DATA PRIVACY, COLLECTION AND TRANSFER OF EMPLOYEE DATA - WHAT EMPLOYERS MUST KNOW AMIDST THE CORONAVIRUS (COVID-19) OUTBREAK

Posted on February 17, 2020

Categories: CNPupdates, Covid-19 Resource

Date Published: 17 February 2020

Authors: Wong Pei-Ling and Lorraine Liew.
Contributors: Susannah Dobbie and Joel Chew.

Ever since the World Health Organisation declared the outbreak of the novel coronavirus (COVID-19) a global health emergency, the world has reported more than 70,000 cases and the death toll has surpassed 1,700, with 75 confirmed cases in Singapore (as at 16 February 2020). The Singapore government has remained vigilant in setting up multiple lines of defences to contain the virus and to prevent further spread amongst residents. Local organisations are also to be applauded for their efforts to obtain health and travel declarations from employees for the purposes of contact tracing. However, potential data privacy issues in the collection, use or disclosure of employee information may arise.

Are you collecting personal data through your employees' health declarations?

Unless collected anonymously, health and travel declarations collected from the employees of private organisations would constitute personal data.

The requirements that organisations need to observe in the collection of personal data

Generally, organisations will need to obtain consent from the individuals whose personal data are to be

collected. However, in light of the purpose of preventing the spread of COVID-19, the Personal Data Protection Commission ("PDPC") has issued an advisory on the collection of personal data for contact tracing and other response measures, which specifically states that relevant personal data can be collected, used and disclosed without consent during this period as it is necessary to respond to an emergency that threatens the life, health or safety of other individuals.

Nevertheless, this exemption does not absolve organisations from the obligations in Parts III to VI of the Personal Data Protection Act 2012 ("PDPA"). Organisations must take care to ensure that the personal data collected will only be used or disclosed for reasonable purposes. However obvious, these purposes should be notified to their employees.

Upon collecting the information, reasonable efforts should be taken to ensure that the data is accurate, complete and also well-protected to prevent unauthorised access, use, disclosure, modification to the information or any such similar risks. Employees must be given access to their personal data if requested, and they have the right to make any corrections to the personal data. Once retention of the information is no longer needed for any legal or business purposes, the employer is to remove possession of the data completely.

Finally, the employer is responsible for undertaking the relevant measures to demonstrate that it can meet the above obligations, and should be open to disclosing information about its protection practices to authorities.

Will the personal data be transferred across borders?

During this period, multinational corporations may more likely transfer employee health and travel information between their offices in different countries. A transfer across borders would necessarily involve a higher level of restriction over and above transfers within Singapore, even if the recipient is an affiliated organisation.

Outbound transfer of personal data from Singapore

Generally, unless specifically exempted by the PDPC, organisations may only transfer personal data outside Singapore if they have taken appropriate steps to:

- ensure compliance with the various sections of the PDPA (i.e. Parts III to VI of the PDPA) while the personal data to be transferred remains in their possession; and
- ascertain and ensure that the overseas recipient is bound by legally enforceable obligations to provide a standard of protection comparable to that of the PDPA in Singapore.

One measure would be that the transferring organisation must obtain informed consent from the individual whose personal data is to be collected and transferred. The individual must be given a reasonable summary (in writing) of the extent to which his personal data (which is to be transferred), will be protected to a standard comparable to that under the PDPA. The individual's consent has to be freely given and not

procured by using deceptive or misleading practices, or required as a condition of the organisation's service, unless it is reasonably necessary to the provision of the service.
However, in the specific scenario of the overseas transfer of employee health information for purposes of prevention of the spread of COVID-19, the "*health and safety emergency*" exemption under the PDPA is likely to apply and the transferring organisation is deemed to have satisfied the transfer requirements so long as the transfer is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual and the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose.
In this regard, a transferor should ensure that personal data is transmitted securely and also that the transferee has agreed to only use the data for the limited purpose and to destroy such data after a reasonable period, *for example* - two to four weeks.

Inbound transfer of personal data into Singapore

Where personal data from overseas is transferred into Singapore, Parts III to VI of the PDPA will similarly apply. Additionally, organisations may be subject to the data protection laws of the country or territory where the personal data was collected.

Data protection regimes of neighbouring jurisdictions

Since both outbound and inbound transfers of personal data will likely require local employers to have a consideration or adherence to foreign data protection regimes, it is beneficial to have a general understanding of the laws in other jurisdictions and employers are advised to seek advice from local counsel in the relevant jurisdictions on the applicable personal data laws. For comparison, we set out below a brief outline of the requirements in Australia and Malaysia:

Australia

The data privacy protection in Australia comprises federal and state/territory laws. At a federal level, the Privacy Act 1988 and its prescribed Australian Privacy Principles ("**APPs**") apply to organisations that have an annual turnover of AUD3 million or more, and some other organisations such as the Australian government and government agencies ("**APP entity**").
The collection and use of an individual's personal information must be reasonably necessary for the APP entity's legitimate functions or activities. Details that the APP entity must inform the individual of include, but are not limited to, how the APP entity collects and holds the personal information; the purposes for collecting, holding, using or disclosing the personal information; how an individual may complain about breaches of the APPs; and whether the APP entity is likely to disclose the information to overseas recipients.
Personal information transferred outside of Australia is permitted where the APP entity has taken

reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the personal information being transferred.
Notwithstanding the above, a specific exemption from compliance with the APPs relating to the collection and use, and overseas transfers of, personal information may be availed where the APP entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety. According to the guidelines to the APPs, a '*serious threat to public health or safety*' includes the potential spread of a communicable disease, which may include the current COVID-19.

Malaysia

Personal data must be processed in accordance with the personal data protection principles under the Personal Data Protection Act 2010 (Act 709) of Malaysia ("**PDPA(M)**"). These principles include, but are not limited to, requiring the subject's prior consent for collecting the personal data which must be fairly and lawfully processed; observing the prescribed limitations on disclosing personal data; putting in place practical security measures to protect personal data; and not retaining the personal data for longer than necessary.
Under the PDPA(M), a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister, upon the recommendation of the Personal Data Protection Commissioner (PDP Commissioner) by notification published in the Gazette. However, there are exceptions to this including where the transfer is necessary as being in the public interest in circumstances as determined by the Minister – presumably, the current COVID-19 may fall within this exception.
It is interesting to note that on 14 February 2020, a public consultation paper no. 01/2020- Review of Personal Data Protection Act 2010, was issued by the PDP Commissioner, which sought to *inter alia*, review the transfer of personal data provisions, including whether guidelines on the implementation of cross border data transfer will be issued with regard to the exchange of personal data with an entity located outside Malaysia.