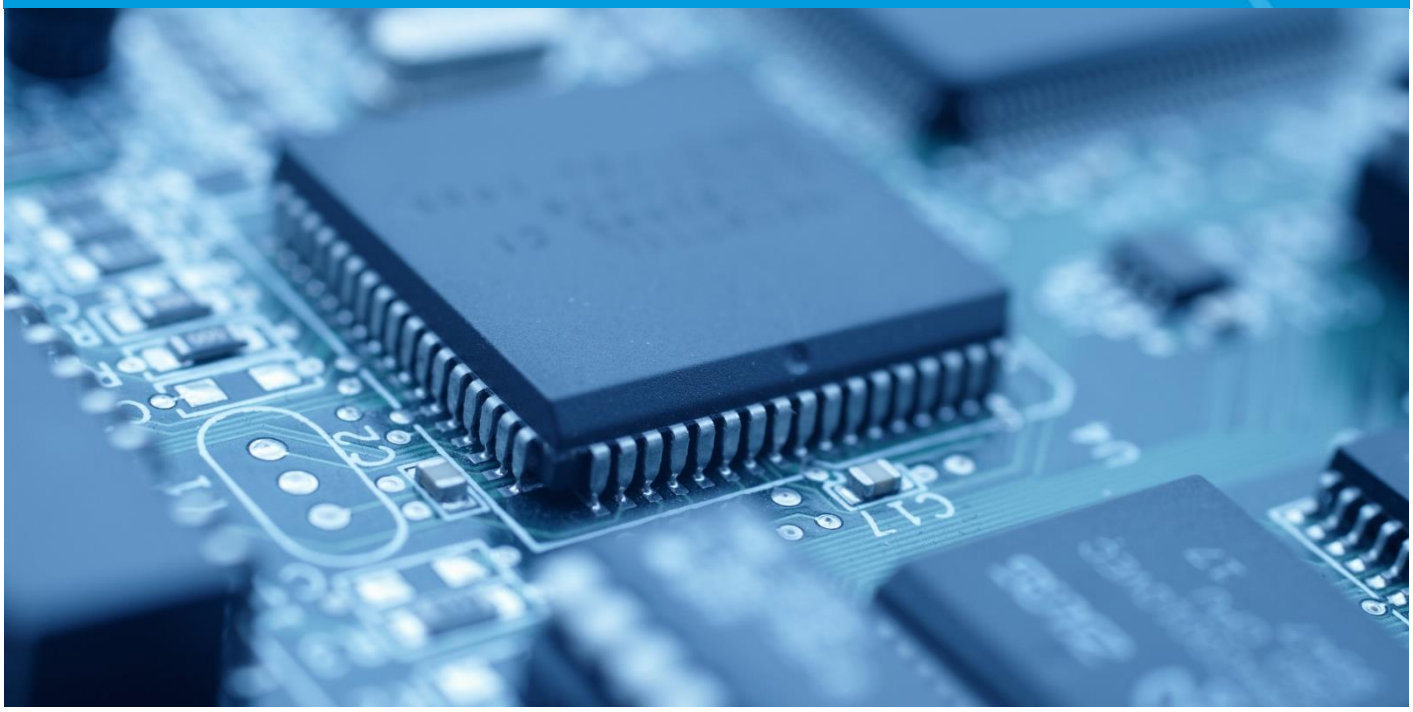
BRIEFINGNOTE

STEPHENSON HARWOOD (SINGAPORE) ALLIANCE

April 2020

COVID-19 series: Singapore updates

Data protection issues



As the COVID-19 situation continues to develop in Singapore, the laws and regulations governing businesses and their activities are constantly being updated to address business continuity and conduct issues. Businesses will need to stay abreast of these updates, and be mindful of ancillary issues that may arise from new measures being put in place.

This article is part of a series of updates aimed at providing a snapshot of issues that businesses should actively consider in the current climate. In this article, we will discuss data protection issues arising from the COVID-19 situation and provide insight to the measures organisations may implement to ensure compliance with the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**") during this period of heightened risk.

We recognise that organisations are currently under pressure to enact new measures as quickly as possible to address risks and meet business-as-usual needs, such as contact tracing measures and work-from-home arrangements. In doing so, organisations must remain cognisant of the data protection obligations which they are bound to comply with as there is no hiatus from compliance during this period.

COVID-19 contact tracing

Contact tracing is an important process through which the government keeps track of the number of active cases, identifies those at risk and curbs the spread of COVID-19. To maintain accurate records of persons who have entered specific premises, many organisations are currently collecting the personal data of visitors, such as their names, NRIC numbers, and contact numbers.

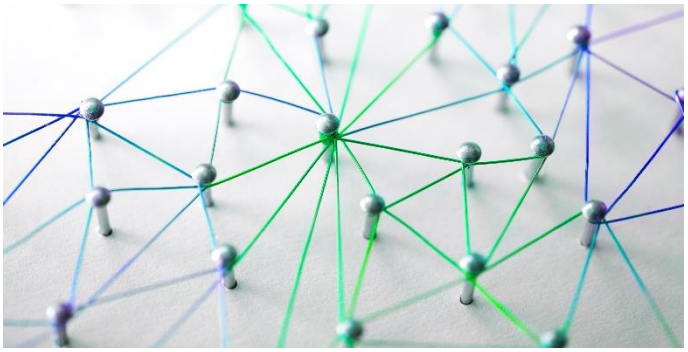
With the heightened safe distancing measures now in force from 7 April to 4 May 2020 ("**Circuit Breaker Measures**"), non-essential businesses have temporarily closed. However, contact tracing measures are still being implemented by essential service

providers which remain in operation. Keeping records of visitors will also be important in the coming months after the Circuit Breaker Measures fall away and non-essential businesses resume operations, as the need to continually trace and detect cases early will remain crucial to curbing the spread of the disease.

In relation to the PDPA, the question that arises is whether organisations may collect, use and disclose personal data for this purpose. We elaborate on some key pointers below.

Key points to note when collecting data for contact tracing

- **Emergency exemption**. The Personal Data Protection Commission ("**PDPC**") has clarified that organisations may collect personal data (including NRIC/FIN/passport numbers) from visitors to their premises where it is necessary to accurately identify such individuals for purposes of contact tracing and other response measures. In collecting, using and disclosing such personal data, organisations may rely on the emergency exemption available under the PDPA, as the collection, use and disclosure of the personal data is necessary to respond to the COVID-19 emergency. This therefore represents an exception to the usual consent regime.
- **Collect only relevant information**. Organisations should ensure that only necessary information is collected from visitors. For example, it may be reasonable for contact details, personal particulars and information regarding recent travel history to be collected. However, care must be taken to ensure that no non-essential information is collected.
- **Ensuring compliance with all other data protection obligations**. Notwithstanding the foregoing, organisations that collect personal data from visitors must continue to comply with the other data protection obligations under the PDPA. These include the obligation to protect personal data by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, and the obligation to cease retaining such personal data as soon as retention is no longer reasonably necessary for legal or business purposes.
- **Disclosure of data collected**. Organisations must be careful to prevent unauthorised disclosure of personal data. Records and personal data of visitors should not be disclosed except to authorised government bodies or other regulatory bodies. For example, organisations may disclose information to health officers appointed under the Infectious Diseases Act (Cap. 137 of Singapore) in order to aid the investigation of any suspected outbreak or prevent the possible spread of the disease.
- **Keeping personal data collected separate**. Organisations should take proper precautions to prevent the commingling of personal data collected pursuant to the emergency exemption with other personal data in its possession or control. This is to ensure that the personal data of visitors collected is not utilised for other purposes not relevant to the purpose of collection. For example, organisations should not add the personal contact details of visitors to recipient lists for marketing materials and/or send any non-essential communications unrelated to the COVID-19 situation to those persons.



Work-from-home arrangements

With the implementation of the Circuit Breaker Measures, most employees are now required to work from home as a matter of law. This brings about new challenges for organisations in relation to their data protection obligations under the PDPA, as remote working inherently carries with it a higher risk of compromised data protection and security. We elaborate on some of these risks below.

Compliance risks

- **Use of third-party technologies**. With employees working from home, organisations have resorted to third-party technologies to stay connected. These include telephone and video conferencing software, as well as remote working technologies. The use of third-party technologies (for example, Zoom) has recently raised security issues, as it is not clear how secure data

transferred through such applications is kept. Sensitive information may be leaked if the third-party software does not offer a sufficient level of security, which may cause detriment to the parties involved.

- **Use of personal devices.** Employees working from home are also more likely to access personal data belonging to the company on their personal devices, especially if company laptops are not issued to them. If these personal devices are not fitted with appropriate security protections such as antivirus software and firewalls, they are more prone to security breaches and malware attacks, which may compromise both personal and work-related information. Even where laptops are issued to employees, it may be difficult for employers to ensure these devices remain fitted with updated protections.
- **Amplified business-as-usual risks.** While working from home, business-as-usual risks are amplified as personal data may be more easily exposed to people who are not employees of the organisation, such as family members or partners living in the same household. These risks may be difficult to manage, especially in respect of employees living with large families, or in smaller living areas.
- **Increased cybersecurity threats.** There has been a surge in COVID-19 themed cyberattacks and phishing emails perpetrated by actors seeking to exploit the sense of heightened fear and general weakened cybersecurity resulting from people working from home *en masse*. These threats typically come in the form of emails asking the reader to activate a link, which will trigger the download of malicious software.

As mentioned above, the PDPA's security obligations continue to apply during this period. Organisations will therefore need to enhance their data protection standards to ensure they remain commensurate with the aggravated security threats in the wake of the COVID-19 situation. Businesses should consider the security measures being adopted for homeworking with the aim of ensuring that personal data remains protected to the standard required under the PDPA.

Suggested measures to combat the risks

To address the shift towards the remote working model, below are some measures businesses may consider adopting.

- **Up-to-date data protection policies.** Organisations should update their policies on data protection to ensure that they address any new risks that arise as result of the alternative working arrangements. Organisations should also provide guidance to employees on how best to reduce these risks, including additional steps employees can take to safeguard personal data in their care or control.
- **Communicating risks to employees.** Organisations should ensure effective communication to employees so that they are aware of new or heightened security risks, and how to identify and address them. To encourage employees to stay vigilant, organisations may consider providing a list of frequently asked questions to pre-empt and address any concerns relating to measures being implemented. Virtual training seminars may also be provided to employees who handle a high volume of information, or who work with highly sensitive information.
- **Communications regarding infections.** If there is a need to communicate any news on infections within the organisation to employees, this should be done in a respectful manner. Care must be taken to ensure that any personal data of the affected employee which is disseminated to the firm as a whole is limited to necessary and relevant information only.
- **Providing IT support and enhancing IT protections.** As far as possible, organisations should also endeavour to continue providing IT support to identify and address security issues, and additionally consider implementing additional IT protections as necessary. Potential measures that can be adopted include two-factor authentication for remote access applications, encryption of devices, and requirements for employees to install mandated security software and/or utilise virtual private networks when accessing organisations' drives or documents.

  Organisations may also want to consider enhanced email-specific controls in the short term to minimise the risk of email cybersecurity attacks, such as strengthening password policies, developing a response system, and implementing automated email warning reminders in respect of emails received from external sources.

For organisations with a presence in the EU, or whose businesses target EU citizens, our London team has prepared a similar summary of what you need to know in relation to the General Data Protection Regulation 2016/679, accessible here.

Each week, new legislative and regulatory developments arise, resulting in further implications for businesses. This article has identified and addressed pertinent data protection issues arising from the COVID-19 period.

This article was written by 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. We remain committed to assisting our clients during this challenging period.

Get in touch

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

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

Parikhit Sarma
Partner
T: +65 6661 6528
E: parikhit.sarma@shlegalworld.com

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

George Cyriac
Partner
T: +65 6622 9692
E: george.cyriac@shlegal.com

Kelly Pang
Associate
T: +65 6661 6529
E: kelly.pang@shlegalworld.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.

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