HERBERT SMITH FREEHILLS

KEY CHANGES IN DATA PRIVACY AND CYBER SECURITY LAWS ACROSS SOUTHEAST ASIA IN 2022

22 November 2022 | Asia
Legal Briefings – By **Peggy Chow** and **Yeo Sue May**

2022 is a milestone year for data privacy and cyber security laws developments across Southeast Asia.

We set out the key changes as follows:

- The new Personal Data Protection Law in Indonesia became effective on 17 October 2022.
- Multiple data protection guidelines have been issued to supplement the Personal Data Protection Act in Thailand, which became fully effective on 1 June 2021.
- The draft Personal Data Protection Decree is still pending promulgation in Vietnam, while a new Decree 53 has been issued to provide guidance on the Cybersecurity Law.
- The draft data protection bill 2019 in India was withdrawn on 3 August 2022. It will be replaced by a new data protection bill which is expected to be presented to the Parliament in December 2022.[1]
- A recent Singapore court case has recognised distress as actionable loss and damage in a claim brought by a data subject. Further, the increased administrative fine of up to 10% of an organisation's annual turnover in Singapore (if annual turnover exceeds SGD 10 million) under the Personal Data Protection Act came into effect on 1 October 2022.
- Various privacy law reform proposals have been tabled for parliamentary discussion in

Malaysia. The proposals include mandatory breach notification (amongst other things).

- Novel approaches in determining fines under data privacy laws have been introduced in the Philippines.

INDONESIA

New data privacy laws in Indonesia

The long-awaited Personal Data Protection Law ("**PDPL"**) has been in place since October 2022. PDPL is Indonesia's first omnibus data protection legislation. Organisations will have a 2-year transition period to comply with PDPL.

All existing laws and regulations which regulate personal data protection will remain valid to the extent that they do not contradict the provisions of PDPL (including data localisation requirements under Government Regulations No. 71 of 2019 as data localisation is not dealt with under PDPL). We expect regulations providing guidance about key aspects of PDPL in coming months.

There are similarities and differences between PDPL and the EU General Data Protection Regulation ("**GDPR**"):

- PDPL adopts the concepts of "data subject", "data controller" and "data processor" and requires mandatory breach notifications to be made to authorities within 3 days (significantly shorter than the 14-day-period under the previous regime).

- The legal bases for processing personal data are similar to those under GDPR. In addition to consent from the data subjects, alternative legal bases include contract necessity, legal obligations, protection of the data subject's vital interest and controller's legitimate interest (among others). The availability of alternative legal bases is a significant departure from the previous regime, which required consent in almost all circumstances.

- The extra-territorial scope of PDPL is broader than under GDPR in the sense that it is not limited to certain triggering conditions. Personal data controllers and processors located outside of Indonesia must comply with PDPL if they process personal data in Indonesia and such processing has a "legal impact" on Indonesia or anyone in Indonesia. There is no guidance on what "legal impact" means under PDPL.

Exemptions from the application of PDPL are similar to those under other jurisdictions, e.g. where personal data is processed for personal or household purposes, and data processing activities for (a) the interests of national defence and security; (b) the interests of law enforcement process; (c) the public interest in the context of state administration; or (d) the interests of supervising the financial services, monetary, payment system sectors, and financial system stability carried out in the context of state administration.

The transfer mechanisms for cross-border data transfers are similar to those in other jurisdictions but are listed in order of priority as follows: (i) adequacy decision (i.e. comparable level of protection); (ii) binding contractual clauses on the overseas data recipient; and (iii) consent from data subjects. This is a significant relaxation from the previous system which require pre- and post-notification to the Ministry of Communications and Informatics. It remains to be seen if the regulator will issue model contractual clauses for (ii) under future regulations.

The new sanctions regime sets out a range of criminal and administrative fines of a range of magnitude depending on the nature of the violation. Criminal sanctions include fines of up to USD400,000 for individuals and USD4 million for corporations plus imprisonment of up to 6 years for individuals. Criminal sanctions may be imposed on the board of directors and beneficial owners of the companies. An offending party may be liable for administrative fines of up to 2% of its annual turnover. Through these sanctions the government is sending a strong message that personal data protection must be taken seriously in Indonesia.

Please refer to our full briefing.

THAILAND

Privacy Laws in Thailand coming together

Multiple guidelines with various effective dates have been introduced in Thailand since the main data protection provisions under the Personal Data Protection Act ("**PDPA**") came into full effect on 1 June 2021. Organisations in Thailand should consider the new guidelines to ensure that their data privacy practices remain compliant with the PDPA.

- The *Guideline on Requesting Consent from the Data Subject under the Personal Data Protection Act* B.E. 2562 (2019) ("**Consent Guideline"**) released on 7 September 2022 sets out detailed requirements for obtaining valid consent from individuals including timing and the information to be provided to the data subjects.

- The *Guideline on Procedures for Notifying the Purpose and Details relating to the Collection of Personal Data from Data Subjects under the Personal Data Protection Act.*

2562 (2019) ("**Notification Guideline"**) sets out the principles for organisations when providing notice to a data subject on how their personal data is processed.

- The *Notification re Exemption on Record-Keeping Duties of SMEs* ("**ROPA Guideline"**) sets out the minimum information that must be included on the ROPA records.

- The Office of Personal Data Protection Committee ("**PDPC"**) is currently undertaking a public hearing regarding its draft notification on cross-border transfers of personal data ("**Draft Notification"**) which will supplement the PDPA in respect of cross border transfers of personal data outside Thailand. The Draft Notification follows the approach of GDPR and sets out requirements in respect of binding corporate rules and other safeguards including standard contractual clauses, codes of conduct and certification. The hearing ran until 24 October 2022.

While there is a grandfathering provision under the PDPA which allows data controllers to continue processing personal data that was collected before 1 June 2021, data controllers are required to publicise channels by which data subjects can stop data controllers from doing so.

VIETNAM

Decree 53 finally provides some clarity on the Cybersecurity Law

Decree No. 53/2022/ND-CP ("**Decree 53"**), which took effect on 1 October 2022, clarifies some important aspects of the Law on Cyber Security No. 24/2018/QH14 (**"Cybersecurity Law "**), including the application of the data localisation requirements to Vietnam domiciled entities and foreign enterprises.

The criteria under the Cybersecurity Law and Decree 53 together provide that the data localisation requirements only apply to Vietnam domiciled entities that are: (i) service providers in the telecommunications network, internet or providing value added services in cyberspace; and (ii) processing personal data of Vietnam users, data about the relationship of users in Vietnam or data created by users in Vietnam. The domestic entity must retain such specified categories of data in Vietnam indefinitely. We understand from the Ministry of Public Security that it is possible to mirror such data in a local server and to keep a copy of the personal data outside of Vietnam.

For foreign enterprises, Decree 53 clarifies that such specified categories of data will need to be stored in Vietnam and a local presence needs to be established only where all of the conditions below are met:

1. the company operates in a prescribed sector related to the cyberspace, which means, amongst other things, telecom services, services for storing and sharing data in cyberspace, e-commerce and online payment services ("**Specified Services"**);

2. there is a violation of Cybersecurity Law in performing the Specified Services;

3. non-compliance with a notice or request from the Department for Cybersecurity and Prevention of High-Tech Crime ("**DCPHC"**); and

4. DCPHC issues a request for data localisation and local presence establishment.

The Cybersecurity Law requires domestic and foreign service providers to store user's data in Vietnam. This requirement has raised concerns from organisations due to its ambiguity including regarding the scope of data localisation requirements.

While Decree 53 is helpful in clarifying some aspects of the Cybersecurity Law, under Decree 53 a data subject's consent must always been obtained as there is no other alternative legal basis for processing their data. Further, Decree 53 does not contain any thresholds for notifiable data breaches, which means that all types of data breaches are notifiable to the PDPC.

INDIA

Are we expecting a complete overhaul of Indian data protection laws?

On 3 August 2022, India withdrew the personal data protection bill introduced in 2019. The scrapped bill had been considered by the Indian Parliament in significant detail with over 80 amendments and 12 recommendations proposed before the withdrawal. A new data protection bill is expected to be presented to the Indian Parliament for approval in December 2022.

Key areas of concern under the scrapped bill include the management of sensitive information and the scope of Indian Government's access to data.

SINGAPORE

(i) Emotional distress recognised as actionable loss and damage

The Singapore Court of Appeal has held that emotional distress may constitute actionable "loss or damage" under the Personal Data Protection Act 2012 ("**PDPA"**). In determining whether emotional distress is a form of loss or damage, the Court of Appeal in *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 found that a wider interpretation of the PDPA better promotes the purposes of the PDPA and that parliament intended for the enforcement regime of the PDPA to be an effective means by which individuals can enforce their rights to protect their personal data. The Court held that the loss of control of personal data would *not* constitute loss or damage for the purposes of the PDPA.

(ii) New administrative fine of up to 10% of an organisation's annual turnover in Singapore

The administrative fine for data breaches under the PDPA, which is up to 10% of an organisation's annual turnover in Singapore (if annual turnover exceeds SGD 10 million) took effect on 1 October 2022 pursuant to amendments set out in the Personal Data Protection (Amendment) Act 2020. Organisations will be potentially liable for fines for contraventions of the personal data protection requirements under the PDPA (excluding Part 9 and section 48B(1) of the PDPA).

MALAYSIA

Privacy law reform tabled for parliamentary discussion in Malaysia

Malaysia does not currently have a mandatory data breach notification requirement under its data privacy legislation, the Personal Data Protection Act 2010 ("**PDPA**"). Reforms to implement a mandatory data breach notification regime were tabled for parliamentary discussion in October 2022.

The proposed mandatory data notification regime was one of 22 recommendations in the PDPA public consultation paper published by the Personal Data Protection Commission ("**PDPC**") in February 2020.

The proposed mandatory data breach notification regime will require notifiable personal data breaches to be reported to the PDPC within 72 hours. The PDPC proposes to issue guidelines to assist organisations' compliance with this new mandatory notification requirement.

Other recommendations tabled for parliamentary discussion are reported to include: (i) imposing a direct obligation on data processors to comply with security principles under the PDPA; (ii) appointing a data protection officer; (iii) enshrining rights to data portability i.e. a data user should transfer personal data of a data subject to another data user in a user-friendly machine readable format at the request of the data subject (if technically feasible); and (iv) a 'blacklist' of jurisdictions for cross-border transfers of Malaysia (to replace the current prescriptive 'whitelist' system).

THE PHILIPPINES

Novel approaches in determining fines under data privacy laws

The recent introduction of the NPC Circular No. 2022-01 ("**Circular"**) on the *Guidelines on Administrative Fines* sees the Philippines adopting a novel approach in determining fines for breach of the Data Privacy Act 2012.

The Guideline sets out three categories of infractions namely: (i) grave infractions; (ii) major infractions; and (iii) other infractions. Infractions are categorised based on:

(a) the number of data subjects affected;

(b) frequency of the infractions; and

(c) reason for non-compliance (e.g. oversight, recklessness or intentional acts).

"Grave infractions" and "major infractions" carry an administrative fine linked to a certain percentage of the offender's annual gross income (i.e. 0.5% to 3% and 0.25% to 2% respectively). "Other infractions" are liable for a fine of between Php 50,000 (USD 870) and Php 200,000 (USD 3,500).

OUR ASIA DATA PRIVACY AND CYBER SECURITY PRACTICE

Herbert Smith Freehills' Asia data and cyber team is a regional practice focusing on data privacy, data security and cyber security issues across Asia.

We assist our clients in navigating the complex and evolving data privacy landscape and responding to the full gamut of data protection and cybersecurity issues and events. We work with our clients to come up with legally compliant and commercial solutions to address their data and cyber issues.

We advise on a whole spectrum of issues including privacy audit and gap analysis, data privacy law compliance covering cross-border jurisdictional issue, outbound data transfer, privacy documentation, strategic projects such as implementing privacy compliance programmes and scenario planning, as well as cyber incidents responses. We also advise our clients on data monetisation and data licensing documentation.

"Data Notes" is Herbert Smith Freehills' data know-how and news blog where you will find the latest legal developments worldwide on all things data, including data protection, privacy and cyber security.

1. After publication of our article on 14 November 2022, the new India draft data protection bill was released on 18 November 2022.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

MARK ROBINSON
PARTNER, GLOBAL CO-HEAD OF TMT SECTOR, SINGAPORE
+65 68689808
Mark.Robinson@hsf.com

CELLIA COGNARD
PARTNER, JAKARTA
+62 21 3973 6125
cellia.cognard@hsf.com

PEGGY CHOW
OF COUNSEL, SINGAPORE
+65 6868 8054
Peggy.Chow@hsf.com

SUE MAY YEO
ASSOCIATE (MALAYSIA), KUALA LUMPUR
+603 2777 5149
suemay.yeo@hsf.com

LEGAL NOTICE