

FAQs on hot topics under PDPA and Employment Laws relating to the 2019 Novel Coronavirus (2019-nCoV)

These FAQs provide a general indication of how the Personal Data Protection Act 2012 (**PDPA**) and employment law may apply in relation to the collection, use and disclosure of personal data from visitors and employees as a result of an organisation's 2019-nCoV (officially named COVID-19 by the World Health Organisation on 11 February 2020) response measures. Organisations should consider how best to comply with the requirements of the PDPA, employment law and other control measures in general based on their particular needs. For advice on specific matters or situations, please contact Drew & Napier LLC.

Data Protection-specific issues

Consent and Notification

- 1. Q: Do I need to obtain consent to collect, use or disclose personal data (e.g. body temperature, contact details, travel history, etc.) of the visitors to my office/building?**

A: Consent (and any related notification of purposes) is not required under the PDPA for personal data collected in an anonymised form. For example, where temperature taking is done at the entrance to premises to confirm that individuals entering the premises do not have a fever and no records are kept of specific individuals' temperatures, consent is not required.

However, if personal data relating to specific individuals will be collected and retained by an organisation, for example, contact information collected for the purpose of contact tracing, consent would be required unless otherwise provided under written law.

In particular, under the PDPA, organisations may collect, use and disclose an individual's personal data without their consent where necessary in response to an emergency that threatens the life, health or safety of the individual or another individual (the **Emergency Exception**). The Personal Data Protection Commission has noted that the Emergency Exception applies in relation to personal data collected for contact tracing and other 2019-nCoV response measures.

Organisations which collect personal data pursuant to the Emergency Exception should note that they cannot use or disclose such data for other purposes unless consent is obtained from the individuals concerned or any other exception under the PDPA or any other written law applies. For example, under the Infectious Diseases Act (Cap. 137), there are broad powers for the Director of Medical Services to, *inter alia*, require the furnishing of information or to conduct surveillance or tracing of individuals.

- 2. Q: When do I need to notify individuals before I collect their personal data?**

A: Notification under the PDPA is not required for collection of personal data in an anonymised form or where collection is pursuant to the Emergency Exception or any other provision of written law. Nevertheless, as individuals may wish to know when their personal data is being collected by organisations, and the purposes for which such data are collected, organisations may wish to provide some notification to individuals when they do so.

3. **Q: How can I notify individuals and/or obtain their consent? Do I need to make visitors sign a consent form, or put up a signage at a prominent location before collecting their personal data?**

A: The PDPA does not specify the form or content of notifications to individuals. In general, organisations should state their purposes for the collection of personal data.

In relation to the 2019-nCoV situation, such notifications may be as simple as having a signage to indicate “Temperature checks” or “Collection of Contact Information for Contact Tracing” (or similar wording) at a suitable location at the entrance or lobby of premises.

Organisations which may be collecting more personal data, for example, health declarations or employee data, may wish to provide more information to the individuals concerned about their purposes for collecting the information in question.

4. **Q: What can I do if a visitor refuses to provide their contact details or travel history, or refuses to allow us to take their temperature?**

A: In general, the PDPA does not prevent organisations from making provision of personal data by individuals a condition of their entry into the organisation’s premises.

For the purposes of contact tracing and other response measures to the 2019-nCoV situation, it may be reasonable for organisations to require personal data to be provided by visitors as a condition of entry to the organisation’s premises. If visitors refuse to provide the requested information, the organisation may then deny entry to such visitors.

However, organisations should be mindful that they should not over-collect personal data and only collect data which is necessary to respond to the 2019-nCoV situation.

5. **Q: As an employer, do I need consent to collect my employees’ personal data, for example, when establishing “work-from-home” or other arrangements?**

A: Under the PDPA, employers may collect, use and disclose personal data of their employees without their consent if the collection, use or disclosure is reasonable for the purpose of managing or terminating the employment relationship. However, the PDPA requires employers to first notify their employees of the purposes for such collection, use or disclosure of personal data.

Where an organisation requires personal data from its employees in relation to its 2019-nCoV response measures, for example, establishing telecommuting or working from home arrangements, it may be reasonable for employers to rely on this exception to collect the personal data from employees without requiring their consent.

Access to Personal Data

6. **Q: Can individuals request for access to their personal data collected by an organisation?**

A: In general, under the PDPA, individuals may request for access to their personal data which is in the possession or under the control of an organisation. Upon request, an organisation shall, as soon as reasonably possible, provide the individual with such personal data (and certain other information), unless otherwise provided under the PDPA or any other written law. Further, there may be specific situations under the law where access is prohibited.

As a practical measure, if an individual requests for access to their personal data, the organisation should take care to ensure that it does not inadvertently reveal the personal data of other individuals when providing the access to the individual.

Protection of Personal Data

7. Q: How should I store the personal data collected?

A: Under the PDPA, regardless of whether consent was required for the personal data collected, organisations must provide reasonable security arrangements to protect personal data in their possession or under their control. The PDPA does not prescribe a “one size fits all” solution, and it is up to each organisation to adopt security arrangements that are reasonable and appropriate in the circumstances.

If the personal data is collected and stored in electronic form, organisations should ensure that there are appropriate technical measures in place to protect the personal data.

If the personal data is collected and stored in physical format, organisations may consider adopting physical measures such as storing confidential documents in locked file cabinets, and properly dispose of confidential documents by shredding them when they are no longer required.

Organisations may also adopt administrative measures, such as ensuring that staff are trained to handle personal data and that there are policies and procedures in place to maintain confidentiality of the personal data.

Retention of Personal Data

8. Q: For how long can I keep the information collected?

A: Under the PDPA, organisations must cease to retain personal data as soon as it is reasonable to assume that the personal data no longer serves the purposes for which it was collected, and there are no longer any other legal or business reasons for retention of the personal data.

In view of the present 2019-nCoV situation, organisations may wish to retain personal data collected through their 2019-nCoV response measures until it is reasonably clear that such data is no longer required, for example, if the DORSCON status returns to green. Depending on further developments in the present 2019-nCoV situation, organisations may wish to assess the necessity of retaining the personal data on an ongoing basis.

Employment-specific issues

9. Q: What happens when an employee refuses to attend work because of the 2019-nCoV situation?

A: Apart from employees who are subject to a quarantine order or a mandatory leave of absence, employers may generally determine their response to such refusals to attend work by employees in accordance with the terms and conditions of their employment contract, or company policy on absenteeism, medical or hospitalisation leave and/or annual leave (where applicable).

In light of the 2019-nCoV situation, employers may consider the adoption of business continuity measures such as work-from-home options for employees.

10. Q: Can I prevent an employee from visiting a 2019-nCoV-affected area or country?

A: Apart from business travel situations which are within the control of employers, and specific terms and conditions of an individual's employment contract, employers do not have a general right to restrict their employees from travelling outside of work to 2019-nCoV-affected areas or countries. However, to ensure the safety and health of their employees and for contact tracing and other response purposes, it may be reasonable for employers to require their staff to provide travel declarations and/or advance notification of plans to travel to 2019-nCoV-affected areas or countries.

11. Q: Can I apply for or renew work passes for employees from 2019-nCoV-affected areas or countries?

A: With effect from 31 January 2020, the Ministry of Manpower will reject all new work pass applications for foreign workers from mainland China until further notice. However, renewal applications for existing work pass holders will not be affected.¹

12. Q: Can I direct my employees to see a doctor?

A: While employers do not have a specific right to direct employees to seek medical advice, it may be reasonable for employers to take such measures as part of their statutory duty to ensure the safety and health of their employees,² especially if their employees have plans to visit or have previously visited 2019-nCoV-affected areas or countries.

13. Q: Can I direct my employees to stay at home and take unpaid/annual leave?

A: In general, employers should discuss with their employees (and union representatives, if any), and mutually agree on the appropriate leave and flexible work arrangements (e.g. paid/unpaid annual leave) to be adopted.³

¹ <https://www.mom.gov.sg/newsroom/press-releases/2020/0131-update-on-additional-measures-by-mom-to-minimise-the-risk-of-community-spread>

² Section 12 of the Workplace Safety and Health Act (Cap. 354A).

³ <https://www.mom.gov.sg/faq/haze/can-employers-ask-employees-to-take-annual-leave-if-the-company-closes-or-operations-have-stopped-due-to-the-haze-situation>

14. Q: Can I direct my employees to work from home?

A: Where appropriate, employers may, as part of their business continuity measures, direct their employees to work from home.

Should you have any queries on the above or if you require any assistance at all, please do not hesitate to contact:

Lim Chong Kin Tel: +65 6531 4110
Managing Director, Corporate & Finance
Co-Head, Data Protection, Privacy & Cybersecurity Practice
Head, Technology, Media and Telecommunications
Head, Competition, Consumer & Regulatory
Email: chongkin.lim@drewnapier.com

Benjamin Gaw Tel: +65 6531 2393
Director
Technology, Media and Telecommunications
Employment
Email: benjamin.gaw@drewnapier.com

David Alfred Tel: +65 6531 2342
Co-Head,
Data Protection, Privacy & Cybersecurity Practice
Email: david.alfred@drewnapier.com