Technology, Media and Telecommunications

PDPC Issues Response to Feedback Received from the Public Consultation on the Review of the PDPA

Introduction

On 1 February 2018, the Personal Data Protection Commission (the "**PDPC**") issued its response to feedback received from a public consultation ("**Public Consultation**") launched on 27 July 2017 on the review of the Personal Data Protection Act 2012 ("**PDPA**"). Please see here for our earlier Client Update on the Public Consultation.

This Update summarises the PDPC's responses and its new proposals to the feedback received.

Enhanced Framework for the Collection, Use and Disclosure of Personal Data

'Notification of Purpose' approach

The PDPC had considered in the Public Consultation whether notifying individuals of the purpose (**"Notification of Purpose**") can be an appropriate basis for an organisation to collect, use and disclose personal data where it is impractical to obtain consent. This was proposed to be subject to the following conditions:

(a) it is impractical for the organisation to obtain consent (and deemed consent does not apply) (the "**Impracticality Condition**"); and

(b) the collection, use or disclosure of personal data is not expected to have any adverse impact on the individuals ("**Adverse Impact Condition**").

Some concerns were raised by the public regarding the conditions required for the collection, usage and disclosure of personal data under the "Notification of Purpose" basis. Specifically, certain respondents raised concerns over the ambiguity of the Impracticality Condition (for example, whether organisations would be required to exhaust all avenues of contacting the individual before this condition is satisfied). Other respondents raised similar concerns regarding the ambiguity of the Adverse Impact Condition (for example, whether the collection, use or disclosure of personal data for marketing purposes would be regarded to have an adverse impact on the individual).

Having considered the feedback, the PDPC will remove the Impracticality Condition. However, the PDPC will retain (and rephrase to similar effect) the Adverse Impact Condition. The retention of the Adverse Impact Condition stems from the PDPC's original intent for introducing the Notification of Purpose basis; there may be situations where there is no foreseeable adverse impact on the individuals stemming from the collection, usage and disclosure of personal data provided the individuals have been notified of the purpose of such processing. The PDPC will be issuing guidelines to provide guidance on the Notification of Purpose basis.

Appropriate notification to be provided under the Notification of Purpose basis

The Public Consultation had also proposed that organisations seeking to rely on the Notification of Purpose basis would have to provide appropriate notification of the purpose of the collection, use or disclosure of the personal data. Where feasible, organisations would have to allow individuals to opt out of such collection, use or disclosure.

Clarifications were sought as to the mode of notification, and the thresholds for cost and difficulty at which it would be considered unfeasible to allow individuals to opt out.

However, in line with the approach for notifications under the PDPA's Notification Obligation, the PDPC has stated that the responsibility will be on organisations to assess and determine the most appropriate way of notifying individuals. Rather than specifying the appropriate means, the PDPC will instead provide further guidelines on the appropriate notification to be provided. The PDPC recognises the need to cater to circumstances where large volumes of personal data are instantaneously and seamlessly collected, and the difficulty in allowing individuals to opt out in such circumstances.

Revised consent framework to incorporate the Notification of Purpose basis

Section 15 of the PDPA currently allows the collection, usage and disclosure of personal data provided that an individual has expressly consented to it (the "**Actual Consent**"), or if an individual is deemed to have consented to such collection, usage and disclosure through his/her conduct (the **"Deemed Consent by Conduct**").

In addition to both the Actual Consent and Deemed Consent by Conduct requirements, the PDPC intends to provide for a new opt-out approach for organisations to fulfil the consent requirement under the PDPA. An individual would be deemed to have consented to the collection, use or disclosure of his/her personal data, provided that he/she is notified of the purposes of the processing of his/her personal data, and a reasonable time period to opt out is provided (where opt-out is feasible) to him/her. Where the individual does not opt out within the time period, there will be deemed consent by notification (the "**Deemed Consent by Notification**"). However, organisations may not rely on the Deemed Consent by Notification for direct marketing purposes, and organisations must obtain Actual Consent from the individual for such purposes.

Further, regarding the Deemed Consent by Notification, the PDPC has announced that organisations will be required to conduct a risk and impact assessment – such as a data protection impact assessment – as an accountability measure to ascertain whether the intended processing of personal data is likely to have any adverse impact on the individual.

Proposed Legitimate Interests Exception

During the Public Consultation, the PDPC noted that a "legitimate interests" basis was provided under the EU General Data Protection Regulation (the "**GDPR**") for the processing of personal data. Accordingly, the PDPC recognised that there are circumstances where organisations need to collect, use or disclose personal data without consent for a legitimate purpose not authorised under the PDPA or other written laws. Such collection, usage or disclosure would be subject to the following conditions:

(a) it is not desirable or appropriate to obtain consent from the individual for the purpose; and

(b) the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual.

Clarifications were sought by the public as to the definition of various terms in the conditions, such as "not desirable or appropriate to obtain consent". Respondents suggested that the PDPC should instead use the term "legitimate interests" and adopt the legitimate interest test used in the GDPR.

Having considered the feedback, the PDPC has decided that the "legitimate interests" test of the GDPR (the "**Legitimate Interests Exception**") should be adopted as a basis to collect, use or disclose personal data regardless of consent. The PDPC's intent is to enable organisations to collect, use or disclose personal data in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public, and such processing should not be subject to consent as the individuals may not provide consent in such circumstances.

Nonetheless, similar to the proposed Deemed Consent by Notification, the PDPC does not intend for the Legitimate Interests Exception to cover direct marketing purposes.

It is noted that the conditions in respect of the earlier "Legal or Business Purpose" approach will be retained for the Legitimate Interests Exception.

Moreover, the PDPC has proposed to impose accountability measures on organisations by requiring them to conduct a risk and impact assessment on the processing of personal data, similar to the proposed Deemed Consent by Notification.

Finally, the PDPC also intends to provide for an openness requirement to the Legitimate Interests Exception. This is similar to section 20(4) of the PDPA which requires organisations to inform individuals of the purpose of processing personal data when managing or terminating an employment relationship. Under this openness requirement, an organisation seeking to rely on the Legitimate Interests Exception will be required to:

(a) disclose its reliance on the Legitimate Interests Exception as a ground for collection, use or disclosure of personal data (for example, through the organisation's data protection policy which is made available to the public); and

(b) make available a document justifying the organisation's reliance on the Legitimate Interests Exception, and the business contact information of the person who is able to answer individuals' questions about such collection, use or disclosure on behalf of the organisation.

Proposed risk and impact assessment when the Deemed Consent by Notification or the Legitimate Interests Exception is relied upon

As mentioned earlier, the PDPC has proposed that organisations conduct and document a risk and impact assessment when the Deemed Consent by Notification or the Legitimate Interests Exception is relied upon.

However, due to the potential commercial sensitivity of such assessments, the PDPC will not be requiring these assessments to be made public. Nonetheless, the PDPC reserves the right to require organisations to disclose these assessments for the PDPC to determine if an organisation is in contravention of the PDPA.

Mandatory Data Breach Notification

Criterion for the mandatory reporting of a data breach

The PDPC had earlier proposed to introduce a mandatory data breach notification regime during the Public Consultation. The rationale provided was to ensure that notification practices are standardised across organisations, and for the PDPC to better oversee the level of incidences and management of data breaches at a national level. The PDPC had also noted in the Public Consultation that various jurisdictions have or are looking to introduce mandatory data breach notification in their legislation. These include Australia, Canada, New Zealand, the EU, the UK, and the US.

Additionally, the PDPC had proposed that organisations notify affected individuals and the PDPC when there is a breach that poses any risk of impact or harm to the affected individuals. Where the breach does not pose any risk of impact or harm to the affected individuals, but is of a significant scale (where there are 500 or more affected individuals), organisations would only be required to notify PDPC of the breach.

While the responses were supportive of the mandatory data breach notification, most of the respondents proposed that the PDPC adopt a consistent risk-based approach to avoid onerous regulatory burdens on organisations to report insignificant data breaches. Further, many of the respondents disagreed with the proposed threshold of 500 affected individuals as a criterion.

In consideration of the responses provided, the PDPC intends to retain and rephrase the criterion to "*likely to result in significant harm or impact to the individuals to whom the information relates*". This would allow affected individuals to take steps to protect themselves from risks of harm or impact from the breach, while minimising notification fatigue for individuals and regulatory burden on organisations.

Moreover, while the PDPC intends to retain the criterion of significant scale of breach, they will no longer prescribe a statutory threshold for the number of affected individuals.

The PDPC will be issuing guidelines on how organisations may assess the impact or harm caused by a data breach to individuals, and the scale of a data breach.

Time frame for notification

The Public Consultation also sought views on the proposed time frames for mandatory reporting. Having considered various responses, the PDPC has proposed to retain the time frames for notifications stated in the Public Consultation. Essentially, organisations are to notify affected individuals as soon as practicable, and to notify the PDPC no later than **72 hours** (the "**Required Time Frame**") after becoming aware of the breach.

The PDPC also recognises that organisations may require time to determine the veracity of suspected breaches, and has therefore proposed an assessment period of up to **30 days** from the day the organisation is first aware of a suspected breach (the "**Assessment Period**"). As noted by the PDPC, this is similar to Australia's notifiable data breaches scheme. Regardless of whether an organisation has fully utilised the Assessment Period, so long as the organisation has determined that the breach is eligible for reporting, the organisation must notify the relevant parties (the affected individuals and/or the PDPC) within the Required Time Frame.

The PDPC has also proposed similar requirements for data intermediaries. Such requirements would, in turn, be similar to requirements under the GDPR.

Exceptions to notify affected individuals

The PDPC has provided its response regarding the two exceptions (law enforcement exception and technology protection exception) to the notification of affected individuals which were proposed in the Public Consultation.

First, the PDPC has announced that the ambit of the law enforcement exception will be widened to include investigations which are carried out by authorised agencies. Specifically, organisations will not be required to notify affected individuals of an eligible breach as soon as practicable, if such notifications would impede ongoing or potential investigations under the law.

Next, the PDPC had also stated in the Public Consultation that organisations will not be required to notify affected individuals of an eligible breach as soon as practicable, if the breached personal data is encrypted to a reasonable standard. Such an exception would be similar to Article 34(3) of the GDPR. However, the PDPC has stated in its response that it intends to broaden the exception beyond technological encryption and make it technology neutral. Hence, the unauthorised collection, use or disclosure of personal data that has been encrypted may not constitute a data breach unless such data can be decrypted.

The PDPC also intends to provide a further exception for organisations which undertake remedial actions to reduce the potential harm or impact to the affected individuals.

Concurrent notification to PDPC and other regulators

The PDPC has stated that where an organisation is required to notify a sectoral or law enforcement agency of a data breach under other written law, and that data breach meets the criteria for notification under the PDPA, the organisation must notify both the PDPC and the other law enforcement agency based on the respective regulations. Organisations may however choose to report to the sectoral or law enforcement agency in the same notification format so as not to create unreasonable burden for organisations.

Going forward, the PDPC will explore mechanisms to streamline notifications to PDPC and relevant sectoral or law enforcement agencies.

Closing Comments

It is clear from the response to the Public Consultation that the PDPC recognises feedback that consent should not be the sole mechanism for organisations to collect, use and disclose personal data. The introduction of the Deemed Consent by Notification provides organisations with a separate basis by which they may collect, use and disclose personal data.

Nonetheless, the PDPC still intends for a balance to be struck between an individual's right to protect their personal data, and the right of organisations to collect, use and disclose such personal data. As mentioned, the PDPC removed the Impracticality Condition under the Deemed Consent by Notification basis. The Impracticality Condition would have been easily fulfilled by organisations seeking to rely on Deemed Consent by Notification, since the organisation collecting, using or disclosing the personal data would only need to demonstrate that it was impractical to obtain such consent from an individual. The requirement that an organisation must carry out a risk and impact

assessment before relying on the Deemed Consent by Notification basis also ensures that an individual is protected to a limited extent before his/her personal data is processed by the organisations.

Further, the adoption of the Legitimate Interest Exception is a welcome change. The new Legitimate Interests Exception is in line with the EU's GDPR approach. Organisations which have previously requested for the Legitimate Interests Exception to also apply in Singapore as a basis for the processing of personal data would approve of the PDPC's proposal.

The mandatory breach reporting notifications is also a timely development and would bring the PDPA in line with best practices in other jurisdictions. Specifically, many jurisdictions have already legislated, or are looking to legislate, mandatory breach notification. For example, the Privacy Amendment (Notifiable Data Breaches) Act 2017 was passed by the Australian Senate in February 2017, and will take effect on 22 February 2018. Similarly, the New Zealand Law Commission had in 2011 recommended mandatory reporting in its privacy law review, and a Cabinet Paper released in 2014 largely agreed with the recommendation. The PDPC's proposal would thus bring the PDPA in line with notification standards with other jurisdictions.

With these upcoming changes to the PDPA, and along with the recently passed Cybersecurity Act, there will be multiple reporting obligations. By way of an example, an owner of a critical information infrastructure (the "**CII**") as designated under the Cybersecurity Act may face a cyber-attack on its CII, which results in a data breach. Under the Cybersecurity Act, and the proposed amendments, the CII owner would be obliged to report to both the Cyber Security Agency of Singapore ("**CSA**") under section 14 of the Cybersecurity Act, and to the PDPC under the proposed mandatory data breach notification regime.

However, organisations should not be worried that these regulations will increase their administrative burdens substantially. The various agencies have stated that administrative processes, which amongst others would include reporting obligations, would be streamlined for organisations. As mentioned earlier, the PDPC has said that it will explore mechanisms to streamline notifications to relevant sectoral or law enforcement agencies. Further, the Minister for Communications and Information mentioned during the closing speech for the second reading on the Cyber Security Bill that the CSA has developed a Cybersecurity Legislation Initialisation Programme for Sector Leads (the "**CLIPS**"), to streamline incident reporting processes with other sector regulators (ostensibly, this would include the PDPC). The CLIPS will establish clarity on the roles and responsibilities between the various regulators. Such inter-agency coordination is necessary in order to unify reporting processes and to minimise administrative burdens on organisations should the aforementioned cyber breach occur.

For further enquires or discussion, please do not hesitate to contact our team below.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0751
F (65) 6428 2204
rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0786
F (65) 6428 2216
steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0752
F (65) 6428 2119
lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0738
F (65) 6428 2233
benjamin.cheong@rajahtann.com

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

D (65) 6232 0298
F (65) 6225 0747
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
F +65 6225 9630
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) Sole 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 NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 7304 0763 / +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 +632 894 0377 to 79 / +632 894 4931 to 32 / +632 552 1977
F +632 552 1978
www.cagatlaw.com

RAJAH & TANN | *Thailand*

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

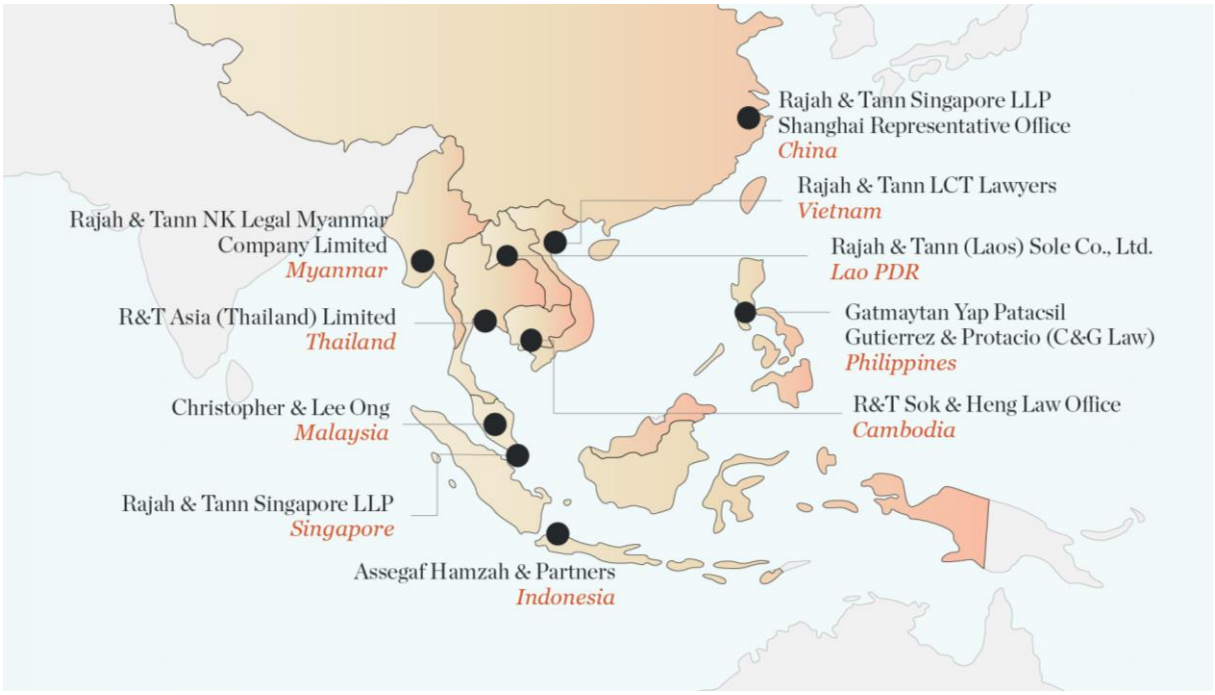
RAJAH & TANN LCT LAWYERS | *Vietnam*

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, Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.