# WHAT YOUR BUSINESS SHOULD TAKE NOTE ABOUT THE NEW AMENDMENTS TO DATA PROTECTION IN 2024

Published on 22nd July 2024

## INTRODUCTION

The amendments to the Personal Data Protection Act 2010 ("**PDPA**") have been long discussed. The Government had issued a public consultation paper[1] in 2020 to elicit feedback. Recently, the Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**") was tabled to the Dewan Rakyat (House of Representatives) and was subsequently passed without amendments upon its second reading on 16 July 2024. 5 out of the 22 amendments proposed in a public consultation paper were adopted in the Amendment Bill.

In this article, we will briefly highlight the key amendments to the PDPA, and matters that businesses should take note of in anticipation of the coming into effect of the new amendments. The Amendment Bill must be tabled and passed in the Dewan Negara (House of Senate) before it becomes law.

1. **Expansion of the "Sensitive Personal Data" Definition**

   The definition of "sensitive personal data" has been expanded to include "biometric data". "Biometric data" means *any personal data resulting from technical processing relating to the physical, physiological or behavourial characteristics of a person*.

   **Takeaway 1:** Businesses must be mindful that processing biometric data, which is now regarded as sensitive personal data, is subject to more stringent requirements under the PDPA.

2. **Increased in Sanctions for Non-compliance with Personal Data Protection Principles**

   The sanction for non-compliance of the Personal Data Protection Principles[2] is increased to RM1,000,000.00 and/or imprisonment for a term not exceeding 3 years compared to the current sanction of RM300,000.00 and/or imprisonment for a term not exceeding 2 years.

   **Takeaway 2**: Businesses' existing policies and processes ought to be reviewed to ensure stricter compliance with the Personal Data Protection Principles to avoid hefty sanctions.

3. **Direct Liability on Data Processor for Security of Personal Data**

   Data processors now have direct obligation to comply with the Security Principle[3], which stipulates that a data processor who processes personal data solely on behalf of a data controller [4] shall protect that personal data from, among others, any loss, misuse, modification, unauthorised access by providing practical sufficient technical and organisational security measures for the processing of personal data and taking reasonable steps to ensure compliance with those measures.

---

1 Public Consultation Paper No. 01/2020: Review of Personal Data Protection Act 2010 (Act 709).
2 This encompasses the General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle and Access Principle.
3 Section 9 of the PDPA.
4 The Amendment Bill changed the terminology of "data users" to "data controllers".

Failure of data processors to comply with the Security Principle will subject themselves to the sanctions set out in Paragraph 2 above.

**Takeaway 3**: This is a welcome change for businesses who rely on data processors e.g. payroll providers or disaster recover centers to help process personal data on its behalf. Notwithstanding this change, data controllers still have the overall responsibility to comply with the Security Principles. It is still important for data controllers to take practical steps to ensure that data processors have the necessary security measures in place to protect the data controller's personal data.

## 4. Mandatory Appointment of Data Protection Officer(s)

It is now mandatory for data controllers and data processors to appoint one or more Data Protection Officer(s) (DPO) to oversee data protection within their organisation. The data controller is to notify the Commissioner of the appointment of the DPO.

**Takeaway 4**: Businesses who have not appointed a DPO will need to identify a candidate who is suitable and skilled for the job. For those businesses who have already done so, they are to notify the Commissioner of such appointment.

## 5. Mandatory Notification for Data Breach

A data controller now has an obligation to notify the Commissioner, as soon as practicable, if it has a reason to believe that a personal data breach has occurred[5]. "Personal data breach" is defined as "*any breach of personal data, loss of personal data, misuse of personal data or unauthorized access of personal data*".

Where the personal data breach causes or likely to cause any significant harm to the data subject, the data controller shall notify the data subject of such breach without unnecessary delay. The Amendment Bill does not define "significant harm" but it is expected that additional guidelines relating to breach notification will be developed to provide more clarity.

**Takeaway 5**: Businesses will need to review their existing policies to incorporate personal data breach notification procedures. The DPO will play an important role in developing the process starting from the determining the threshold of a data breach, timeframes for the relevant stakeholders to notify the DPO of any suspected breach, to the notification process to the Commissioner.

## 6. Data Portability – Transmit Your Data Across Different Entities

The Amendment Bill introduces the right to data portability[6]. The data subject now has the right to request a data controller to transmit his/her personal data to another data controller within a prescribed time period. The data subject's request is however subject to technical feasibility and compatibility of the data format.

**Takeaway 6**: Businesses would need to cater in its existing processes this obligation of data portability in addition to the data subject's existing rights to access data, correct data and withdraw consent. Data controllers would also need to ascertain the data format in which it would be able to transfer the said personal data to the other data controller.

---

5 Section 12B of the Amendment Bill.
6 Section 43A of the Amendment Bill.

## 7. Data Transfer Outside Malaysia Now Permitted

The "whitelist" of countries, as may be Gazetted by the Minister, to which personal data may be transferred to outside of Malaysia has been deleted. Notwithstanding that, data controllers are still able to transfer personal data to a place outside Malaysia if that place has law which is substantially similar to the PDPA or that place ensures adequate level of protection in relation to the processing of data which is at least equivalent to that afforded by the PDPA.

**Takeaway 7**: Prior to the deletion of the Minister's power to Gazette the whitelist of countries, data controllers were already permitted to transfer personal data outside of Malaysia under the exceptions provided under Section 129 of the PDPA. This change is unlikely to have a significant impact on businesses since there is no whitelist Gazetted by the Minister currently.

## CONCLUSION

The proposed changes enhance data protection in Malaysia and bring Malaysia a step closer to the high standards set by the European Union General Data Protection Regulation (GDPR). Whilst the details regarding the implementation of some of the new amendments have yet to be addressed, e.g breach notification, appointment of DPO and data portability, it is anticipated that these will be detailed out in guidelines to be issued by the Commissioner.

It is highly advisable for businesses to adapt its current processes to new changes brought about by the Amendment Bill. Whilst there will inevitably be cost for compliance which businesses would need to budget for, the cost for non-compliance would be more significant.

**Authors**

**Darren Kor Yit Meng**
(Partner)
darren@zulrafique.com.my

**Phang Sin Yee**
(Legal Associate)
sinyee.phang@zulrafique.com.my

**Lee Chloee**
(Legal Associate)
chloee.lee@zulrafique.com.my

If you require advice on personal data protection matters, please feel free to contact any member of our team as above. We are here to assist you with all your data protection needs.

*Disclaimer: The contents do not constitute legal advice, are not intended to be a substitute for legal advice and should not be relied upon as such.*