New Personal Data Protection Requirements Effective 1 June 2025 - Mandatory DPO Appointment and Data Breach Notification Obligations

April 2025
One Asia Lawyers Group

Yuki Hashimoto
Lawyer(Japan)
Heng Zhen Hung

1. Introduction

On 25 February 2025, the Personal Data Protection Commissioner of Malaysia issued two key guidelines under the Personal Data Protection Act 2010 (PDPA), introducing compliance obligations for organisations that process personal data in Malaysia. These are the Guideline on the Appointment of a Data Protection Officer and the Guideline on Data Breach Notification, both of which will come into effect on 1 June 2025.

Foreign companies operating in Malaysia, or handling Malaysian personal data through subsidiaries, branches, service providers or cross-border transfers, should prepare for these changes immediately. The new requirements impose both structural obligations (the appointment and registration of a Data Protection Officer) and procedural obligations (strict timelines for notifying data breaches). Non-compliance may result in criminal penalties and reputational harm.

Appointment of a Data Protection Officer (DPO)

Under the new rules, certain organisations will be required to formally appoint one or more individuals to serve as Data Protection Officer. This obligation arises where the personal data processing activities conducted by a company meet any of the following conditions:

- the processing involves personal data of more than 20,000 individuals;
- the processing involves sensitive personal data, including financial or health-related data, of more than 10,000 individuals; or
- the processing includes regular and systematic monitoring of individuals.

**Regular and systematic monitoring may include behavioural advertising, tracking of health data through mobile applications or wearables, or automation systems in residential or commercial environments. However, the management of a loyalty programme is not necessarily considered to constitute such monitoring if it is limited to administering user accounts and does not involve tracking the purchasing behaviours of the data subjects.*

Once appointed, the Data Protection Officer must be someone who is physically present in Malaysia for at least 180 days per calendar year or who is easily contactable by the Malaysian authorities. The individual must be proficient in both Bahasa Malaysia and English and more importantly, has a good understanding of the PDPA. The Data Protection Officer may be selected from the company's existing employees or may be appointed from an external service provider. However, the individual must not hold responsibilities that could conflict with their role as DPO, and must report directly to the organisation's senior management.

The Commissioner must be notified of the appointment of the Data Protection Officer within 21 days of appointment, using the official registration portal. A dedicated email address must also be created and assigned specifically for the DPO. This business email must be separate from the individual's personal or other business email addresses. If there is a change in the individual appointed or their

contact details, the Commissioner must be informed within 14 days. In the event that the appointed DPO resigns or their contract ends, the company must promptly appoint a replacement or, at minimum, an interim officer who can respond to regulatory or data subject enquiries.

In terms of responsibilities, the DPO is expected to advise the organisation on its obligations under the PDPA, monitor compliance with internal data protection policies, conduct or support the execution of data protection impact assessments and serve as the official point of contact for the Personal Data Protection Commissioner and affected data subjects. The DPO must also play an active role in overseeing the handling of any data breaches, including the preparation of related reports and submission of documentation to the Commissioner, if required.

Foreign companies with significant data operations in Malaysia, particularly those in the finance, healthcare, e-commerce, or technology sectors, should assess whether their operations meet the thresholds that trigger the mandatory appointment requirement. Where required, they should identify and evaluate potential candidates, clarify the reporting line of the DPO, develop internal governance structures to support the DPO's function and establish procedures for registration and communication with the Commissioner.

Mandatory Data Breach Notification Obligations

Effective 1 June 2025, the new framework will also require data controllers to notify the Personal Data Protection Commissioner of any personal data breach that causes or is likely to cause significant harm to affected individuals. A personal data breach is defined broadly and includes incidents resulting in the unauthorised access, disclosure, alteration or destruction of personal data, whether due to human error, system malfunction or malicious activity.

Where a data breach meets the harm threshold, the data controller must notify the Commissioner as soon as practicable, and in any event, within 72 hours of becoming aware of the breach, if the breach results in or is likely to result in significant harm to any data subject. The following situations are explicitly recognised as constituting "significant harm" under the PDPA and its implementing guidelines:

- **Physical injury:** Where the breach exposes data that may result in bodily harm or endanger an individual's physical safety, such as the unauthorised disclosure of medical or health-related information.
- **Financial loss:** Where the breach may lead to actual or potential financial damage to the data subject, including exposure of banking details, payment information, or login credentials that could be exploited for fraudulent transactions.
- **Negative impact on credit standing:** Where the compromised data may affect an individual's credit score or creditworthiness, including unauthorised access to credit-related data.
- **Damage to or loss of property:** Where the breach could facilitate theft or destruction of personal or organisational assets, such as when access credentials or location data are exposed.
- **Use for unlawful purposes:** Where the breached data may be used for illegal activities, including identity theft, fraud, extortion or activities in violation of Malaysian or foreign laws.
- **Involvement of sensitive personal data:** Where the breach involves data categorised as sensitive under the PDPA, such as health information, financial status, religious belief, political opinion or criminal records.
- **Combination of data enabling identity fraud:** Where the breach involves a combination of data, such as name, identification number and contact details, that, when taken together, could be used to impersonate or fraudulently represent the data subject.
- **Large-scale impact:** Where the breach affects more than 1,000 individuals. In such cases, the breach is considered significant by scale and notification is required regardless of the specific harm caused to each individual.

The notification must include specific information such as the date and time the breach occurred, the nature of the breach, the type and volume of data involved, the number of individuals affected, the

suspected cause and any measures taken to contain the breach. If it is not feasible to submit a complete report within 72 hours, additional details may be submitted in phases, provided they are completed within 30 days of the initial notification. If more than one data controller is involved in the breach, each must submit a separate report to the Commissioner.

In addition to notifying the Commissioner, the data controller must notify affected individuals if the breach is likely to cause significant harm. This must be done without undue delay, and no later than seven (7) days after the initial report to the Commissioner. The notification to individuals must include clear information about the breach, its likely consequences, the steps taken to mitigate the impact and contact information for the organisation's DPO. The notification must be made through direct means such as email, SMS or postal mail. If direct contact is impractical, for example, if the contact information is outdated or the volume of affected individuals is too large, notification may be made via public announcements, such as on the company's website, social media channels or newspapers.

The PDPA requires companies to retain records of all data breaches and notifications for a minimum of two years, and to make these records available to the Commissioner upon request. Failure to notify the Commissioner as required may result in criminal penalties, including a fine of up to RM250,000 or imprisonment for up to two years, or both.

Companies should therefore review their incident response protocols to ensure that they include internal mechanisms for breach identification, assessment of harm, coordination of notification processes and preservation of relevant documentation. In addition, roles and responsibilities for breach handling should be clearly assigned and relevant personnel should be trained in how to respond within the strict notification timelines.

Preparation Steps Before 1 June 2025

To ensure compliance by the effective date, foreign companies with operations involving Malaysian personal data should take the following measures.

First, a detailed assessment should be conducted to determine whether the organisation meets the thresholds that require the appointment of a Data Protection Officer. Where the obligation applies, preparations must include identifying and onboarding a qualified candidate, establishing a dedicated business contact channel and completing registration with the Commissioner within the required timeframe.

Second, data breach management policies should be reviewed and where necessary, updated to ensure that they include specific procedures aligned with the PDPA's new notification obligations. This includes defined internal reporting chains, documentation protocols, risk assessment criteria and a readiness to meet the 72-hour and 7-day notification deadlines. Contracts with third-party processors should also be reviewed to ensure that they contain provisions requiring prompt breach reporting and cooperation.

Third, internal data protection governance should be reinforced by ensuring that employees involved in data processing, information security and compliance are adequately trained on the new legal obligations. Privacy notices, internal policies and external-facing materials should also be updated to reflect the appointment of a DPO and the process for responding to breaches.

◆ One Asia Lawyers ◆

One Asia Lawyers Group is a network of independent law firms created to provide seamless and comprehensive legal advice for Japanese and international clients across Asia. With our member firms in Japan, Southeast Asia, Oceania and other ASEAN countries, One Asia Lawyers Group has a strong team of legal professionals who provide practical and coherent legal services throughout each of these jurisdictions.

For any enquiry regarding this article, please contact us by visiting our website: https://oneasia.legal/or email: info@oneasia.legal.

＜Author＞

Yuki Hashimoto
One Asia Lawyers Malaysia
Lawyer (Japan)

He established his own firm in Japan and worked as a representative partner of a law firm with three offices in Japan. He has provided legal service as advisor to a wide range of organization in Japan, including companies in construction, real estate management, system development as well as local government and politic parties. He has been a member of One Asia Lawyers since September 2020, providing advice on general cross-border Asian legal matters (M&A, regulatory investigations, etc.) with a focus on Malaysia.
yuki.hashimoto@oneasia.legal

Heng Zhen Hung
One Asia Lawyers Malaysia
Legal associate (Malaysia)

Heng Zhen Hung (Zed) obtained his law degree in 2018 and was called to the England & Wales bar in 2020.
Before returning to Malaysia, he worked at a London based charity where he provides legal advice, case preparation and advocacy in social security tribunal cases. He also did some employment tribunal cases when he was there.
Before he joined One Asia lawyers, he was a member of a tax legal team of a law firm located in Kuala Lumpur, he worked on transfer pricing, tax, SST & GST and Customs cases. After joining One Asia Lawyers, he has been providing services for regulatory compliance, employment law, contract law and land law matters.
zhenhung.heng@oneasia.legal