BRIEFINGNOTE

STEPHENSON HARWOOD
(SINGAPORE) ALLIANCE

January 2020

Data protection in Singapore: Year in review

It has been five years since the coming into force of the main data protection provisions of the Personal Data Protection Act 2012 ("**PDPA**"). 2019 brought numerous changes to the data protection regime in Singapore, and at the start of the new year, it's time to take stock of where we're at with data protection laws.

Key updates to the data protection regime in 2019

1. Regulation of collection of NRIC numbers and other unique personal identifiers

In September 2019, a new set of advisory guidelines regulating the collection of NRIC numbers, other unique personal identifiers (collectively referred to as NRIC numbers) and physical NRIC cards issued by the Personal Data Protection Commission ("**Commission**") came into force. As an NRIC number is a permanent and irreplaceable identifier which can potentially be used to unlock large amounts of information relating to the individual, the collection, use and disclosure of an individual's NRIC number is of particular concern.

Under these guidelines, organisations are no longer allowed to collect, use or disclose NRIC numbers or copies of NRICs except: (1) as required under law; or (2) where collection, use or disclosure of NRIC numbers of NRICs is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity. As regards the second limb, the Commission has provided that it would generally consider collection, use or disclosure necessary in the following situations:

- where the failure to accurately identify the individual to a high degree of fidelity may pose a significant safety or security risk; or
- where the inability to accurately identify an individual to a high degree of fidelity may pose a risk of significant impact or harm to an individual and/or the organisation.

Do note that this list is not exhaustive.

> Organisations are therefore required to re-evaluate their collection, use and processing of any NRIC numbers or copies of physical NRICs, and consider if they fall within the scope of the exemptions.

If not, possible alternatives include collection of the last 3 digits of the NRIC number and the checksum (which the Commission does not consider to be collection of the full NRIC number), or collection of another type of personal information, such as an individual's handphone number or date of birth etc.

2. Update to guidelines on accountability obligation

Under the PDPA, organisations are generally required to be accountable for how it discharges its data protection obligations in relation to the personal data it collects or has control over.

The Commission has revised the accountability obligation guidelines to provide further guidance on the steps an organisation can take to meet this requirement. For example, organisations are currently required to appoint a data protection officer ("**DPO**") who will oversee the discharge of the organisation's data protection obligations. Under the new guidelines, the Commission has expanded on the role a DPO should play. For example, a DPO should work closely with senior management and the organisation's business units to develop and implement data protection policies. The DPO should also undertake a wide range of activities, which may include:

- producing (or guiding the production of) a personal data inventory;
- providing internal training on data protection compliance; and
- engaging with stakeholders on data protection matters.

The DPO should ideally also be appropriately trained and certified; e.g. the DPO may hold a Practitioner Certificate for Personal Data Protection (Singapore), which is co-issued by the Commission and the International Association for Privacy Professionals.

Under the revised guidelines, the Commission also recommends that organisations conduct Data Protection Impact Assessments ("**DPIAs**") in appropriate circumstances, and implementing a Data Protection Management Programme ("**DPMP**") to ensure that their handling of personal data is in compliance with the PDPA. This is further elaborated upon below.

3. Guidelines on active enforcement and managing data breaches

The Guide on Active Enforcement and the Guide to Managing Data Breaches 2.0 were released by the Commission on 22 May 2019.

The Guide on Active Enforcement details the Commission's investigative process and powers in relation to complaints it receives, and sheds light on the Commission's decision-making procedures. If the Commission decides to investigate a complaint, the Commission will first go through a fact-gathering process by giving notices to parties to produce information and documents, conducting interviews, and making site visits.

It also details the types of enforcement actions the Commission may take, which include:

- suspending or discontinuing the investigation;
- requiring the organisation in question to provide an undertaking;
- making an expedited decision where the organisation is prepared to identify the areas to which it is admitting liability and providing all relevant information; or
- conducting a full investigation process, which may result in the following decisions:
    - a determination that no breach occurred;
    - a determination that a breach occurred, and the issuance of a warning;
    - providing directions; or imposing financial penalties; or
    - providing directions and imposing financial penalties.

The Guide to Managing Data Breaches 2.0, which amends the earlier guide issued in 2015, provides guidance on steps an organisation should take in the event of a data breach. In particular, it outlines a process for notifying the Commission and/or affected individuals when the data breach is likely to result in significant harm or impact to the affected individuals or

the data breach is of a significant scale, which is defined as meaning where the breach affects the personal data of 500 or more individuals.

Based on this guide, the Commission should be informed as soon as practicable, and no later than 72 hours after it is established that the data breach is one that is likely to result in significant harm or impact or is of a significant scale. Data intermediaries should inform their client of a potential or confirmed data breach within a period of no longer than 24 hours.

4. Update to guidelines on notification obligation

Under the PDPA, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their valid consent to such collection, use or disclosure. The Commission has since revamped the guidelines on the notification obligation to clarify how exactly individuals should be properly notified of the purposes for which their data will be used.

Below is a list of factors that organisations should take into account when making notifications to individuals:

- **Audience**: Organisations should understand the demographic of the intended audience and tailor notifications to suit their profile. For example, simple language should be used if the service is targeted at children or youth.
- **Layout**: Key information that may be of particular concern to individuals should be expressly highlighted to them. Individuals should be able to locate the notification and corresponding terms and conditions easily.
- **Just-in-time notifications and dynamic consent**: Organisations should consider providing just-in-time notifications, where the necessary information is provided to individuals just before data processing takes place. This is particularly useful for more sensitive types of data such as health-related data. Individuals should also be given dynamic choices where possible at specific situations, rather than a single, all-or-nothing choice.

5. Update to guidelines on access requests

Under the PDPA, organisations are required to grant individuals access to personal data held about them by the organisation and information on how this data has been processed by the organisation in the preceding year, unless certain exemptions apply.

The Commission has updated the guidelines on access requests to provide further clarity on situations in which an exemption to this obligation would apply.

Briefly, an organisation may refuse to grant access in the following situations:

- an exception set out in the Fifth Schedule to the PDPA, applies, e.g. the personal data kept for evaluative purposes or relating to legal proceedings, or the access request is for information that is trivial;
- the individual has failed to pay the reasonable fees specified by the organisation to respond to the request;
- the personal data is necessary for any investigation or proceedings and has been disclosed to an authorised officer of a law enforcement agency; or

"Our team is well-situated to develop innovative, bespoke solutions to assist in planning and management of your internal compliance structure to avoid breaches of your regulatory obligations."

Sheetal Sandhu
Partner

- provision of access would: (a) reasonably threaten the physical or mental health of a third party; or (b) cause immediate or grave harm to an individual.

In relation to legal proceedings, the guidelines also clarify that where personal data has been collected prior to the commencement of prosecution and investigations but is nonetheless relevant to the proceedings, an individual should obtain access through criminal and civil discovery avenues rather than through the access obligation under the PDPA.

While no new exemptions to the access obligation have been introduced, the revised guidelines elaborate on how the exemptions apply and how an organisation should consider the purpose of an access request when responding to such requests.

6. Commission decisions and penalties

In 2019, the Commission cracked down on enforcement of the PDPA, and had by October 2019 issued more than S$1.3 million in data breach fines, a figure which exceeded the cumulative amount of fines meted out across the previous three years.

The highest financial penalties to date were imposed on Integrated Health Information Systems and Singapore Health Services for their failure to adequately secure patient data, amounting to a breach of their data protection obligations under the PDPA. They were fined S$750,000 and S$250,000 respectively.

The most common breaches the Commission acted on were breaches of the protection obligation, followed by breaches of the accountability obligation.

Under the PDPA, the protection obligation requires organisations to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, disposal or similar risks.

The sufficiency of the security measures undertaken would depend on, amongst others, the type of personal data collected, and the risks associated with the processing to be undertaken.

The accountability obligation requires an organisation to implement necessary policies and procedures in order to meet its obligations under the PDPA. Organisations are also required to make information regarding such policies and procedures publicly available. At the minimum, an organisation would need to:

- appoint an individual as its data protection officer, who will be responsible for ensuring the organisation's compliance with the PDPA; and
- enact a data privacy policy and standard operating procedures to regulate its processing of personal data.

Organisations that have breached the PDPA face penalties of up to S$1 million. Individuals who have breached the PDPA also face fines and imprisonment.

"With the rise of the digital era, there is an increasing need for laws to continually evolve to address data privacy and cybersecurity issues. It remains important for organisations to be fully aware of and compliant with their legal obligations in order to prevent lapses in their processes which may facilitate cybersecurity attacks and data leaks."

Kelly Pang
Associate

What's to come in 2020

With the increasing use of technology in nearly every facet of society, data protection is an area that will need to continuously evolve to keep pace with the needs of businesses and individuals.

The Commission has stated that it intends to keep abreast of international best practices, and to do so, updates to the legislation are required to align Singapore's regime with progressing international standards.

It is currently envisaged that amendments to the PDPA will be made in the course of 2020. Below are some of the key changes we can expect at this stage.

1. Mandatory breach notifications and single contact point for notifications.

Currently, there is no requirement for organisations to report breach incidents that occur. However, the Commission announced on 1 March 2019 that it intends to introduce a mandatory breach notification system as part of the upcoming amendments to the PDPA.

Additionally, the Public Sector Data Security Review Committee, a committee convened by the Prime Minister to conduct a comprehensive review of data security practices across the entire public service, also announced on 27 November 2019 that it intends to establish a single contact point for the public to report breaches. This is to streamline the incident-reporting process across agencies, and minimise confusion on where the public may lodge complaints on government data incidents.

The contact point is slated to be ready in the coming months, and will comprise a website and an email directly to the Government Data Office, which currently receives reports from government agencies on data incidents.

2. Third-party government vendors to be subject to the PDPA

The Commission has announced that third-party vendors handling government data and who misuse personal data will come under the PDPA, following amendments to the Act, which will likely be announced next year.

How we can help

We are well-versed with the workings of Singapore's data protection regime, and have advised numerous organisations on their data protection obligations. We have also conducted complete data protection audits on various international companies, through which we identify, assess and address gaps in their compliance regime.

If you are an organisation, we can assist with ensuring your company is fully compliant with all its obligations under the PDPA. Our capabilities include assisting with:

- the review of commercial agreements which concern or involve the processing of personal data by third parties to ensure you remain able to meet your obligations under the regime;
- drafting bespoke data protection policies (e.g. employee data policies and website policies) and standard operating procedures to address your organisation's obligations based on your business operations; and
- providing in-house training sessions to ensure your employees are fully cognisant of the practical steps they will need to take to maintain a robust data protection practices within the company.

Many Singaporean businesses are also subject to other data protection laws, such as the EU's General Data Protection Regulation ("**GDPR**"). Companies that breach the GDPR can be fined up to four percent of their annual global revenue or €20 million, whichever is higher. If your company is also required to comply with the GDPR, we are able to work with our dedicated London-based data protection team to provide advice on your GDPR obligations.

This article was written by partner Sheetal Sandhu and associate Kelly Pang at Virtus Law LLP (a member of the Stephenson Harwood (Singapore) Alliance). For more information, please do not hesitate to contact any of the team at Stephenson Harwood (Singapore) Alliance.

"The quality of service is very high. The team is responsive, commercial and we have seen a hands-on approach by partners, giving our clients a lot of confidence."

The Legal 500 Asia Pacific 2020

Get in touch

Sheetal Sandhu
Partner

T: +65 6661 6523
E: sheetal.sandhu@shlegalworld.com

Kelly Pang
Associate

T: +65 6661 6529
E: kelly.pang@shlegalworld.com

Tom Platts
Partner

T: +65 6622 9641
E: tom.platts@shlegal.com

Elaine Beh
Partner

T: +65 6661 6851
E: elaine.beh@shlegalworld.com

Dan Holland
Partner

T: +44 20 7809 2108
E: dan.holland@shlegal.com

Jonathan Kirsop
Partner

T: +44 20 7809 2121
E: jonathan.kirsop@shlegal.com

Stephenson Harwood is a law firm of over 1100 people worldwide, including 180 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with ten offices across Asia, Europe and the Middle East. In addition we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

The Stephenson Harwood (Singapore) Alliance (the "**Alliance**") is part of the Stephenson Harwood network and offers clients an integrated service in multi-jurisdictional matters involving permitted areas of Singapore law. The Alliance is comprised of Stephenson Harwood LLP and Virtus Law LLP. Court litigation services in Singapore are provided by the Singapore law firm, Virtus Law LLP.

© Stephenson Harwood LLP 2020 / Virtus Law LLP 2020. Any reference to Stephenson Harwood in this document means Stephenson Harwood LLP and/or its affiliated undertakings and/or the Stephenson Harwood (Singapore) Alliance. Any reference to a partner is used to refer to a member of the LLPs making up the Stephenson Harwood (Singapore) Alliance. Full details of Stephenson Harwood LLP and or/its affiliated undertakings can be found at www.shlegal.com/legal-notices.

STEPHENSON HARWOOD (SINGAPORE) ALLIANCE