Technology, Media, Telecommunications & Data Protection

Processing Personal Data in the Context of COVID-19 and the Movement Control Order

Introduction

In an effort to contain the COVID-19 pandemic, the Government of Malaysia extended the Movement Control Order ("**MCO**") until 14 April 2020 to contain the further spread of the virus. Organisations are, in turn, playing their part by taking steps to ensure the health and safety of their employees and clients, and the visitors to their premises. A key step being taken by the Government to contain the spread of the virus includes taking measures such as carrying out contact tracing of individuals who have contracted or are suspected to have contracted COVID-19.

The impact of these and other actions means that organisations may be faced with very real questions about their rights and obligations to collect, use and disclose personal data, both during and after the MCO.

Organisations will need to consider the possibility that their employees or the visitors to their premises might be infected with COVID-19 and if so, how this could potentially expose work colleagues or other parties to the infection. Until such time as a vaccine is created, organisations will need to continue to ensure the safety and welfare of their employees and clients, and the visitors to their premises, particularly after the MCO ends, when business resumes as usual.

From the data protection perspective, organisations may face immediate and very real questions such as:

(a) Can organisations collect personal data for purposes of contact tracing, or take other response measures?
(b) Where there are confirmed cases, is the organisation entitled to share or disclose information about the infected persons to the rest of the organisation or to any other third party?
(c) What are the obligations of the organisation in respect of personal data or sensitive personal data collected?

In this client update, we explore the possible legal grounds for the collection, disclosure and retention of personal data under the Personal Data Protection Act 2010 ("**PDPA**") in the context of the COVID-19 outbreak.

"Sensitive Personal Data" and the PDPA

In light of the COVID-19 outbreak, organisations may collect more information about individuals than they normally do, unaware that such data collection may exceed the scope declared in the organisations' existing privacy notices. Examples of information that may be collected include:

- whether individuals are displaying symptoms of the virus;
- the health status of individuals in the same household;
- results of COVID-19 testing, if any;
- locations visited;
- whether employees have self-isolated when unwell; and
- body temperature of personnel and visitors to premises.

The information above is considered to be "personal data" as defined by the PDPA, and insofar as the information relates to the individuals' health or physical condition, the information also falls within the sub-category of "sensitive personal data", which is subject to stricter compliance requirements as compared to "personal data".

Generally, organisations are only permitted to "process" (which is defined to include any set of operations on the data including the use, collection and disclosure of) sensitive personal data where:

(a) the individual in question has given his / her explicit consent; or
(b) the processing satisfies one of the prescribed conditions (i.e. exceptions) under the PDPA.

From the above, it is clear that organisations can process sensitive personal data collected in the context of the COVID-19 outbreak where the individual has provided his / her explicit consent (e.g. by way of a written declaration).

However, the follow-on questions which then arise are:

- What if the individual refuses to provide his consent?
- What if it is not possible or practicable to obtain the consent of the individual?
- Are there any legal grounds that an organisation can rely on in such cases?

Processing Sensitive Personal Data without Explicit Consent

(1) Processing for protection of "vital interests"

Section 40 of the PDPA provides that sensitive personal data may be processed without the individual's explicit consent, where the processing is necessary:

(a) to protect the vital interests of the data subject or another person, in a case where consent cannot be obtained from the data subject OR the data user cannot reasonably expect to obtain the consent of the data subject: section 40(1)(b)(ii) of the PDPA; or

(b) to protect the vital interests of another person, in a case where consent of the data subject has been unreasonably withheld: section 40(1)(b)(iii) of the PDPA.

"*Vital interests*" is defined by the PDPA to mean *"matters relating to life, death or security"*.

Arguably, processing personal and sensitive personal data in the context of the COVID-19 outbreak would fall under the scope of these provisions as it is a matter relating to an individual's life or death. However, the scope of the provision is unclear, and as of the date of this client update, there has been no statement issued by the Personal Data Protection Commissioner ("**Commissioner**") in this regard. In view of this, under circumstances where an employee or customer tests positive for COVID-19, and the organisation needs to immediately notify other employees or customers of this fact but is unable to obtain the consent of the infected person, we are of the view that such cases may fall within the scope of section 40 of the PDPA, and organisations may consider relying on such provision for the disclosure of personal data.

Please note, however, that this does not mean that the organisation has the right to disclose the identity of the infected person in reliance of the "vital interests" provision above. As far as possible, the identity of the infected individual should not be disclosed, unless it is absolutely necessary for the individual to be identified in order to protect the "vital interests" of other persons.

In situations which fall short of the above, e.g. where organisations collect information as a pre-emptive measure absent of any real "trigger" which necessitates such collection, it is open to question whether such processing would qualify as processing necessary for protection of the "vital interests" of data subjects.

(2) Processing in connection with employment

In respect of employees, section 40 of the PDPA further provides that sensitive personal data may be processed without the employees' explicit consent, where the said processing is pursuant to the

exercise or performance of any right or obligation conferred or imposed by law on the organisation in connection with employment: section 40(1)(b)(i) of the PDPA.

Again, the scope of the provision is unclear and there has been no statement issued by the Commissioner relating to this. While it is envisaged that this provision generally provides for instances where the employer is processing employees' sensitive personal data in compliance with its legal obligations in the context of the employment relationship (e.g. in compliance with revenue laws or social security laws; or pursuant to mandatory employment insurance requirements; etc.), it remains to be confirmed whether the provision can also be relied upon in the context of the COVID-19 outbreak.

Under the Occupational Safety and Health Act 1994 ("**OSHA**"), employers have a general duty to ensure the safety, health and welfare of all of their employees at work. This duty extends to (i) the provision of such information as is necessary to ensure the safety and health of employees at work; and (ii) maintaining a workplace in a condition that is safe and without risks to health, so far as is practicable: section 15 of the OSHA.

When processing personal data of employees in the context of the COVID-19 outbreak, employers may not be required to obtain the explicit consent of its employees where the employer is able to establish that the processing in question is pursuant to its legal obligation to ensure health and safety at work under the OSHA and / or any other obligation conferred on the employer in connection with employment.

Based on our reasoning above, considering that the relevant provisions are still open to interpretation in the context of the COVID-19 outbreak, and to minimise any non-compliance risk from the PDPA perspective, **the starting position for the organisation should always be to obtain the explicit consent of the individual to process his sensitive personal data**.

Only where consent is not forthcoming or it is being unreasonably withheld and the situation necessitates collection, use or disclosure of the information, should the organisation proceed to disclose the relevant information on grounds that such disclosure must be made to protect the vital interests of the data subject or other individuals, or that it was done in compliance with legal obligations in connection with employment.

Complying with the PDPA

Owing to the sensitive nature of the data collected and processed, it is imperative that organisations ensure that all personal data protection principles are complied with. In particular, organisations must take into account the following where processing personal data in the context of the COVID-19 outbreak:

(1) Data minimisation

The PDPA requires organisations to ensure that all processing carried out is adequate and not excessive in relation to the purpose for which the information is collected. As such, organisations must ensure that only such information as is strictly necessary for the purpose in question is collected.

Before collecting any information, organisations should have a clear purpose in mind as well as a clear understanding of what information is required, and the level of detail required to achieve this purpose.

For example, in the context of the COVID-19 outbreak, organisations collecting information for the purpose of making a decision whether an employee should work from home, should only ask relevant questions such as whether any person in the individual's household has recently travelled to identified jurisdictions, or is displaying any symptoms of COVID-19, and such questions should be framed for either 'yes' or 'no' responses instead of open-ended questions, to minimise the information collected.

(2) Purpose of processing

Organisations must ensure that the information collected is processed strictly for purposes related to the COVID-19 outbreak (e.g. for the purposes of contact tracing, contacting healthcare authorities, HR administration purposes), and that the information is not processed for any other unrelated purposes (e.g. disclosure to unrelated persons).

(3) Limit disclosures

When making disclosures about COVID-19 cases, disclosures should be restricted, as far as possible. In situations where it is not necessary to disclose the identity or other personal data of the individual, the disclosure may be made on an anonymous basis. Where it is necessary to disclose the identity of the individual, the individual should first be informed of the intended disclosure and (where possible) his explicit consent obtained.

Even if the individual has provided his / her explicit consent, organisations must ensure that the disclosures are made only on a "need to know" basis and not to exceed this perimeter.

(4) Data security and retention

Under the PDPA, organisations must have regard to the nature of the personal data and the harm that would result from any loss, misuse, unauthorised access or disclosure in respect of the same.

Bearing in mind the sensitivity of the information collected in this context, it is especially important for organisations to ensure that they have sufficient security measures to protect the information from any unauthorised or accidental access or disclosure, alteration or destruction.

Further, organisations should ensure that the information collected is retained only for as long as necessary. For example, where an individual has tested negative for COVID-19 and the relevant

incubation period for the individual has ended, the information collected should be deleted as soon as it is no longer needed. However, with the COVID-19 outbreak, organisations may be justified in retaining the information collected for longer as, in many cases, individuals who have initially tested negative and are asymptomatic can, when tested later, be established to be positive.

(5) Review and update privacy notices

Organisations should review existing privacy notices and where necessary, revise these to ensure that they cover any new data fields being collected in light of the COVID-19 pandemic, and the purposes for processing may need to be updated as well.

We trust that the above provides you with a quick analysis in relation to the PDPA. Should you require any assistance or clarification in respect of the above or in relation to any other aspect of personal data protection, please feel free to get in touch with us at your convenience.

For more articles and updates from our teams across the region on COVID-19 and related legal issues, please visit Rajah & Tann Asia's COVID-19 Resource Centre.

Contacts

Deepak Pillai
Head
Technology, Media & Telecommunications; Data Protection

T +60 3 2275 2675
F +60 3 2273 8310
deepak.pillai@christopherleeong.com

Intan Haryati Binti Mohd Zulkifli
Partner
Technology, Media & Telecommunications; Data Protection

T +60 3 2675 2674
F +60 3 2273 8310
intan.haryati@christopherleeong.com

Anissa Maria Anis
Partner
Technology, Media & Telecommunications; Media & Entertainment

T +60 3 2267 2750
F +60 3 2273 8310
anissa.anis@christopherleeong.com

Yong Shih Han
Senior Associate
Technology, Media & Telecommunications; Data Protection

T +60 3 2273 1919
F +60 3 2273 8310
shih.han.yong@christopherleeong.com

Michelle Wu
Associate
Technology, Media & Telecommunications; Data Protection

T +60 3 2273 1919
F +60 3 2273 8310
michelle.wu@christopherleeong.com

Lee Suke Mune
Associate
Technology, Media & Telecommunications; Data Protection

T +60 3 2273 1919
F +60 3 2273 8310
suke.mune.lee@christopherleeong.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

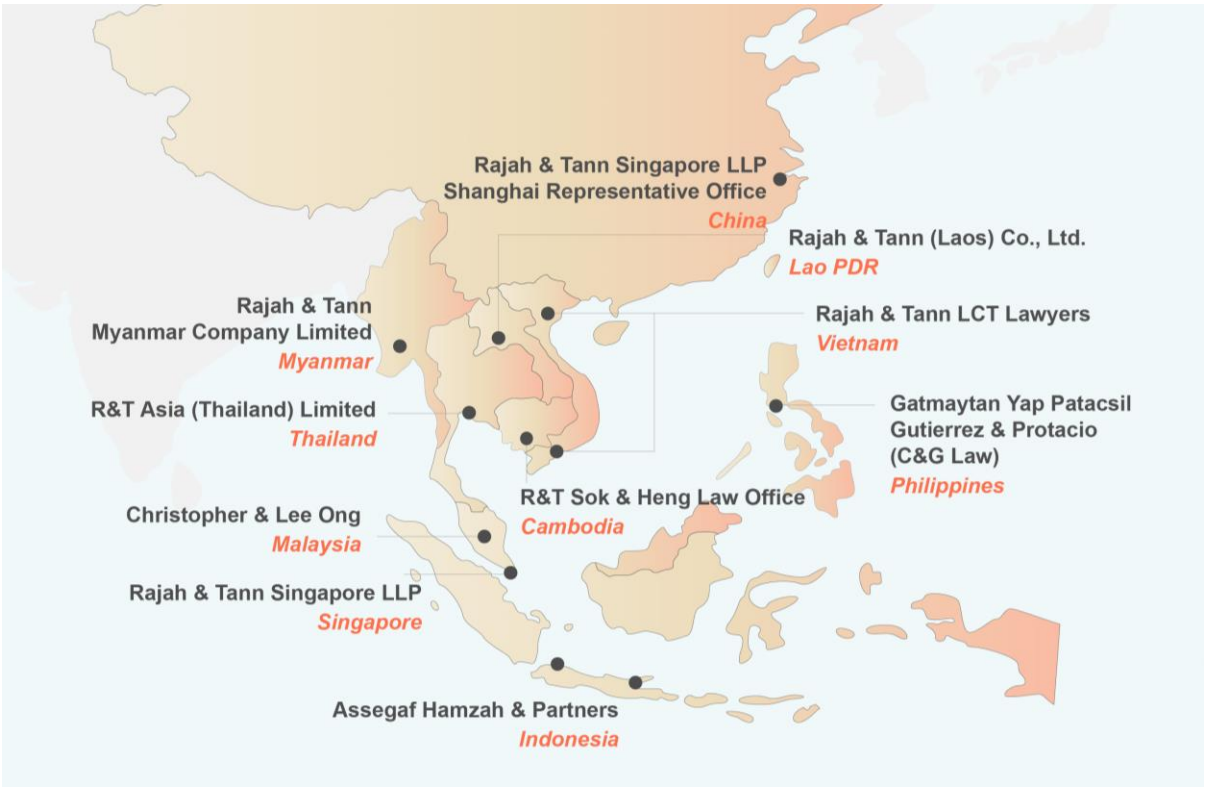
RAJAH & TANN LCT LAWYERS | *Vietnam*

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



Christopher & Lee Ong is a full-service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

Christopher & Lee Ong 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.