Nair
Director
+65 6422 3061
prakash.nair@rpc.com.sg

Prakash is an experienced litigator having appeared as lead counsel in both domestic and international arbitration as well as in the Supreme Court of the Republic of Singapore and the Singapore International Commercial Court. Prakash has also appeared as counsel for criminal cases in the State Courts of the Republic of Singapore. Although his current focus is on commercial and marine work, Prakash also does work on matters relating to data breaches under Singapore's Personal Data Protection Act ("PDPA"), harassment under Singapore's Protection from Harassment Act ("POHA"), employment disputes, insolvency actions, land/tenant disputes, personal injury and property damage claims. Prakash also gives talks on a wide range of topics under Singapore law. As of late he has been focusing on talks on data breaches under the PDPA.

12 Marina Boulevard
38/F MBFC Tower 3
Singapore 018982
T +65 6422 3000

38/F One Taikoo Place
979 King's Road
Quarry Bay, Hong Kong
T +852 2216 7000

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000