DATA SECURITY IN FLEXIBLE WORKING ARRANGEMENTS

by Arissa Ahrom

Managing remote employees requires organisations to take a different approach to data security compared to managing employees working from centralised offices. With employees working from various locations, often outside the secure office environment, maintaining data security becomes more complex. The statutory recognition of flexible working arrangements ("**FWA**") in Malaysia provides employees with the right to apply to their employers for the variation of their hours, days, or place of work. Employers may then decide whether to approve or refuse such an application.

In making this decision, especially in relation to the variation of an employee's place of work to remote work, the crucial issue of data security should not be overlooked. This is because an employer's failure to ensure that adequate measures to safeguard personal data are implemented when allowing FWA could expose the organisation to prosecution for failing to comply with the Security Principle outlined in the Personal Data Protection Act 2010 ("**PDPA 2010**"). Such a failure amounts to an offence under the PDPA 2010, and if convicted, the organisation is liable to a fine not exceeding RM300,000.00 and / or imprisonment for a term not exceeding 2 years[1].

Cybersecurity and Data Breaches

In 2023, the Malaysia Computer Emergency Response Team ("**MyCERT**") received a total of 5,917 reports on cyber-related incidents[2]. While concerning, this may not accurately represent the true extent of cybersecurity breaches in the country, given that there are no general obligations for organisations to report any incidents of data breaches, apart from sector-specific requirements. For example, financial institutions and capital market entities are required to notify Bank Negara Malaysia[3] and the Securities Commission of Malaysia[4], respectively, of any cybersecurity incidents.

Minimum Security Measures

The Security Principle under the PDPA 2010 provides that data users are required to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction[5]. In complying with the Security Principle, employers may refer to the Personal

[1] Section 5 (2) of the Personal Data Protection Act 2010
[2] https://mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b accessed on 23 June 2024
[3] Bank Negara Malaysia Risk Management in Technology (RMiT) Policy Document
[4] Securities Commission Malaysia's Guidelines on Management of Cyber Risk
[5] Section 9 of the Personal Data Protection Act 2010

Data Protection Standard 2015 and the General Code of Practice published by the Personal Data Protection Commissioner. These documents outline the general minimum security measures that must be taken. Some of the relevant measures that should be emphasised in an FWA include:

(a) Registering all employees involved in the processing of personal data;

(b) Terminating an employee's access rights to personal data after their resignation, termination or adjustments in accordance with changes in the organisation;

(c) Controlling and limiting employees' access to personal data systems;

(d) Providing authorised employees with user IDs and passwords to access personal data, and terminating such user IDs immediately when an employee no longer handles personal data;

(e) Ensuring that any transfer of personal data through removable media devices and cloud computing services are subject to the written consent of an authorised officer of the top management of the organisation and recording any such transfers;

(f) Safeguarding computer systems from malware threats and updating the back-up / recovery systems;

(g) Maintaining proper records of access to personal data periodically and making such records available for submission when directed by the Personal Data Protection Commissioner; and

(h) Ensuring that all employees involved in processing personal data always protect the confidentiality of the personal data.

Although the above measures apply to all data users, employers should assess the types of personal data in their possession and impose a level of security appropriate to each type of personal data.

Practical Steps for Employers

To safeguard data and ensure compliance with cybersecurity standards in FWA, employers can begin by implementing the following 3 practical measures:

1. <u>Establish Clear Policies</u>

   It is crucial to develop and communicate a comprehensive policy outlining not only clear rules and procedures of FWA but also setting out cybersecurity guidelines for employees working under FWA. This policy should detail expectations regarding data protection practices and adherence to the organisation's cybersecurity framework.

2. <u>Secure Remote Devices & Control Access</u>

   All devices provided to remote employees should be secured by installing firewalls to create a secure barrier between the business network and the internet. This measure can be strengthened by ensuring automatic updates or regularly updating the relevant software and operating systems to fix vulnerabilities and protect against cyber-attacks. Additionally, personal data stored on all devices should be encrypted to prevent unauthorised access.

   It is also good practice to deploy Virtual Private Networks ("**VPN**") to establish

secure, encrypted connections for remote access to company resources and adopt encrypted cloud storage solutions to securely store and share documents, setting clear protocols for data classification and access permissions.

3. Provide Ongoing Training

   It is essential for remote employees to be equipped with the knowledge and practices needed to enhance the organisation's cybersecurity. Employers should conduct regular cybersecurity training sessions for employees, focusing on best practices, identifying cyber threats, and responding to incidents promptly. Additionally, having a dedicated support team equipped to assist FWA employees in managing cyber incidents can bolster security measures.

In today's digital age, organisations should not shy away from adopting FWA to accommodate diverse work styles and enhance productivity. By taking proactive steps to educate employees, establish clear policies, and enhance cybersecurity measures, organisations can effectively mitigate risks associated with FWA while fostering a secure and productive work environment.

ARISSA AHROM
Senior Associate
Cyber Data Privacy |
Employment & Industrial
Relations
aa@lh-ag.com