APRIL:

Data Privacy in the Covid-19 Pandemic

TAY & PARTNERS

As the Covid-19 pandemic continues its scourge, the Malaysian government imposed a two-week movement control order ("**MCO**") that has subsequently been extended for another month, which restricts the free movement of the people. This includes the prohibition of mass gatherings, restrictions on overseas travel for Malaysians, and entry for foreign visitors as well as the closure of schools, government and private premises except those involved in essential services. Written police permit is required for interstate travels. The Royal Malaysian Police and subsequently the Malaysian Armed Forces, including personnel and drones were mobilized to enforce the order. Unprecedented in peacetime, Malaysia became the first South East Asian country to put its citizens under restricted movement to slow the rate of infection for as long as possible and so alleviate the burden on its healthcare system while protecting those most at risk.

Prior to the MCO, beleaguered businesses had already reacted by implementing work from home and other commercially feasible social distancing measures. Armed with hand sanitizers and 3-ply surgical masks, Malaysians braved the threat of infection to attend to daily affairs which for most was going to work. A purposeful stroll into workplaces had been replaced with long queues for temperatures checks and recording of personal details. "Now Everyone Can Fly" became veritably muted as declaration of travel history, contact tracing, travel restrictions and self-isolation and finally closure of borders of several countries affected travel plans. Social media platforms were awashed with photo uploads of people being health screened, names of infected individuals and their workplace were being freely shared. Information was being collected and processed in the name of containment of the virus. As Malaysia and much of the world continues to grapple with the virus, data privacy and its vulnerability becomes heavily tested. The following focuses on the use and sharing of personal information of employees, contractors and visitors by employers in the face of the Covid-19 pandemic.

APRIL:
Data Privacy in the Covid-19 Pandemic

TAY & PARTNERS

1. Are there any specific guidelines for the processing of personal data in the context of the Covid-19 outbreak?

There are yet to be any specific guidelines from the Malaysian Personal Data Protection Commissioner on the lawful processing of personal data on the Covid-19 pandemic. Businesses are to adhere to the Personal Data Protection Act 2010 ("PDPA").

The Ministry of Health has issued guidelines to event organizers to keep a record of the contact details of all participants for at least one month from the date of completion of the events. They are required to assist the Ministry of Health who carry out contact tracing and placing close contacts under home surveillance where participants are infected. The guidelines are here.

2. What type of personal data is typically being processed during the Covid-19 outbreak?

Apart from personal data such as basic identity, contact details, location information and travel history and information of close contacts, health status, body temperature measurement and medical condition which are sensitive personal data are also being processed. Sensitive personal data is subject to more stringent and additional safeguards under the PDPA.

3. May employers conduct temperature screening for employees, contractors and visitors?

Yes. Employers may collect body temperature readings of employees, contractors and visitors to protect the safety and health of individuals at the workplace as required under the Occupational Safety and Health Act 1994 ("OSHA").[1]

Such information constitutes sensitive personal data which may be collected without explicit consent to comply with the legal obligations under the OSHA or to protect the vital interests (i.e. life, death or security) of their employees, contractors, visitors and others where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld. [2]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[3]

4. May employers collect information about travel history of employees, contractors and visitors?

Yes. Employers may collect information about travel history of employees, contractors and visitors to protect the safety and health of individuals at the workplace as required under the OSHA.[4] Further, employers are encouraged to obtain travel declaration from employees pursuant to the guidelines issued by the Ministry of Health.[5]

Such information may be collected without consent of their employees, contractors and visitors to comply with the safety and health obligations imposed on the employers.[6] It is also possible to invoke the exception of protecting their vital interests (i.e. life, death or security) to dispense with the consent requirement.[7]

---

1 Occupational Safety and Health Act 1994 (OSHA), s 15 and s 17.
2 Personal Data Protection Act 2010 (PDPA), s 40(1)(b)(i), 40(1)(b)(ii) and s 40(1)(b)(iii).
3 PDPA, s 7.
4 OSHA, s 15 and s 17.
5 Ministry of Health, Covid-19: Management Guidelines for Workplaces (24 March 2020), accessible at http://www.moh.gov.my/moh/resources/Penerbitan/Garis%20Panduan/COVID19/Annex_25_COVID_guide_for_workplaces_22032020.pdf.
6 PDPA, s 6(2)(c).
7 PDPA, s 6(2)(d).

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[8]

5. May employers collect information about symptoms of employees, contractors or visitors?

Yes. Employers may collect information about symptoms of employees, contractors and visitors to protect the safety and health of individuals at the workplace as required under the OSHA.[9] Further, monitoring symptoms of employees at workplace is one of the safety measures recommended for adoption by employers under the guidelines of the Ministry of Health.[10]

Such information constitutes sensitive personal data which may be collected without explicit consent to comply with the legal obligations under the OSHA or to protect the vital interests (i.e. life, death or security) of their employees, contractors, visitors and others where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld.[11]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[12]

6. May employers request employees, contractors or visitors to notify them if the latter is diagnosed?

Employers may request employees to notify them if the employees are diagnosed by having such requirement as part of the health and safety measures in the HR policy of the organization.[13] Employees are bound by legal duties to cooperate with employers to comply with such measures including the notification requirement.[14]

Contractors and visitors may be required by an organization to notify to prevent or contain the spread of the virus among employees and other individuals at the workplace pursuant to the OSHA.[15]

Such information constitutes sensitive personal data which may be collected without explicit consent to comply with the legal obligations under the OSHA or to protect the vital interests (i.e. life, death or security) of their employees, contractors, visitors and others where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld.[16]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[17]

---

8 PDPA, s 7.
9 OSHA, s 15 and s 17.
10 Ministry of Health (n 5).
11 PDPA, s 40(1)(b)(i), 40(1)(b)(ii) and s 40(1)(b)(iii).
12 PDPA, s 7.
13 OSHA, s 16. It requires employers to formulate a safety and health policy and bring the policy to the notice of all employees.
14 OSHA, s 24.
15 OSHA, s 15 and s 17.
16 PDPA, s 40(1)(b)(i), 40(1)(b)(ii) and s 40(1)(b)(iii).
17 PDPA, s 7.

APRIL:
Data Privacy in the Covid-19 Pandemic

TAY & PARTNERS

7. May employers notify others of any employee, contractor or visitor who is infected or suspected of being infected?

Yes. It would be prudent for employers to disclose information of any employee, contractor or visitor who is infected or suspected of being infected, only to other individuals who have come into contact with the employee, contractor or visitor who is infected or suspected of being infected if this is necessary to prevent or contain the spread of the virus among employees and other individuals at the workplace pursuant to the OSHA.[18]

Such information involves the identity and health status (i.e. whether infected or suspected) of the infected or suspected persons which constitute personal data and sensitive personal data, respectively. Employers may collect and subsequently disclose the personal data to the other individuals without consent for compliance with the safety and health obligations imposed on the employers.[19]

Similarly, the sensitive personal data may be collected and subsequently disclosed to the other individuals without explicit consent to comply with the legal obligations under the OSHA or to protect the vital interests (i.e. life, death or security) of the individuals where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld.[20]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of personal data and sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[21]

If the purpose is not covered in the relevant notices, the information may still be disclosed to the other individuals as the disclosure is required or authorized by the OSHA.[22]

8. Are employers required to disclose personal data of their employees, contractors or visitors to the authorities pursuant to a request by them?

Yes, and three provisions cover this requirement:-

- Section 22I of the Prevention and Control of Infectious Diseases Act 1988 ("**PCIDA**") which criminalizes the refusal to furnish any information required for the purposes of the PCIDA or any regulations made thereunder;

- Regulation 6 of the Prevention and Control of Infectious Diseases (Measures Within the Infected Local Areas) Regulations 2020 and Regulation 9 of the Prevention and Control of Infectious Diseases (Measures Within the Infected Local Areas) Regulations (No. 2) 2020 (collectively, "**PCIDR**") which mandate compliance with the request of an authorized officer for any information relating to prevention and control of the infectious disease throughout the 14-day period of the MCO and the extended MCO, respectively; and

- Section 46 of the OSHA which requires employers to provide assistance to occupational safety and health officers ("officers") as they may require for any entry, inspection, examination or inquiry in respect of a place of work or for the exercise of their duty thereunder.

---

18 OSHA, s 15 and s 17.
19 PDPA, s 6(2)(c).
20 PDPA, s 40(1)(b)(i), s 40(1)(b)(ii) and s 40(1)(b)(iii).
21 PDPA, s 7. 22 PDPA, s 39(b)(ii).
22 PDPA, s 39(b)(ii).

Accordingly, where there is a request by the health authorities or the officers for personal data of an employee or a visitor for investigation or contact tracing purpose, employers are bound by the legal obligations under the PCIDA, the PCIDR and the OSHA to assist and cooperate with them and to comply with their respective requests.

This ultimately means that employers are allowed to collect and subsequently disclose the information to the health authorities and the officers without consent to comply with the legal obligations under the PCIDA, the PCIDR and the OSHA.[23]

Sensitive personal data may be collected and subsequently disclosed to the health authorities and the officers without explicit consent to comply with the legal obligations under the PCIDA, the PCIDR and the OSHA or to protect the vital interests (i.e. life, death or security) of their employees, contractors, visitors and others where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld.[24]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of personal data and sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[25]

If the purpose is not covered in the relevant notices, it is still possible to disclose the information to the health authorities without consent relying on the exception that the disclosure is required or authorized by the PCIDA, the PCIDR and the OSHA.[26]

Further, notice to the individuals may be exempted for the collection and disclosure of their information to the health authorities on the basis that the information is being processed for research purposes to identify, test and isolate the affected persons in order to stem the spread of the virus, and not for any other purpose, provided the identity of the affected persons are not disclosed. [27]

9. What about whistle-blowing? Are employers required to notify the authorities of any employee or contractor who is infected or suspected of being infected?

No. Employers are not obliged to do so under the PCIDA and the PCIDR. However, if the Covid-19 virus is classified as an occupational disease28, employers will be required to notify the nearest occupational safety and health office.[29]

In most cases, except for healthcare services, the Covid-19 virus is not an occupational disease as a pathogen is typically not a hazard associated with the nature of work in the course of one's employment. Therefore, there is no obligation on employers to notify the occupational safety and health office.

Having said that, it would be prudent for employers to notify the health authorities of any employee, contractor or visitor who is infected or suspected of being infected to prevent or contain the spread of the virus among employees and other individuals at the workplace pursuant to the OSHA.[30]

---

23 PDPA, s 6(2)(c).
24 PDPA, s 40(1)(b)(i), 40(1)(b)(ii) and s 40(1)(b)(iii).
25 PDPA, s 7.
26 PDPA, s 39(b)(ii).
27 PDPA, s 45(2)(c).
28 Occupational Safety and Health (Notification of Accident, Dangerous Occurrence, Occupational Positing and Occupational Disease) Regulations 2004 (OSHR), r 2(1). It defines "occupational disease" as a disease arising out of or in connection with work and is of a class specified in Schedule 3. According to Paragraph 7 of Schedule 3, an illness caused by a pathogen is an occupational disease if the work involves a pathogen which presents a hazard to human health. Covid-19 would be an occupational disease in the health sector.
29 OSHA, s 32; OSHR, r 7(1). 30 OSHA, s 15 and s 17; PDPA, s 40(1)(b)(i). 31 PDPA, s 6(2)(c) and s 6(2)(d).
30 OSHA, s 15 and s 17; PDPA, s 40(1)(b)(i).

The information may involve the identity and health status (i.e. whether infected or suspected) of the infected or suspected persons which constitute personal data and sensitive personal data, respectively. Employers may collect and subsequently disclose the personal data to the health authorities without consent for compliance with the safety and health obligations imposed on the employers or to protect the vital interests (i.e. life, death or security) of the infected and suspected persons.[31]

Similarly, the sensitive personal data may be collected and subsequently disclosed to the health authorities without explicit consent to comply with the legal obligations under the OSHA or to protect the vital interests of the infected and suspected persons and others where the consent cannot be given by them, cannot be reasonably obtained by the employers or is unreasonably withheld.[32]

Nevertheless, employers must ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of personal data and sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.[33]

If the purpose is not covered in the relevant notices, the information may still be disclosed to the health authorities as the disclosure is required or authorized by the OSHA.[34]

10. How long may the personal data processed for the purpose of Covid-19 containment be retained?

The personal data may be retained for as long as is necessary for the containment of the Covid-19 and should be permanently deleted or removed when the Covid-19 outbreak is over.[35]

Despite these challenging and uncertain times, organizations should be mindful of their obligations under the PDPA when processing personal data of individuals.

With the exponential growth in the number of infected individuals, there has been an increasingly large amount of personal data, including sensitive personal data, being processed and transmitted between organizations and the health authorities, urging the need to strengthen data security measures and the exercise of data minimization. Any improper handling or unlawful use of the personal data may expose organizations to the risk of a fine and/or a term of imprisonment for breaching the PDPA which is far more painful than social distancing.

Global demand for data security continues to grow with emerging technologies being deployed across the world in a race against time to trace and track close contacts of infected persons. The contact tracing efforts bear witness to the scale of mobile apps and electronic tracking devices sprouting up across Asian countries such as China[36], South Korea[37], Hong Kong[38], Taiwan[39] and Singapore[40], for instant contact tracing, facilitating strict enforcement of quarantine and alerting users of a possible exposure.

---

31 PDPA, s 6(2)(c) and s 6(2)(d).
32 PDPA, s 40(1)(b)(i), s 40(1)(b)(ii) and s 40(1)(b)(iii).
33 PDPA, s 7.
34 PDPA, s 39(b)(ii).
35 PDPA, s 10.
36 BBC News, 'China launches coronavirus 'close contact detector' app' (11 February 2020), accessible at https://www.bbc.com/news/technology-51439401.
37 Ivan Watson and Sophie Jeong, 'Coronavirus mobile apps are surging in popularity in South Korea' CNN Business (Seoul, 28 February 2020), accessible at https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html.
38 Zoe Low, 'Covid-19: inbound travellers from Europe, US to be issued Bluetooth quarantine wristbands at Hong Kong airport' South China Morning Post (25 March 2020), accessible at https://www.scmp.com/news/hong-kong/society/article/3076994/coronavirus-inbound-travellers-europe-united-states-will-be.

APRIL:

Data Privacy in the Covid-19 Pandemic

TAY & PARTNERS

With the shift of the epicenters westwards towards the United States of America and Europe, countries such as the United Kingdom[41], Ireland[42] and Germany[43] following the Asian experience, had announced initiatives to develop similar contact-tracing apps. In Europe, pan-European mobile tracking app that is compliant with the European Union's data protection laws is being explored to facilitate contact tracing within its countries and across borders.[44]

In Malaysia, the *MySejahtera* mobile app was recently introduced by the Ministry of Health in collaboration with the National Security Council (NSC) and Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), to assist the government in monitoring, managing and mitigating the Covid-19 outbreak by collecting data from citizens through health self-assessments.[45]

While digital contact tracing has proven effective in slowing the spread of the virus, appropriate security measures must be incorporated to protect the personal data of users against cybersecurity threats.

---

39 Yimou Lee, 'Covid-19: Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring' Reuters (Taipei, 20 March 2020), accessible at https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK.

40 Fathin Ungku, 'Singapore launches contact tracing mobile app to track coronavirus infections' Reuters (Singapore, 20 March 2020), accessible at https://www.reuters.com/article/us-health-coronavirus-singapore-technolo/singapore-launches-contact-tracing-mobile-app-to-track-coronavirus-infections-idUSKBN2171ZQ.

41 Hannah Devlin, 'NHS developing app to trace close contacts of coronavirus carriers' The Guardian (31 March 2020), accessible at https://www.theguardian.com/uk-news/2020/mar/31/nhs-developing-app-to-trace-close-contacts-of-coronavirus-carriers.

42 Credit RSS, 'Ireland to roll out voluntary phone tracker app to tackle coronavirus' Reuters (Dublin, 29 March 2020), accessible at https://www.reuters.com/article/health-coronavirus-ireland/ireland-to-roll-out-voluntary-phone-tracker-app-to-tackle-coronavirus-idUSL8N2BM0GR.

43 Douglas Busvine, 'Germany aims to launch Singapore-style coronavirus app in weeks' Reuters (Berlin, 30 March 2020), accessible at https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-aims-to-launch-singapore-style-coronavirus-app-in-weeks-idUSKBN21H26Z.

44 Foo Yun Chee, 'EU privacy watchdog calls for pan-European mobile app for virus tracking' Reuters (Brussels, 6 April 2020), accessible at https://www.reuters.com/article/us-health-coronavirus-tech-privacy/eu-privacy-watchdog-calls-for-pan-european-mobile-app-for-virus-tracking-idUSKBN21O1KJ.

45 Qishin Tariq, 'Govt launches pilot project to monitor spread of Covid-19 pandemic via app' The Star (6 April 2020), accessible at https://www.thestar.com.my/tech/tech-news/2020/04/06/govt-launches-app-to-monitor-spread-of-covid-19-pandemic.

The foregoing has been prepared for the general information of clients and friends of the firm. It is not meant to provide legal advice and should not be acted upon without legal advice. If you have any questions or require any further information regarding these or other related matters, please contact us.

LEE LIN LI
Partner, Head of IP & Technology Practice Group.

For further information and advise on this article and/or on any areas of IP & Technology, please contact:
linli.lee@taypartners.com.my

CHONG KAH YEE- Associate
kahyee.chong@taypartners.com.my