Deloitte.

Navigating the Future:
Amendments to Malaysia's Personal Data Protection Act 2010

MAKING AN IMPACT THAT MATTERS since 1845

Background

The Personal Data Protection Act 2010, Malaysia's primary privacy legislation – also the first in the ASEAN region to regulate processing of personal data in commercial transactions – is now set for significant revision. This long-anticipated update follows the passage of the Personal Data Protection (Amendment) Act 2024, which received Royal Assent on 9 October 2024 and was officially gazetted on 17 October 2024. Converging with global privacy regulations, the revised law introduces significant amendments:

Types	Amendments	Personal Data Protection Act 2010	Personal Data Protection (Amendment) Act 2024
Novel amendments	Mandatory appointment of a Data Protection Officer (DPO)	N/A	• Mandatory for the data controller and processor to appoint a DPO, providing a formal notification to the Commissioner.
	Mandatory data breach notification to the Commissioner and data subjects	N/A	• Notify the Commissioner of the data breach as soon as practicable. • Notify the data subjects without undue delay if the breach is likely to cause significant harm.
	Rights to data portability	N/A	• Data subjects may request the transfer of their data to another data controller within a specified time frame, subject to technical feasibility and format compatibility.
Amendments built upon pre-existing provisions	Data transfer to countries with equivalent level of protection	• Personal data transfers were limited to countries on an approved whitelist, but no countries were officially gazetted since the inception of the law.	• Transfer of personal data is allowed outside Malaysia to countries with substantially similar laws or equivalent levels of protection. • Removal of the whitelist regime, but existing exceptions remains.
	Direct responsibilities on data processors	• Data users must ensure data processors provide adequate security guarantees and take steps to comply with those measures.	• Data processors are directly obligated to comply with the security principles.
	Increase of penalties for breach of personal data protection principles	• Penalties include a fine of up to RM300,000 and / or imprisonment for up to 2 years.	• Proposed penalties to be increased to a fine of up to RM1,000,000 and / or imprisonment for up to 3 years.
Amendments related to administration & enforcement	Change of terminology from "data user" to "data controller", and from "data user register, data user form register" to "data controller register, data controller forum register".		
	Inclusion of biometric data as sensitive data, which requires a stricter legal basis for processing (i.e., explicit consent).		
	Exclusion of deceased individuals from the definition of data subject.		
	Introduction of "personal data breach" definition, which is defined as any breach of personal data, loss of personal data, misuse of personal data or unauthorised access of personal data.		
	Expansion of the "requestor" definition to include data subjects who submit data access requests, data correction requests, and data portability requests.		
	The Commissioner can designate a body or a data controller as "data controller forums" for specific classes of data controllers.		

Amendments in comparison to APAC privacy regulations

Amendments	SG PDPA[1]	ID PDPL[2]	VN PDPD[3]	PH DPA[4]	TH PDPA[5]	TW PDPA[6]	JP APPI[7]	KR PIPA[8]	CN PIPL[9]	IN DPDPA[10]	HK PDPO[11]	AU PA[12]
Mandatory appointment of Data Protection Officer (DPO)	√	√	√	√	√	×	×	√	√	√	×	×
Data breach notification to the Commissioner & data subjects	√	√	√	√	√	√	√	√	√	√	×	√
Rights to data portability	√	√	√	√	√	×	×	√	√	×	×	×
Data transfer to countries with equivalent level of protection	√	√	√	√	√	√	√	√	√	√	√	√
Direct responsibilities on data processors	√	√	√	√	√	√	√	√	√	×	×	√
Inclusion of biometric data as sensitive data	×	√	√	√	√	×	×	√	√	×	×	√
Exclusion of deceased individual as data subject	√	×	×	×	√	√	√	√	√	×	√	√

Organisational impact on people, process, policy, and technology

The Personal Data Protection (Amendment) Act 2024 brings significant impact on organisations across four key dimensions: People, Process, Policy, and Technology. These changes necessitate a comprehensive re-evaluation and adaptation of current practices.

Policy

- **Update of existing policies and procedures**: Develop or enhance the existing policies and procedures (i.e., privacy notice and data inventory) to align with the latest regulatory requirements and industry standards.
- **Periodic review**: Conduct periodic review on the existing policies and procedures to ensure their relevancy and alignment with the latest regulatory requirements and technological advancements.

Process

- **Data handling process review**: Review and enhance processes for data collection, storage, processing, transfer, and disposal, taking into account the latest regulatory requirements.
- **Data subject rights management**: Enhance existing data subject rights handling process to incorporate and facilitate the right of data portability.
- **Incident response and data breach handling**: Develop and implement a robust incident response and data breach notification process, ensuring that breaches are detected, assessed, contained, and reported in a timely manner to both regulators and affected data subjects.
- **Third-party risk management**: Review and enhance the third-party risk management framework and due diligence checklist to ensure data processors, where applicable, have appointed a DPO and adhere to security principles and other relevant contractual and regulatory requirements.
- **Compliance monitoring program / audit**: Establish a structured compliance monitoring program that regularly audits the organisation practices to ensure continuous compliance with the regulatory requirements.
- **Privacy by design and default**: Embed privacy principles into the development and design of new technologies and systems, ensuring that privacy considerations are considered at every stage of the product lifecycle.

People

- **Role and responsibility expansion**: Appoint or designate a Data Protection Officer (DPO) and privacy champions, with formal notification provided to the Commissioner, to oversee the organisation's privacy program, ensuring continuous compliance with the latest regulatory requirements.
- **Cultural shift**: Foster a privacy-conscious organisational culture that emphasises accountability, proactivity, transparency in data handling practices, and collaboration across teams.
- **Enhanced training and awareness**: Enhance efforts to educate and raise awareness among all employees, providing both general and role-based training on the latest regulatory requirements and their responsibilities.

Technology

- **Security upgrades**: Enhanced security measures for data protection and security, such as encryption, data tokenisation, data access governance, and data loss prevention.
- **Privacy management solution**: Implement privacy management solutions to streamline and automate privacy operations, integrating privacy-by-design principles into workflows.
- **Privacy Enhancing Technologies (PETs)**: Implement PETs, such as secure multi-party computation, differential privacy, and homomorphic encryption, which enable secure data processing and potential data monetisation while minimising privacy risks.

Our transformation program

We provide a suite of services that can help your organisation evolve your program to protect the data and business models that truly matter, while keeping up with the latest regulatory changes. We also offer tailored solutions based on your organisation's characteristics and needs.

1 Assess

- Evaluate the data processing landscape, and organisation's framework and program against local regulation, and industry standards and maturity model.
- Provide recommendations to enhance overall maturity and/or compliance.

Current state / gap / maturity assessment and audit

Data Protection Impact Assessment (DPIA)

Remediation roadmap

2 Discovery

- Establish a strategic direction and governance framework to ensure effective oversight of data risks.
- Define the data landscape by identifying where data resides and flows, while ensuring proper data classification and protection.

Strategy, governance and target operating model

Data discovery, inventory, lineage

Data classification

3 Implement

- Enhance the organisation's framework and program by developing relevant policies and deploying appropriate technology solutions (i.e., Privacy Management and Data Security Solutions, PETs, etc.)
- Support the organisation in getting ready for the selected certification (i.e., ISO 27701, DPTM, APEC CBPR, etc.)

Framework implementation

Technical implementation

Certification advisory support

4 Operationalise

- Advice on operationalising the organisation's program and framework, featuring training and awareness, and a tabletop simulation exercise.
- Provide continuous support to ensure ongoing compliance with local regulations and optimisation of processes throughout the operational deployment of technology.

Operationalisation advisory

Training and awareness / tabletop simulation exercise

Data Protection Officer as a Service (DPOaaS)

Contact us

Ho Siew Kei
Malaysia Cyber Risk Leader
sieho@deloitte.com

Venkat Paruchuri
SEA Data Privacy and Protection Risk Leader
veparuchuri@deloitte.com

Melvin Toh
Senior Manager, Technology & Transformation
Deloitte Southeast Asia
mtoh@deloitte.com

Melbourne Lim
Manager, Technology & Transformation
Deloitte Southeast Asia
melblim@deloitte.com

References

1 Singapore Personal Data Protection Act 2012
2 Indonesia Law No. 27 of 2022 on Personal Data Protection
3 Vietnam Decree No. 13/2023/ND-CP on Personal Data Protection
4 Philippines Data Privacy Act of 2012 (Republic Act No. 10173)
5 Thailand Personal Data Protection Act 2019
6 Taiwan Personal Data Protection Act 2023
7 Japan Act on the Protection of Personal Information (Act No. 57 of 2003)
8 Korea Personal Information Protection Act 2023
9 China Personal Information Protection Law
10 India Digital Personal Data Protection Act 2023
11 Hong Kong Personal Data (Privacy) Ordinance (Cap. 486)
12 Australia Privacy Act 1988. (No. 119, 1988) (as amended)

Deloitte.