



In 2025, the saying “*data is the new oil*” has taken on even greater meaning. Data now stands as one of the most critical resources in the digital economy, driving innovation, powering business decisions, and shaping regulatory enforcement.

On 28 April 2025, the highly anticipated Data Sharing Act 2025 (“**Act**”) officially came into force¹. The Act includes provisions relating to the facilitation of data sharing between Federal Government and public agencies, and the establishment of the National Data Sharing Committee. This article highlights the key provisions of the Act.

Key provisions

1. Establishment of the National Data Sharing Committee

The Act provides for the establishment of the National Data Sharing Committee (“**Committee**”)².

(a) Composition of the Committee

The Committee will comprise of the following members³:

- (i) the Secretary General of the ministry, who shall be the Chairman;
- (ii) a representative from each of the ministries;
- (iii) a representative of the Prime Minister's Department;
- (iv) the Chief Government Security Officer;
- (v) a representative of the National Cyber Security Agency(NACSA); and
- (vi) a representative of the Personal Data Protection Department (PDPD).

¹https://www.digital.gov.my/api/file/file/28042025_PRESS%20RELEASE_DATA%20SHARING%20ACT%202025%20COMES%20INTO%20EFFECT%20TODAY%20-%20SET%20TO%20ENHANCE%20GOVERNMENT%20SERVICES%2C%20PROTECT%20PERSONAL%20DATA.pdf dated 28 April 2025

² Section 5(1) of the Act

³ Section 5(2) of the Act

(b) Committee's functions

The Committee is tasked with the following⁴:

- (i) to formulate policies and strategies relating to data sharing;
- (ii) to oversee the effective implementation of the Act;
- (iii) to take or recommend appropriate steps or administrative actions to resolve the difficulties or administrative issues which arise during the implementation of the Act;
- (iv) to formulate policies relating to database for the purposes of data sharing; and
- (v) carrying out any other functions arising out of or consequential to the functions of the Committee under this Act consistent with the purposes of this Act.

The policies and strategies referred to in paragraph 1(b) above may include⁵:

- (i) procedures to preserve the privacy and confidentiality of data;
- (ii) safeguards relating to data handling and storage;
- (iii) method for data sharing under this Act; and
- (iv) risk assessment frameworks for data handling and storage.

2. Data Sharing

The Act introduces provisions relating to the procedure, purpose, refusal and the duties relating to data sharing.

(a) Request for Data Sharing

Any public sector agency may request to another public sector agency for the sharing of data under the control of such other public sector agency⁶ and shall specify⁷:

- (i) the data requested;
- (ii) the purpose for which the data is requested;
- (iii) the public service agencies intended to be the data recipient and the data provider; and
- (iv) the manner of handling the data requested.

(b) Purpose of the request for Data Sharing

The purpose of the request for Data Sharing may be granted for the following reasons, including⁸:

- (i) to enhance the efficiency or effectiveness of policies, programme management or service planning and delivery by the public sector agencies;
- (ii) to reduce or prevent threat to the life, health or safety of a person, or threat to public health or safety;
- (iii) to respond to a public emergency; or
- (iv) in the public interest.

⁴ Section 6(1) of the Act

⁵ Section 6(2) of the Act

⁶ Section 12(1) of the Act

⁷ Section 12(2) of the Act

⁸ Section 13 of the Act

(c) Evaluation of the request for Data Sharing

An evaluation of the request for Data Sharing would need to be made as to⁹:

- (i) whether the purpose for which the data is requested warrants the sharing of the data;
- (ii) whether the sharing of the data is against the public interest; and
- (iii) whether the public sector agency requesting the data has appropriate security and technical safeguards in place to ensure that the shared data is not subject to unauthorized access or use.

(d) Refusal of the request for Data Sharing

A request for Data Sharing may be refused on the following grounds¹⁰:

- (i) the data requested could reasonably be expected to disclose, or enable a person to ascertain, the identity of a confidential source of information relating to the enforcement or administration of law;
- (ii) the data requested could reasonably be expected to disclose the existence or identity of a person included in a witness protection programme;
- (iii) the data requested could reasonably be expected to disclose investigative measures or procedures, including intelligence gathering methodologies, investigative techniques or technologies, covert practices or information sharing arrangements between law enforcement agencies;
- (iv) the sharing of the data requested will constitute a breach of one or more of the following:
 - the solicitor-client privilege or legal professional privilege;
 - an agreement or a contract;
 - an equitable obligation of confidence; or
 - an order of a court or tribunal
- (v) the data requested involves one or more of the following:
 - national security or defence;
 - the investigation of a breach, or possible breach, of any written law;
 - an inquest or inquiry into death; or
 - a proceeding before a court or tribunal
- (vi) the public sector agency believes on reasonable grounds that the sharing of the data requested would be likely to endanger the health, safety or welfare of one or more individuals;
- (vii) the data requested is inconsistent with the purpose specified under section 13 of the Act and does not warrant the data to be shared;
- (viii) the public sector agency requesting the data does not possess appropriate security and technical safeguards to ensure that the data to be shared is not subject to unauthorized access or use.

(e) Procedure of Data Request

- (i) A Data Request would be made by the public sector agency to another public agency¹¹.

⁹ Section 14(1) of the Act

¹⁰ Section 15 of the Act

¹¹ Section 12(1) of the Act

- (ii) The public sector agency to whom the request for data sharing is made shall within fourteen (14) days from the date of receiving the request, evaluate¹² and respond whether:
- The data requested may be provided with or without conditions¹³.
 - The data may be refused under paragraph 2(d) above¹⁴.
 - The data requested may not be possible to be provided within the period specified¹⁵. The public sector agency making the request (i) the reason as to why the response cannot be provided within the period specified; and (ii) the period within which such response will be provided.

(f) Duty of Data Sharing

The Act imposes duties and obligations on the following parties in respect to data sharing:

Data Provider and Data Recipient¹⁶	Third Party managing data from the Data Recipient¹⁷
<p>(a) ensure that the shared data is managed and maintained in compliance with any legal requirements concerning its custody and control that are applicable to such data;</p> <p>(b) take necessary measures to ensure the security and privacy of the data including:</p> <p style="padding-left: 40px;">(i) the protection of data from any loss, misuse, unauthorized or accidental modification, access or disclosure, alteration or destruction; and</p> <p style="padding-left: 40px;">(ii) the preservation of rights of individuals relating to personal data protection;</p> <p>(c) keep record of all particulars relating to the shared data;</p> <p>(d) report any unauthorized sharing of data to the Director General; and</p>	<p>(a) The Data Provider's consent is obtained before the data is handled by such third party¹⁸.</p> <p>(b) Complies with the Act and follows security protocols¹⁹.</p>

¹² Section 14(1) of the Act

¹³ Section 14(2) of the Act

¹⁴ ibid

¹⁵ Section 14(3) of the Act

¹⁶ Section 16 of the Act

¹⁷ Section 17 of the Act

¹⁸ Section 17(1) of the Act

¹⁹ Section 17(2) of the Act

(e) comply with such other requirements as the Committee may determine.	
---	--

3. Penalties

Any officer or servant of a data recipient who use or disclose the shared data not for the purpose of the Act²⁰ or third party managing data from the Data Recipient failed to comply with the Act and its requirements,²¹ commits an offence and shall, upon conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding five years or to both.

4. Implication for businesses

- (a) Enhancing cybersecurity infrastructures: Third parties (i.e. organisations /private business) managing data from Data Recipients would need to ensure that their cybersecurity infrastructure and software are of the highest calibre.
- (b) Implementing cybersecurity practices: Organizations must implement comprehensive security measures, including strong authentication, regular security updates, and incident response planning, to mitigate risks from cyber threats.
- (c) Reviewing of compliance process of handling data: With the enactment of the Act, more care is needed in ensuring compliance in handling data. Business should actively review their data practices, establish strong protective measures, and safeguards.
- (d) Conduct security awareness training for employees: Staff must be trained to ensure compliance and foster a culture of data protection within the organisation.

5. Conclusion

With the enactment of the Act, this would help Malaysia to position itself as a regional hub for data-driven innovation. As quoted by Digital Minister Gobind Singh Deo²², the passing of the law is essential towards creating an ecosystem for innovation to thrive, allowing digital services and solutions to be put into effect quickly and efficiently.

²⁰ Section 18 of the Act

²¹ Section 17 of the Act

²² <https://www.thestar.com.my/tech/tech-news/2024/12/20/malaysia-approves-data-sharing-bill-2024-for-federal-government-agencies> dated 20 December 2024

Further information

Should you have any questions on this Act or how it may affect you or your business, please get in touch with the following person:

Chuck Siew Ka Wai

Partner

kwsiew@tsl-legal.com

Kok Hao Ying

Senior Associate

hykok@tsl-legal.com

© TSL Legal

This article is intended to provide general information only and does not constitute legal advice. It should not be used as a substitute for professional legal consultation. We recommend seeking legal advice before making any decisions based on the information available in this article. TSL Legal fully disclaims responsibility for any loss or damage which may result from relying on this article.