PERSONAL DATA PROTECTION FOR EMPLOYEES AMIDST COVID-19

In the face of the COVID-19 global pandemic, the Government of Malaysia implemented the Movement Control Order ("MCO"), which began on the 18th of March 2020. As a result of the low new infection rates and to ensure economic sustainability, the MCO was then replaced by the Conditional Movement Control Order ("CMCO") which allowed for economic sectors beyond the essential services to reopen.

However, in the future, once the MCO has been fully lifted, it is likely that the threat of COVID-19 will subsist. This article explores issues on personal data protection for employees in light of the COVID-19 pandemic.

Introduction Employees will no longer be working from home, which means internal policies must be put in place to regulate the safety of the workplace. One measure that can be adopted would be to require employees to declare personal information such as, *inter alia*, whether they have been tested for COVID-19, whether they have been primary or secondary contacts to any confirmed COVID-19 cases, and their travel plans and travel history.

With these internal policies in place, these questions then arise:

1. Is explicit consent required by the company to process the personal information given by the employee?
2. Can employees refuse to provide the information requested?
3. Can refusal to provide information be a ground for disciplinary action by the company?

Is explicit consent required by the company to process the personal information given by the employee?

The employee's explicit consent is required to process their health information, which includes, but is not limited to, information pertaining to COVID-19 as these type of data are regarded as "sensitive personal data".

According to **Section 4 of the PDPA**, "Sensitive personal data" is, "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette".

Section 40(1)(a) of the PDPA provides that sensitive personal data should not be processed except where the data subject has given his explicit consent. Note that even if employee's explicit consent cannot be obtained, the personal data may still be processed if it falls within one of the other limited circumstances set out in Section 40(1) that will be further discussed below.

Before processing such data, the employer must give a written notice pursuant to **Section 7 of the PDPA** to the employee to inform them, amongst other things, the purpose of collecting such personal data, the employee's right to request access to such data and to request correction of the personal data, as well as persons or third parties who may have access to the personal data.

Section 7 of the PDPA is reiterated below:

S. 7(1) A data user shall by written notice inform a data subject –

a) that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject;
b) the purposes for which the personal data is being or is to be collected and further processed;
c) of any information available to the data user as to the source of that personal data;
d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
e) of the class of third parties to whom the data user discloses or may disclose the personal data;

f) of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
g) whether it is obligatory or voluntary for the data subject to supply the personal data; and
h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.

(2) The notice under subsection (1) shall be given as soon as practicable by the data user -
a) when the data subject is first asked by the data user to provide his personal data;
b) when the data user first collects the personal data of the data subject;

Hence, the employer/company would need to provide a notice containing the purpose of obtaining such data and all other information stipulated under **Section 7 of the PDPA** when the employer first ask its employees to provide his personal data, or when the employer first collects the personal data of the employee.

Based on the above, it is clear that the employee's explicit consent is needed on how the employer/company is to process such data. The relevant terms regarding the type of information or data that will be required and processed by the employer is usually incorporated in the employment contract or company policies which the employee will have to consent to before the commencement of employment.

Therefore, if the processing of employees' sensitive personal data such as health data relating to COVID-19 is not provided for in the existing contract or data policy, the employers would have to issue a supplementary or fresh notice or policy to the employees, and accordingly, employee's explicit consent will have to be obtained.

Can employees refuse to provide the information requested?

It is generally the prerogative of the employers whether to request personal data such as medical information and recent travel and contact history of the employees. Where the employees agree to provide information relating to their health and wellbeing, this data would fall within the purview of the PDPA.

Pursuant to the PDPA, such personal data (e.g. test result of COVID-19 of an employee), can only be disclosed to a third party when the employee had consented to the disclosure or under certain circumstances stated in the PDPA. Unauthorised disclosure of personal data or non-compliance of the PDPA would amount to a breach of the PDPA and the employer can be subjected to fines and/or imprisonment. As such, employers must be cautious and handle the disclosure delicately to avoid employees from being discriminated against at the workplace upon disclosure of his/her medical condition in respect of COVID-19.

However, the employer may face situations where employees refuse to provide or consent to the processing of said information. The question then becomes, what happens if the employees refuse to disclose the information requested by the employer?

An employee may be a risk-factor if they have symptoms of COVID-19, have been in contact with a confirmed case, or if they have visited a high-risk area. **Section 24 of the Occupational Safety and Health Act 1994 ("OSHA")** provides for the general duties of employees at work.

This Section reads as follows:

S. 24. General duties of employees at work.
(1) It shall be the duty of every employee while at work-
a) to take reasonable care for the safety and health of himself and of other persons who may be affected by his acts or omissions at work;
b) to co-operate with his employer or any other person in the discharge of any duty or requirement imposed on the employer or that other person by this Act or any regulation made thereunder;
c) to wear or use at all times any protective equipment or clothing provided by the employer for the purpose of preventing risks to his safety and health; and

d) to comply with any instruction or measure on occupational safety and health instituted by his employer or any other person by or under this Act or any regulation made thereunder.

(2) A person who contravenes the provisions of this section shall be guilty of an offence and shall, on conviction, be liable to a fine not-exceeding one thousand ringgit or to imprisonment for a term not exceeding three months or to both.

Therefore, based on the section under OSHA, employees are obliged to disclose themselves as a risk-factor to the employer as OSHA mandates employees to ensure the safety and health at the workplace.

Furthermore, **Section 40 of the PDPA** allows for the processing of the sensitive data without the consent of the data subject, subject to fulfilling the following conditions:

S. 40. Processing of sensitive personal data

(1) Subject to subsection (2) and section 5, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions:

(a) the data subject has given his explicit consent to the processing of the personal data;

(b) the processing is necessary—

(iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

The Ministry of Health (MOH) also recently issued a guideline titled, **'COVID-19: Management Guidelines for Workplaces'** ("the Guideline"), which lists out the steps that should be taken by employers and employees to ensure a safe workplace. For example, the Guideline states that employers are recommended to encourage employees to take their temperatures regularly and to also obtain a travel declaration from the employees on their travel history. Employees are also requested to alert their supervisor if they develop any symptoms of COVID-19.

It can therefore be concluded that employees have an obligation to cooperate with employers by disclosing information related to their health and wellbeing concerning COVID-19 as well as their travel and contact history, in order to ensure the safety and health of all parties at the workplace.

It must be noted that even though Section 40(1)(b)(iii) of the PDPA allows for the processing of sensitive data without the consent of the employee, in the event an employee refuses to provide any of the requested health information pertaining to COVID-19, then there may be no such personal data for the employer to process unless such personal data was obtained from or provided through other sources or means e.g. thermal scanners, cctv recordings, personal observation or through third parties.

Can refusal to provide information be a ground for disciplinary action by the company?

Under employment law, disciplinary action can be taken against employees who have breached the company's internal policies. These policies are usually in the form of code of conducts, code of ethics, or standard operating procedures. An employee can be liable for misconduct for breaching these policies and can be dismissed from employment.

The principle of misconduct can be seen in the industrial case of *Safri Leman and Hume Cemboard Industries Sdn Bhd (Award No. 1408 of 2013)*, whereby the court held that:

"…The Industrial Court has confirmed ***that it is for the employer to determine initially whether or not an employee has committed misconduct, but that in doing so the employer must act fairly and reasonably, after appropriate investigation, and on the basis of fact rather than assumption****…"*

In the case of *Subramaniam Krishnasamy v Tesco Stores (Malaysia) Sdn Bhd [2010] ILJU 267*, the court accepted that the claimant had breached the code of conduct of the company and allowed for the punishment of dismissal, whereby the court held that:

"… It is noted that at para II of the Code of Conduct, the Company had stated:-
"… Any breach of the code will be regarded as an offence requiring disciplinary action which could lead ultimately to the termination of employment".

The Court thus on a balance of probabilities finds that the Company from the evidence adduced had reasonable cause and excuse to dismiss the Claimant. The Company is of the view that the said misconduct committed was serious in nature which warrants the punishment of dismissal and so does this Court. ***The punishment of dismissal taking into account that of the Claimant's position and nature of the misconduct was on a balance of probability a fair labour practice and in the circumstances appropriate…"***

Also, in the case of ***Mohd Shahrom Bin Mohd Sidek lwn Cimb Bank Berhad [2017] ILJU 193***, where the claimants had breached the bank's internal policy, the court dismissed the claim and held that:

"…Setelah Mahkamah meneliti keseluruhan kes ini yang mana Pihak Menuntut 1 merupakan Pengurus Kewangan Bank dan Pihak Menuntut 2 Pegawai Perkhidmatan Pelangan yang mempunyai pengalaman yang luas di dalam bidang tugas masing- masing. Tindakan Pihak Menuntut 1 dan Pihak Menuntut 2 mengesahkan surat tanpa mengambil tindakan berhati-hati yang perlu ada pada seorang pegawai bank untuk menjaga kepentingan majikan mereka ***menunjukkan tindakan mereka ini telah melanggar peraturan dan polisi bank. Setelah mengambilkira peruntukan di bawah seksyen 30(5) Akta Perhubungan Perusahaan, Mahkamah memutuskan tindakan buang kerja terhadap Pihak Menuntut 1 dan Pihak Menuntut 2 adalah wajar dan adil…"***

Therefore, it is established that disciplinary action can be taken against employees who do not abide by the company's internal policy. As such, if the employee is required to give certain information under the company's policy, a refusal to provide such information can amount to misconduct.

Conclusion In conclusion, moving forward, it is imperative for companies to update their internal policy and standard operating procedures in order to reflect the need to acquire relevant information to ensure the safety and health of all parties in the workplace. Otherwise employers will not be in a position to take action against employees who refuse to provide the necessary information.

For more information, kindly contact the undersigned.

Authors

Darren Kor Yit Meng
darren.kor@zulrafique.com.my

P. Jayasingam
jaya@zulrafique.com.my

Wong Keat Ching
keat_ching@zulrafique.com.my

Thavaselvi Pararajasingam
selvi@zulrafique.com.my

Assisted by: Azfar Asadullah Abdul Sathar, Nadiea Afiqah Abdul Hadi and Lim Khang Yen

Zul Rafique & Partners
29 May 2020