Technology, Media & Telecommunications

Amendments to the Personal Data Protection Act to Take Effect in Phases Starting from 1 February 2021

Introduction

The Personal Data Protection (Amendment) Act 2020 ("**Amendment Act**"), which was passed in Parliament on 2 November 2020, is set to take effect in phases. On **1 February 2021**, the implementation of the amendments entered its first phase, with the first batch of amendments coming into operation.

The Amendment Act marks the culmination of a series of reviews and public consultations, and introduces a raft of changes to the Personal Data Protection Act 2012 ("**PDPA**"). The amendments seek to enhance the PDPA and strengthen organisational accountability and consumer protection, while giving organisations the confidence to harness personal data for innovation. This would be the first comprehensive review of the PDPA since its enactment.

In this Update, we highlight the changes in the Amendment Act which have taken effect in this first phase of implementation, and summarise the changes which have yet to come into operation.

For more information on the scope of the changes in the Amendment Act and the Advisory Guidelines on the amendments, please see our earlier Client Updates on "Amendments to the Personal Data Protection Act – Key Implications for Organisations in Singapore", available here, and "Draft Advisory Guidelines on the Key Amendments to the Personal Data Protection Act" available here.

Amendment Act

The Amendment Act aims to:

- Strengthen organisational accountability;
- Enhance consumer autonomy;
- Enhance effective enforcement; and
- Enable data use and innovation by organisations.

The first set of amendments have come into operation via the Personal Data Protection (Amendment) Act 2020 (Commencement) Notification 2021, which was gazetted on 29 January 2021. Accompanying regulations have also been introduced to support these amendments, including the following:

Technology, Media & Telecommunications

- Personal Data Protection Regulations 2021
- Personal Data Protection (Enforcement) Regulations 2021
- Personal Data Protection (Notification of Data Breaches) Regulations 2021
- Personal Data Protection (Appeal) Regulations 2021
- Personal Data Protection (Composition of Offences) Regulations 2021

To help organisations with compliance, the Personal Data Protection Commission ("**PDPC**") has updated the following resources:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act
- Advisory Guidelines on the Do Not Call Provisions
- Advisory Guidelines on Enforcement of Data Protection Provisions

First Phase of Changes

In this section, we highlight the amendments which have come into effect from 1 February 2021.

1) Organisational accountability

Mandatory breach notification

Under the new mandatory data breach notification system, once an organisation has credible grounds to believe that a data breach has occurred, it must take reasonable and expeditious steps to assess whether a data breach meets the criteria for notification.

Organisations which discover a data breach must notify the PDPC if the breach:

- is likely to result in significant harm to the individuals whose personal data is affected by the breach; or
- is of a significant scale (not fewer than 500 individuals).

Organisations must also notify the affected individuals once they have assessed that the breach is one that is likely to result in significant harm to said affected individuals.

Accountability principle

The amendments insert an explicit reference to accountability in Part III of the PDPA. This emphasises that organisations are accountable for personal data in their possession or under their control.

Technology, Media & Telecommunications

Mishandling of personal data

Organisations acting on behalf of public agencies are no longer excluded from the ambit of the Data Protection Provisions in relation to the collection, use and disclosure of personal data. New offences have also been introduced to hold individuals (including employees and service providers) liable for the knowing or reckless unauthorised handling of personal data, subject to certain defences and safeguards.

2) Consumer autonomy

Unsolicited messages

The system of control over unsolicited commercial messages under the PDPA and the Spam Control Act ("**SCA**") has been enhanced. The sending of unsolicited messages to telephone numbers through the use of dictionary attacks and address harvesting software will be prohibited under the PDPA's Do Not Call Provisions. The SCA has also been amended to cover commercial text messages sent in bulk and to Instant Messaging accounts (such as WhatsApp, WeChat and Telegram).

3) Enforcement

Voluntary undertakings

The PDPC has been empowered to accept and enforce voluntary undertakings from organisations in lieu of a full investigation. Organisations which are in breach of the Data Protection Provisions may voluntarily commit to take specified action or refrain from taking specified action in relation to the requirements, as well as to publicise the voluntary undertaking.

Alternative dispute resolution

The amendments establish a system of alternative dispute resolution to manage data protection complaints. The PDPC is empowered to direct complainants to resolve disputes via mediation, without the need to secure consent of both parties to the dispute, and to establish dispute resolution schemes for such purpose. Furthermore, the PDPC may compel the attendance of witnesses and the provision of documents and information, with non-compliance constituting an offence under the amended PDPA.

Do Not Call breaches

The amended PDPA will place Do Not Call breaches under a civil administrative regime, similar to that of data protection breaches. Egregious conduct such as the use of "robocalls" will be subject to higher financial penalties.

4) Data use and innovation

Business improvement exception

Subject to certain conditions, organisations may use personal data without consent for relevant purposes, including the improvement or enhancement of any goods or services, or methods or processes for operations, and for learning about and understanding customers' behaviour and preferences.

Research & development exception

The requirements for using personal data for research and development without consent will be eased, subject to certain conditions. Such conditions include requiring the use of personal data to have a clear public benefit, and that the results of the research will not be published in a form which identifies any individuals and will not be used to make any decision that affects the individual.

Legitimate interests exception

Organisations may collect, use or disclose personal data without consent where it is in the legitimate interests of the organisation or another person, and the legitimate interests outweigh any adverse effect on the individual. The organisation must, before relying on this exception, conduct an assessment to determine whether the specified requirements are satisfied. However, this exception does not apply to sending direct marketing messages to individuals.

Contractual necessity

Where personal data is provided to an organisation by a customer or potential customer, the organisation may rely on their deemed consent to disclose the personal data to its partners or contractors where reasonably necessary for the performance or conclusion of the contract with the customer (or potential customer). This recognises the multiple layers of outsourcing that is common today.

Changes Not Yet in Force

Some of the impending changes contained in the Amendment Act have not been included in this first phase of implementation. In this section, we highlight a couple of the notable changes which have yet to come into force.

1) Data portability

The Amendment Act contains a set of Data Portability provisions which provide an avenue for individuals with an ongoing relationship with an organisation to request for their personal data to be transmitted in accordance with prescribed requirements to a receiving organisation. The receiving organisation must be formed or recognised under the law of Singapore or a prescribed foreign country, or be resident or have a place of business in Singapore or a prescribed foreign country. The Data Portability obligation applies only to user data held in electronic form.

An organisation would not be required to transmit the personal data if it would be contrary to national interest, or would cause grave/immediate harm to or threaten the safety or physical/mental health of the requesting individual or any other individual. An organisation would also not be required to transmit the personal data if the request is frivolous or vexatious, if it would unreasonably interfere with their operations because of the repetitious or systematic nature of the request, or if the burden or expense of transmitting the data is unreasonable or disproportionate to the individual's interests.

2) Enhanced penalties

The Amendment Act provides for the increase of the maximum financial penalty for breaches of the PDPA Data Protection obligations, which is currently capped at S$1 million. When the enhanced penalty provisions come into effect, the maximum financial penalty will be increased to either (a) for organisations with annual turnover in Singapore of more than S$10 million - 10% of such turnover or (b) in any other case - S$1 million.

Currently, for a breach of the prohibition against the use of dictionary attacks and address-harvesting software, the maximum penalty is S$200,000 for individuals and S$1 million in any other case. When the enhanced penalty provisions come into effect, the maximum penalty for a person whose annual turnover in Singapore exceeds S$20 million will be increased to 5% of such turnover.

Concluding Words

The amendments to the PDPA demonstrate the PDPC's ability to recognise and account for advancements in technology and the proliferation of digital tools in the course of business and commerce. The PDPA is expected to continue to develop to keep pace with industry norms and practical realities.

Organisations should take note of the amendments that have come into force and ensure that their internal data protection and cybersecurity policies, training materials and the Data Protection Officers' roles and responsibilities guidelines are updated to be compliant with the amended PDPA.

Technology, Media & Telecommunications

We will continue to monitor the amendments to the PDPA for when the next phase of implementation will take place.

For further queries, please feel free to contact our team below.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications

T +65 6232 0752

lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade; Technology, Media & Telecommunications

T +65 6232 0298

tanya.tang@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

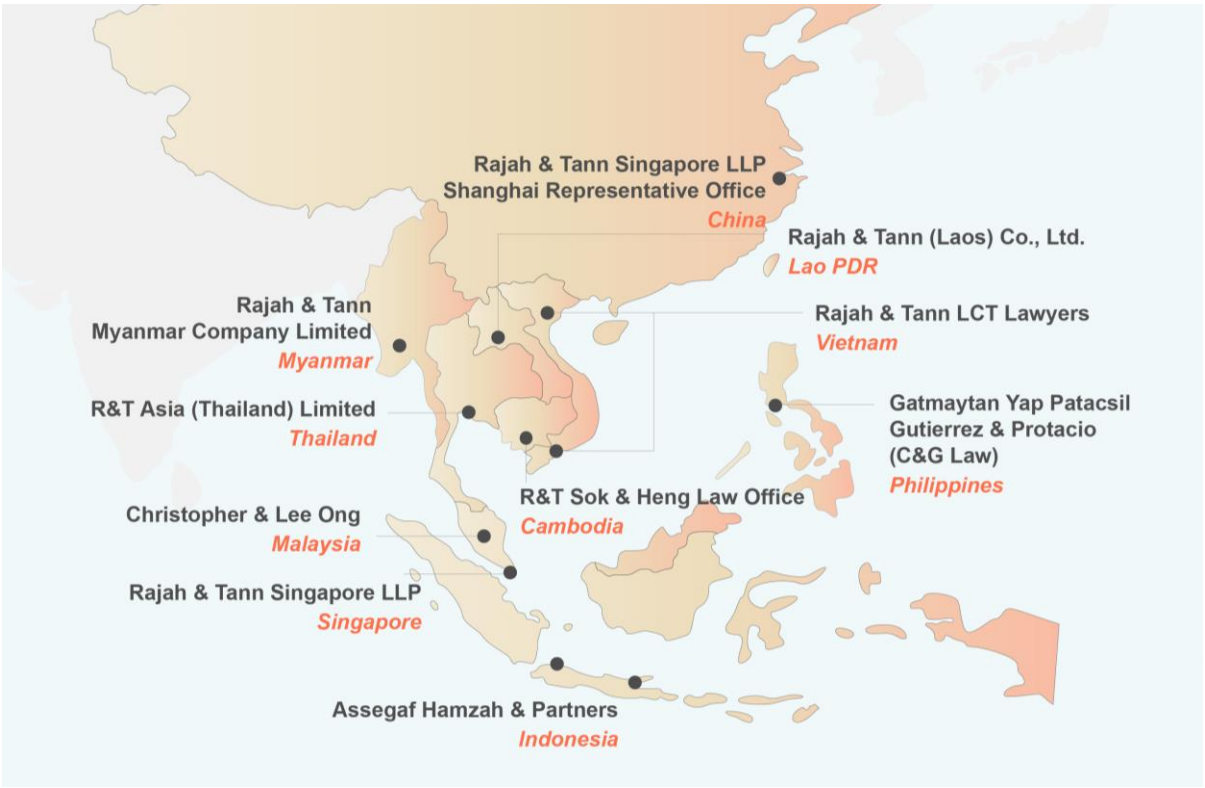
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.