Vol. 33 (2) 2025 IIUMLJ 279 - 320

A LEGAL FRAMEWORK FOR PUBLIC SECTOR DATA SHARING IN MALAYSIA: THE CLASH BETWEEN DATA PROTECTION, PRIVACY AND PUBLIC INTEREST

Mahyuddin Daud*

ABSTRACT

Data sharing is increasingly recognised as a critical enabler of effective governance, improved policymaking, and efficient public service delivery, yet in Malaysia, it has historically been governed through administrative circulars and fragmented provisions rather than a clear statutory framework. Despite recent initiatives such as PADU, MyGDX, and the Open Data Portal, the practice remains hindered by systemic challenges, including misinterpretation of confidentiality clauses as prohibitions, overly cautious agency practices guided by non-binding codes, inconsistent and overlapping data formats, and heightened concerns about privacy and cybersecurity risks. These barriers not only slow inter-agency collaboration but also undermine policy efficiency, weaken service delivery, and erode public trust. Against this backdrop, the enactment of the Data Sharing Act 2025 represents a significant step forward. Yet, questions remain regarding its operationalisation and ability to balance competing demands of accessibility, security, and privacy. This study seeks to analyse Malaysia's current legal and policy framework on data sharing, identify challenges faced by public agencies, and benchmark Malaysia's approach against international best practices from the European Union, United Kingdom, Ireland, Australia, and Singapore. Using content analysis of laws and policies, comparative legal analysis, and semi-structured interviews with government agencies, the research aims to propose reforms that strengthen Malaysia's governance of data sharing. It is expected that findings will highlight the need for privacy-by-design principles, uniform data governance standards, and robust oversight mechanisms to foster

*Associate Professor, Civil Law Department, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Selangor, PO Box 10, 50728 Kuala Lumpur, Malaysia. E-mail: mahyuddin@iium.edu.my

[Received: 30 May 2025, Accepted: 22 October 2025, Published: 30 November 2025]

responsible data sharing, enhance public trust, and align Malaysia with global standards while addressing its domestic realities.

Keywords: Data Sharing, Data Protection, Public Sector Data Sharing, Privacy, Legal Framework.

RANGKA KERJA PERUNDANGAN BAGI PERKONGSIAN DATA SEKTOR AWAM DI MALAYSIA: PERTEMBUNGAN ANTARA PERLINDUNGAN DATA, PRIVASI DAN KEPENTINGAN AWAM

ABSTRAK

Perkongsian data semakin diiktiraf sebagai pemacu penting kepada tadbir urus yang berkesan, penggubalan dasar yang lebih baik, serta penyampaian perkhidmatan awam yang cekap, namun di Malaysia amalan ini secara tradisinya dikawal melalui pekeliling pentadbiran dan peruntukan yang berpecah-pecah tanpa kerangka perundangan yang jelas. Walaupun pelbagai inisiatif seperti PADU, MyGDX dan Portal Data Terbuka telah diperkenalkan, pelaksanaannya masih berdepan cabaran sistemik termasuk salah tafsir peruntukan kerahsiaan sebagai larangan mutlak, pendekatan agensi yang terlalu berhati-hati berasaskan kod amalan tidak mengikat, ketidakseragaman serta pertindihan format data, dan kebimbangan yang meningkat terhadap isu privasi serta keselamatan siber. Halangan ini bukan sahaja memperlahankan kerjasama antara agensi, malah melemahkan keberkesanan dasar, menjejaskan kualiti perkhidmatan, dan mengurangkan kepercayaan awam. Dalam konteks ini, penggubalan Akta Perkongsian Data 2025 merupakan langkah penting. Namun persoalan masih timbul mengenai pengoperasiannya dan keupayaannya mengimbangi keperluan aksesibiliti, keselamatan dan privasi. Justeru, kajian ini bertujuan menganalisis kerangka undang-undang dan dasar semasa berkaitan perkongsian data di Malaysia, mengenal pasti cabaran yang dihadapi oleh agensi kerajaan, serta membandingkan pendekatan Malaysia dengan amalan terbaik antarabangsa seperti Kesatuan Eropah, United Kingdom, Ireland, Australia dan Singapura. Melalui analisis kandungan undang-undang dan dasar, analisis perbandingan, serta temu bual separa berstruktur bersama agensi kerajaan, kajian ini akan mencadangkan pembaharuan bagi memperkukuh tadbir urus perkongsian data. Hasil kajian dijangka menekankan keperluan prinsip “privacy-by-design”, piawaian tadbir urus data yang seragam, dan mekanisme penyeliaan yang kukuh bagi menggalakkan perkongsian data secara

bertanggungjawab, meningkatkan kepercayaan awam, serta menyelaraskan Malaysia dengan piawaian global berasaskan realiti tempatan.

Kata Kunci: Perkongsian Data, Perlindungan Data, Perkongsian Data Sektor Awam, Privasi, Rangka Kerja Perundangan.

INTRODUCTION

Data has become a cornerstone of modern governance, and effective data sharing across government agencies is no longer optional but essential.[1] Internationally, evidence shows the tangible benefits of systematic data sharing. The Organisation for Economic Co-operation and Development (OECD) estimates that effective data sharing in the public sector can boost Gross Domestic Product by 0.1 to 1.5 per cent, while in the private sector, the gains may reach as high as 2.5 per cent.[2] A 2022 Capgemini study further revealed that a well-structured data ecosystem enables 76 per cent of public agencies to make more efficient decisions, saving up to 9 per cent in operational costs.[3] In critical sectors such as healthcare, the integration of patient data from multiple sources not only improves diagnostic and treatment outcomes but also significantly reduces institutional expenditure.[4] These global findings underscore why data sharing matters for Malaysia. The government has embarked on initiatives such as PADU, MyGDX, and the Open Data Portal to unlock the socioeconomic value of data, but challenges persist. Current practices remain fragmented, shaped by

[1]Sukumar Ganapati and Christopher G. Reddick, "Prospects and challenges of sharing economy for the public sector", *Government Information Quarterly*, vol. 35, no. 1 (2018): 77–87.

[2]The Organisation for Economic Co-operation and Development, "Enhancing Access to and Sharing of Data", The Organisation for Economic Co-operation and Development, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/enhancing-access-to-and-sharing-of-data_070835df/276aaca8-en.pdf.

[3]Capgemini,"Connecting the Dots: Data sharing in the public sector", Capgenmini, https://www.capgemini.com/insights/research-library/data-ecosystems-in-public-sector/.

[4]Renáta Máchová, Miloslav Hub, and Martin Lnenicka, "Usability evaluation of open data portals", *Aslib Journal of Information Management*, vol. 70, no. 3 (2018): 252–268.

administrative circulars and misinterpretations of confidentiality provisions, which hinder effective collaboration. The result is overlapping datasets, inconsistent formats, and limited trust, which together diminish the potential impact of data-driven governance. This paper addresses this research gap by analysing Malaysia's existing legal and policy frameworks on public sector data sharing, identifying the barriers that prevent its optimal implementation, and benchmarking Malaysia's approach against international best practices. Through content analysis, comparative legal review, and semi-structured interviews with government agencies, the study contributes recommendations for a coherent and robust legal framework. By doing so, it seeks to demonstrate how Malaysia can strengthen public sector data governance, balance privacy and security concerns, and ultimately build public trust in government data use.

THE BENEFITS OF DATA SHARING IN PUBLIC SECTOR GOVERNANCE

Data sharing is crucial in modern public sector governance. It facilitates informed decision-making, promotes transparency, and encourages innovation creation. By sharing data across public sector agencies and fostering partnerships with the private sector, the government can more effectively plan programmes and initiatives for community and national development, aligning them with actual challenges and needs.[5] Data sharing allows government agencies to access a wider dataset, thereby enhancing the government's ability to make information-based decisions and policies. Effective data use allows policymakers to be better informed about an issue and subsequently identify actions that can lead to comprehensive solutions. Microsoft asserts that the benefits of data sharing can be maximised when shared for collaborative purposes between agencies. For example, individual data allows governments to identify people's needs for targeted assistance and services.[6]

[5]Wei Xiong, Bin Chen, Huanming Wang, and Dajian Zhu, "Public–private partnerships as a governance response to sustainable urbanization: Lessons from China", *Habitat International*, vol. 95, no. July 2019 (2020): 102095.

[6]Microsoft Stories Asia, "Data Sharing Key to Solving Asia's Biggest Economic and Societal Challenges: Microsoft Asia Whitepaper -

Data sharing also assists research initiatives in contributing towards effective policy formulation and development. Researchers and policymakers have access to data that allows them to analyse trends and evaluate the effectiveness of policies. The Australian Research Data Commons (ARDC) highlights that well-structured data sharing policies are crucial for effective data management and governance in research projects. Such policies facilitate collaboration among researchers and policymakers, enabling them to analyse trends and evaluate policy effectiveness, particularly when addressing multifaceted challenges.[7]

In terms of implementation, data sharing is particularly useful in addressing complex issues. In Malaysia, for example, the National Geospatial Centre collects geospatial data and assists state governments, local governments, and researchers in predicting geographical patterns, determining land suitability for agricultural use, etc. The availability of this data can also provide information in efforts to conserve the environment and habitat.[8]

In addition, the development and use of the *MySejahtera* mobile application are prime examples of the Malaysian government's efforts to manage and control the COVID-19 pandemic by leveraging data. Through the *MySejahtera* application, data on the number of patients and close contacts can be shared. It also contains data on individuals who have been vaccinated, self-assessed their health and checked in to the locations visited. This data helps in contact tracing and monitoring the transmission of COVID-19. The implementation of the decision, guided by *MySejahtera* data, demonstrates the government's

Microsoft Stories Asia", Microsoft Stories Asia, https://news.microsoft.com/apac/2021/09/28/data-sharing-key-to-solving-asias-biggest-economic-and-societal-challenges-microsoft-asia whitepaper/?utm_source=chatgpt.com (accessed 28 February, 2025).

[7]Australian Research Data Commons, "Data Sharing Policy Development Guidelines", Australian Research Data Commons, https://zenodo.org/records/7553182/files/DataSharingPolicyDevelopmentGuidelines.pdf?download=1.

[8]National Geospatial Centre, "About MyGDI | MyGeoportal", National Geospatial Centre, https://www.mygeoportal.gov.my/en/about-mygdi?utm_source=chatgpt.com (accessed 28 February, 2025).

commitment, thereby increasing the level of public trust in the government's efforts to combat the pandemic.[9]

Data sharing can reduce operational costs among government agencies by reducing data duplication. For example, data overlap often occurs for recipients of social services who receive a variety of overlapping assistance from different agencies. With data sharing between agencies, overlapping situations can be avoided. This, in turn, allows assistance to be delivered more accurately at a lower cost of resources, thus reducing the agency's operational costs.

Transparency and accountability are important aspects of good governance in any government administration. The availability and accessibility of data can foster trust between the government and the people, as transparency is achieved through data sharing. This is because stakeholders, including citizens, have access to detailed information about various aspects of government administration and operations. This information allows the people to better understand the Government's decisions regarding an initiative and the use of public funds.

For example, the Malaysian Government Open Data Portal allows citizens to gain access to a wide range of public data, such as the economy, education, and health, giving them space to make their own assessments and monitor policy implementation.[10] The Public Financial Management System (FMIS) facilitates the sharing of financial data between agencies. Meanwhile, the *ePerolehan*, *eHealth*, and *eParticipation* systems demonstrate how data sharing can increase transparency in the tender, healthcare, and implementation processes of government projects. With the implementation of these initiatives, Malaysia continues to move towards more open, efficient, and accountable governance.

During a crisis, data sharing simplifies the process of coordinating and managing responses. In times of crisis, authorities are usually faced with uncertainty but require an immediate and accurate

[9]Government of Malaysia, "What is MySejahtera? : MySejahtera", Government of Malaysia, https://helpdesk.mysejahtera.malaysia.gov.my/en/support/solutions/articles/51000293086-what-is-mysejahtera (accessed 28 February, 2025).

[10]The Government of Malaysia, "Malaysia's Official Open Data Portal", The Government of Malaysia, https://data.gov.my/ (accessed 2 March, 2025).

response. With data sharing, agencies involved in disaster management can obtain detailed information. This allows them to make decisions that are responsive to crises immediately.

During the COVID-19 pandemic, for example, the availability of public health data allowed policymakers to accelerate the response and bring the situation under control. Data sharing has helped monitor the pandemic situation, and this contributes significantly to the control and prevention of infectious diseases.[11] The development of the *MySejahtera* system increases Malaysia's preparedness in the face of any future health crises. Furthermore, the availability of data will speed up the distribution of assistance to either the affected individuals or businesses. Furthermore, the government will also be able to accurately identify critical needs in the health sector and channel funds accordingly.

The benefits of data sharing can also be seen in the law enforcement sector. Comprehensive and up-to-date data on criminal activity, missing persons, or potential dangers is very useful in protecting the safety of citizens. Data sharing among law enforcement and public security agencies has the potential to improve crime detection and prevention capabilities.[12]

---

[11]United Nations Office for Disaster Risk Reduction, "Global assessment report on disaster risk reduction 2019", United Nations Office for Disaster Risk Reduction (UNDRR), https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2019 (accessed 2 March, 2025). This report discusses the importance of data sharing in disaster management and coordination.

[12]Kevin Strom, *Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report.*, (Washington, *National Criminal Justice Reference Service*, 2017). The document highlights the importance of data sharing in policing through search and data-sharing software like SharePoint, which enhances service response, investigations, and officer tracking. Regional and national information-sharing programs such as NLETS and COPLINK facilitate crime-related data exchange across jurisdictions, improving intelligence gathering. Crime mapping and data mining tools play a crucial role in directing patrols, follow-up investigations, and community intelligence generation. Information-sharing software is among the top innovations aiding law enforcement, significantly improving investigations. Agencies with robust data-sharing systems report increased efficiency in resource deployment, crime trend

Effective public sector data sharing can stimulate economic growth and create new job opportunities. With easy access to quality data, companies and organisations can come up with new innovations, increase productivity, and expand the digital economy. This data sharing not only benefits large companies, but also opens doors to small and medium businesses (SMEs). This allows SMEs to compete in the global market, which in turn has a positive impact on the economy and the people.

In addition, data sharing also plays an important role in improving the quality of life of the people and improving environmental sustainability. With data collected from a variety of sources, including sensors and tools, developments in areas such as health, education, and climate change can be accelerated.[13] For example, sensor data in agriculture allows farmers to reduce excessive water and chemical use, achieving better economic and environmental outcomes. Generally, the practice of data sharing can have significant socioeconomic impacts, including improvements in the quality of policy-making aspects, reduction in inequality, and general improvements in people's well-being.[14]

---

analysis, and evidence-based decision-making, ultimately strengthening community relations and crime prevention efforts.

[13]The Organisation for Economic Co-operation and Development, "G20 Compendium on Data Access and Sharing Across the Public Sector and with the Private Sector for Public Interest", The Organisation for Economic Co-operation and Development, https://www.oecd-ilibrary.org/governance/g20-compendium-on-data-access-and-sharing-across-the-public-sector-and-with-the-private-sector-for-public-interest_df1031a4-en.

[14]World Economic Forum, "How Can SMEs Become Data-Driven Enterprises?", World Economic Forum, https://www.weforum.org/stories/2023/06/how-can-smes-become-data-driven-enterprises/?utm_source=chatgpt.com; ISO, "Smart Farming: Data-Driven Agriculture", ISO, https://www.iso.org/smart-farming/smart-farming-data-driven?utm_source=chatgpt.com; The Organisation for Economic Co-operation and Development, "G20 Compendium on Data Access and Sharing Across the Public Sector", The Organisation for Economic Co-operation and Development, https://www.oecd.org/en/publications/g20-compendium-on-data-access-and-sharing-across-the-public-sector-and-with-the-private-sector-for-public-interest_df1031a4-en.html?utm_source=chatgpt.com; European Data Portal, "Creating

DATA SHARING INITIATIVES

The Malaysian government is focusing on data sharing initiatives as a strategic step to stimulate the country's economic growth. Data sharing, which was initially introduced to provide data to individual agencies, has now evolved into an asset that can be accessed and leveraged by a wide range of stakeholders. In this regard, the Government has set up a Data Sharing Platform, known as the Malaysian Government Central Data Exchange (MyGDX) and MyGovCloud@PDSA Cloud Computing Services and Cloud Framework Agreement (CFA) for data storage. All these efforts support data sharing in developing government digital services for the people and making more effective decisions at the top levels of the government.

The Pangkalan Data Utama (PADU) was developed collaboratively using internal expertise from the Kementerian Ekonomi, Jabatan Perangkaan Malaysia, and Unit Pemodenan Tadbiran dan Perancangan Pengurusan (MAMPU), with the cooperation of various data-providing agencies.[15] PADU is a database system that contains individual and household profiles of Malaysian citizens aged 18 and above residing in Malaysia. It is designed to assist the government in implementing targeted policies to enhance the efficiency of policy planning and resource distribution, particularly for subsidies and government assistance, ensuring that they reach those who are genuinely eligible. The database is updated regularly through the integration of administrative data from multiple sources, and rakyat

---

Value Through Open Data", European Data Portal, https://data.europa.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf?utm_source=chatgpt.com; Wired, "Environmental Sensing Is Here, Tracking Everything from Forest Fires to Threatened Species", Wired.com, https://www.wired.com/story/environmental-sensing-is-here-tracking-everything-from-forest-fires-to-threatened-species?utm_source=chatgpt.com; Reuters, "From Field to the Cloud: How AI is Helping Regenerative Agriculture to Grow", Reuters, https://www.reuters.com/sustainability/land-use-biodiversity/field-cloud-how-ai-is-helping-regenerative-agriculture-grow-2024-09-18/?utm_source=chatgpt.com.

[15]Pangkalan Data Utama (PADU),"Pangkalan Data Utama (PADU)", Pangkalan Data Utama (PADU), https://www.padu.gov.my/soalan-lazim (accessed 2 March, 2025).

can review and update their information directly within the system. PADU aims to provide a secure, comprehensive, and near real-time national database for periodic analytics and digitalisation, facilitate data-driven policy-making and decision-making, and balance fiscal positions through targeted policy implementation. Its objectives include improving government service delivery efficiency, strengthening the utilisation of limited resources, empowering social systems to enhance economic and societal well-being, and narrowing socio-economic disparities by meeting the needs of the rakyat while balancing development. Data collected for PADU includes information from government agencies, individual updates, and data derived from analysis. Although different government agencies operate various systems, the PADU team ensures data accuracy through cross-verification.

In addition to PADU, the Portal Data Terbuka Rasmi Malaysia serves as a one-stop centre for Data Terbuka Sektor Awam (DTSA) in Malaysia, featuring dashboards, data catalogues, and API documentation. It caters to diverse users, including rakyat seeking information, researchers sourcing data, and developers utilising APIs. The implementation of open data in the public sector was initiated following the 2014, which required all government agencies to identify datasets for open data implementation. This initiative was later formalised through Pekeliling No. 1/2015 Data Terbuka Sektor Awam, with objectives to promote data sharing among public and private sectors and rakyat, enhance data quality and government service transparency, and drive digital economic productivity through industry engagement and innovation.

Open data encompasses only unclassified information, while classified data is managed under MyGDX, a centralised government data-sharing platform established in 2016.[16] MyGDX standardises data-sharing mechanisms across government agencies, optimising resource usage and ensuring data security. Unlike the Portal Data Terbuka Rasmi Malaysia, which is freely accessible, data in MyGDX requires authorisation from the data owner. It consists of components such as Security Server, Trust Service, Registry, Monitoring, Directory,

[16]Department of Digital Malaysia, "MyGDX | Malaysian Government Central Data Exchange", Department of Digital Malaysia, https://www.mygdx.gov.my/ms/landing-page/theme (accessed 2 March, 2025).

and Portal to ensure secure and efficient inter-agency data sharing.[17] MyGDX is a data-sharing ecosystem that aims to strengthen and enhance fully online (end-to-end) service delivery towards a data-driven government. The implementation of MyGDX enables more efficient coordination of inter-agency data sharing while reducing the cost of infrastructure development and system integration. This unified platform also facilitates smoother and more consistent data integration across various government systems.[18]

In addition, the establishment of the Government Open Data portal is implemented to enable data to be freely used, shared and reused by citizens, governments and public agencies for various purposes. This can increase the transparency of public service delivery through accurate, fast and relevant data sharing while increasing the productivity of the country's digital economy. The government's latest initiative on data sharing is PADU, which is the country's main comprehensive and up-to-date database. This allows for an increase in the efficiency of the Government's service delivery system.

Malaysia is formulating the Digital Trust and Data Security Strategy 2026–2030 as a long-term roadmap to strengthen national resilience against emerging digital threats, advance data integrity, and foster public confidence in digital transformation and the use of artificial intelligence (AI). Central to this initiative is the establishment of an independent Data Commission that will serve as an oversight body to ensure robust data governance and promote ethical AI practices. The strategy seeks to build a comprehensive national ecosystem that supports secure and responsible data-driven infrastructure, enabling Malaysia to fully harness the benefits of digitalisation while safeguarding privacy and security. Ultimately, the strategy aims to reinforce both public and investor confidence in Malaysia’s digital future through the implementation of clear

[17]Government Central Data Exchange, "MyGDX | Malaysian Government Central Data Exchange", Government Central Data Exchange, https://www.mygdx.gov.my/ms/landing-page/architecture?theme=second-theme (accessed 17 October, 2025).

[18]Department of Digital Malaysia, MyGDX, Malaysian Government Central Data Exchange.

regulatory and governance frameworks backed by effective enforcement.[19]

PROBLEM STATEMENT

Although data sharing has long been practised between public sector agencies in Malaysia, there are still issues and challenges that hinder effective data sharing. These issues and challenges are explained as follows:

a) Legislation in force that restricts data sharing

There are federal acts and state enactments/ordinances that contain provisions that prohibit data sharing. Such barriers usually exist in the form of confidentiality provisions that essentially protect the information collected from being exposed to unauthorised parties under the law.[20] Such legal provisions are intended to ensure that the data shared complies with the stipulated data requirements and

[19]Bernama, "Data Commission key to strengthening governance and protection, says Gobind", Bernama, https://theedgemalaysia.com/node/767318 (accessed 17 September, 2025).

[20]See for example, Sections 16(2) and 19 and 20 of the Census Act 1960. Any member of a committee appointed under subsection 4(1), any census officer, or any individual employed to prepare summaries under section 15 who discloses or uses information obtained in the course of their duties, except for purposes permitted under this Act, commits an offense and, upon conviction, may be fined up to RM2,000, imprisoned for up to one year, or both. Additionally, no individual statement containing details or information related to any business, employment, or work may be published without prior written consent from the relevant authority. Unauthorized persons not engaged in census-related duties are prohibited from accessing such statements, except for prosecution under this Act or under prescribed conditions. In drafting regulations and forms under section 6, due consideration must be given to various commercial and industrial circumstances, particularly to prevent the disclosure of trade secrets, commercial profits, or any other information that may be detrimental to the person providing the statement. Furthermore, census records are confidential and may not be admitted as evidence in any civil or criminal proceedings, except in prosecutions initiated under this Act concerning specific records made, signed, or submitted by an individual responsible for their creation.

classifications, protects data privacy and minimises the leakage of personal data. However, such provisions are often misunderstood by agencies as legislation that restricts data sharing. In addition, the agencies responsible for collecting and storing data feel bound by a contract to maintain the confidentiality of individual data. These legal constraints also complicate obtaining permission for data sharing, and it takes a long time. For confidential and highly sensitive data, for example, there is uncertainty about obtaining permission to share data.

b) Lack of awareness and understanding among agencies regarding confidentiality provisions has caused agencies to be overly cautious

Although the restrictions on data sharing in the legislation are framed in specific contexts or uses, agencies have been found to take a very cautious approach by not allowing any form of data sharing for fear of violating the provisions of their own laws. In fact, there are also situations where even though the Act does not have any requirements to restrict data sharing, there are regulations, guidelines, or codes of practice that prevent data sharing. For example, from an engagement session conducted with the Ministry of Health (MOH) on 17 November 2023 at the National Digital Department, MOH representatives stated that the Medical Act 1971 [Act 50] is the reason why every information sharing requires consent from the data subject or the patient themselves.[21] This will not be compromised by the MOH to protect public trust in the country's health institutions now and in the future as well as to guarantee the right to privacy of patients.

Notwithstanding what the MOH said, further research on Act 50 indicates that none of the federal acts and state enactments related to public health prohibit data sharing or have confidentiality provisions that prevent civil servants or any person from sharing data and information. However, the obligation of confidentiality is an international practice that is adhered to as part of medical best practices worldwide, including Malaysia.[22] As such, it would be inaccurate to

[21]Ministry of Health (MOH), Focus Group Discussion on Data Sharing and the Medical Act 1971 [Act 50] (National Digital Department, November 17, 2023).

[22]See World Medical Association's (WMA) Declaration on Confidentiality, which emphasizes that confidentiality is essential for maintaining trust and integrity in health databases and biobanks. See also the International

say that current legislation prevents data sharing in public health aspects, which is a reason to reject data sharing. This is one clear example where data sharing is hindered by instruments that are not of legislative status. This includes guidelines, codes of practice or international practices that complicate and prevent public sector agencies from sharing data. Among the issues raised are threats to data security and privacy. In addition, the issue of data quality and accuracy has also affected efforts to make the data sharing agenda between government agencies a success. This has made data sharing between the public sector unable to be implemented effectively. This problem is further complicated by the use of different formats in data collection and recording in public agencies.[23]

In terms of sports development, for example, the Sports Development Act 1997 [Act 576] does not contain a confidentiality provision that prevents data sharing. However, through an engagement session conducted on 30 and 31 October 2023, a representative of the Ministry of Youth and Sports stated that some types of information related to key athletes such as Dato Lee Chong Wei cannot be arbitrarily disclosed to any other agency even if it is in the interest of the country.[24] For example, the data on the cost that countries have spent to develop world-class athletes in terms of training and nutrition.

Ethical Guidelines for Health-related Research Involving Humans, published by the Council for International Organizations of Medical Sciences (CIOMS), highlight that health-related data may contain a very large range of information, and therefore, an important aspect of storing health-related data is confidentiality.

[23]The Organisation for Economic Co-operation and Development, *Enhancing Access to and Sharing of Data*, (The Organisation for Economic Co-operation and Development, *Enhancing Access to and Sharing of Data*, 2019b). See also Bruno Miguel Vital Bernardo, Henrique São Mamede, João Manuel Pereira Barroso, and Vítor Manuel Pereira Duarte dos Santos, "Data governance & quality management—Innovation and breakthroughs across different fields", *Journal of Innovation & Knowledge*, vol. 9, no. 4 (2024): 100598; Ilka Jussen, Frederik Möller, Julia Schweihoff, Anna Gieß, Giulia Giussani, and Boris Otto, "Issues in inter-organizational data sharing: Findings from practice and research challenges", *Data & Knowledge Engineering*, vol. 150 (2024): 102280.

[24]Ministry of Youth and Sports (KBS), Focus Group Discussion on Data Sharing and Sports Development Act 1997 [Act 576], National Digital Department, October 30–31, 2023.

This is not stated as classified information under the Official Secrets Act 1972 [Act 88] and illustrates a certain misunderstanding when the data and information may be deemed a sensitive issue of the ministry concerned.

c) Lack of data format uniformity and data overlap

A common data format or protocol is fundamental to ensuring that data sharing across government agencies is seamless, efficient, and reliable. When agencies collect and store data in different formats or systems, it creates silos that hinder interoperability, leading to duplication, overlap, and inconsistencies[25]—as seen with databases like PADU, MyGrants, and iDme. Without a standardised protocol, agencies may struggle to integrate datasets, verify authenticity, or determine which version of data is most accurate and up to date. This not only wastes resources but also undermines policymaking and service delivery, as decisions may be based on incomplete or conflicting information.[26]

When each agency collects data separately according to the needs and scope of its respective agency, there are situations where the data collected is overlapping, redundant or unnecessary. Each government agency uses government allocations to set up its own databases, such as PADU for the Ministry of Economy, MyGrants for research data in the Ministry of Higher Education and Identity Management System (iDme) for the Ministry of Education.

At the same time, these systems collect data and information in a non-uniform and overlapping format. For example, the Ministry of Education's system collects students' personal information and at the same time, the same data is also collected by the National Registration Department and the Department of Statistics Malaysia through census activities and so on. This causes various government agencies to collect information in different formats and the same information is also collected across agencies. Apart from causing format inconsistencies, it also raises the issue of which agency holds the most up-to-date and

[25]OECD, "OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem", OECD Digital Education Outlook, https://www.oecd-ilibrary.org/education/oecd-digital-education-outlook-2023_c74f03de-en.

[26]Ahmad Ashraf Ahmad Shaharudin, "Open government data in Malaysia: Landscape, challenges and Aspirations", *Khazanah Research Institute*, no. 3/21 (2021): 1–45.

authentic data that can be referenced.

Therefore, these challenges are overcome by establishing clear data-sharing laws. This is to enable public agencies to improve the data sharing process as well as provide privacy protection and maintain data security effectively. Clear provisions on the data sharing process can provide transparency to, not only the agencies involved but also the citizens. Overall, this can increase the confidence of the people and subsequently contribute towards the success of data sharing initiatives in Malaysia.

d) Privacy concerns and security risks

Although data sharing was already in practice between government agencies before the enactment of the Data Sharing Act 2025, some agencies refuse to share data for certain reasons. According to the interview session conducted by the author, privacy concerns and data security risks are the main factors why some agencies do not want to share data, especially when the data is sensitive and has a classified information status under the Official Secrets Act 1972 [Act 88]. In cases of breach of classified information or data leaks, public servants have been investigated and prosecuted for breaching their confidentiality obligations under Act 88.[27]

In addition, cyberattacks targeting government agencies have also exacerbated data security and data privacy issues. According to the World Economic Forum in its 2024 Global Cybersecurity Outlook Report, 54 per cent of organisations have limited cybersecurity capabilities to detect and identify cyber vulnerabilities or vulnerabilities in their supply chains.[28] Additionally, 41 per cent of organisations that experienced cybersecurity incidents in 2023 were caused by third parties. Meanwhile, IBM in its Report on the Cost of Data Leakage, outlined that an average of USD 4.45 million was incurred by organisations due to data leakage in 2023, seeing an increase of 15 per cent over three (3) years.[29]

---

[27]See for example, Public Prosecutor v Subbarau @ Kamalanathan [2017] 6 MLJ 434.

[28]World Economic Forum, "Global Cybersecurity Outlook 2024 | World Economic Forum", World Economic Forum, https://www.weforum.org /publications/global-cybersecurity-outlook-2024/.

[29]IBM Corporation, "Cost of a Data Breach Report 2024", IBM Security, https://www.ibm.com/security/data-breach.

Cyberattacks target government agencies because these institutions hold vast amounts of sensitive, high-value information—such as citizens' personal data, national security intelligence, and critical infrastructure systems—that can be exploited for political, financial, or strategic gain. Governments are also increasingly digitised, making them attractive entry points for attackers seeking to disrupt public services, undermine trust in institutions, or gain leverage through espionage.

Statistics from the National Cyber Security Agency (NACSA), an agency under the National Security Council, Prime Minister's Department (MKN JPM), show that the trend of cyber-attacks such as Distributed Denial of Service (DDOS), Intrusion, Malware Infection, Malware Hosting and Advanced Persistent Threat (APT) increased from 2016 to 2022.[30] In 2022, a total of 7,192 cybersecurity incidents were reported to NACSA compared to 5,575 in 2021 and 4,194 in the previous year.[31]

However, there are positive developments as cybersecurity incidents in 2023, as of December 31, 2023, have dropped significantly to 3,232 cases.[32] This decline reflects the effectiveness of proactive measures implemented to protect our cyberspace. Therefore, the proactive measures implemented need to be expanded in a coordinated manner to ensure that the detection and response period to cyber security incidents can be shortened through systematic processes, the us.

THE LEGAL FRAMEWORK OF PUBLIC SECTOR DATA SHARING IN MALAYSIA

Prior to the enactment of the Data Sharing Act 2025 [Act 864], data sharing amongst public sector agencies was governed by administrative directives.[33] Recognising the need for a stronger legal

[30]Parliament of Malaysia, "Dewan Rakyat Parlimen Kelima Belas Penggal Ketiga Mesyuarat Pertama Rabu 27 Mac 2024", Parliament of Malaysia.

[31]Parliament of Malaysia, Dewan Rakyat Parlimen Kelima Belas Penggal Ketiga Mesyuarat Pertama Rabu 27 Mac 2024.

[32]Parliament of Malaysia.,37.

[33]See, for example, *Dasar Perkongsian Data Sektor Awam* published by the National Digital Department Malaysia. Each agency has its internal data

framework, the enactment of the Data Sharing Act 2025 facilitates and regulates data sharing among public sector agencies in the federal government, which includes statutory bodies established under federal laws. Section 2 provides that the Act is binding on the Federal Government and is intended to complement, not derogate, existing laws that allow for data sharing. The Data Sharing Act 2025 shall be read together with the provisions of other written laws which allow for data sharing to be made, subject to the conditions provided under such laws, and the provisions of this Act shall be in addition to, and not in derogation of, the provisions of the relevant written laws. Any person who shares data under the Data Sharing Act 2025 is deemed to have made such disclosure pursuant to the provisions specified in column (3) under the laws specified in column (2) of the Schedule. Any data of the public sector agency shall be dealt with in accordance with the Official Secrets Act 1972 [Act 88] and any directives relating to the security of official documents issued by the Government.

To operationalise its mandate, the Data Sharing Act 2025 establishes the National Data Sharing Committee,[34] which is responsible to the Cabinet. The Committee comprises representatives from key government ministries and agencies, including the Prime Minister's Department, the National Cyber Security Agency, and the Personal Data Protection Department. Its statutory functions under Section 6 include formulating policies and strategies for data sharing, resolving administrative challenges, and promoting secure and efficient data use across government entities. The Committee is empowered to issue procedures and risk assessment frameworks to safeguard data integrity and privacy.

On data governance, the Director General of the National Digital Department is vested with statutory duties and powers under Section 11 to implement the Committee's policies, facilitate inter-agency data sharing, issue guidelines, and require information from public bodies. The Director General serves as the Committee's Secretary and acts as a central authority in ensuring compliance with the Act. However, it is noteworthy that the Data Sharing Act 2025 does not allocate regulatory or enforcement powers to the National Digital Department or any other

sharing policies that reflect the *Dasar Perkongsian Data Sektor Awam*, for example, the Public Service Department via *Garis Panduan Perkongsian Data Jabatan Perkhidmatan Awam.*

[34]Section 5.

public sector agency. This suggests a focus on coordination, as similar initiatives are being adopted by other countries, including Australia and the United Kingdom.

On the other hand, requests for data sharing among public sector agencies are governed under Part IV. Section 12 outlines the procedural requirements, including the nature of the requested data, its purpose, and the handling protocols. Permissible purposes for data sharing under Section 13 include enhancing public service delivery, managing public emergencies, and acting in the public interest. The receiving agency must evaluate the request based on criteria such as public interest and security safeguards before responding within 14 days.[35]

However, under Section 15, the data provider may refuse to share data on specific grounds, such as threats to national security, breach of legal privileges, or lack of adequate data protection by the requesting agency. Importantly, refusal is also justified where the requested data is inconsistent with the purposes outlined in Section 13 or where disclosure could endanger individual welfare or ongoing investigations by enforcement agencies.

Section 16 imposes a statutory duty on both data providers and recipients to safeguard the shared data. This includes maintaining data confidentiality, ensuring legal compliance, keeping detailed records, and reporting unauthorised access to the Director General. When data is handled by a third party, such as for data integration or analytics, Section 17 mandates prior consent from the data provider, with penalties for third-party breaches reaching up to RM1 million- or five-years' imprisonment.

Sections 18 to 21 introduce further compliance obligations. Section 18 restricts data recipients from using the shared data for purposes other than those originally agreed upon, with non-compliance attracting criminal penalties. Section 20 encourages the sharing of open data and allows access to open data without formal requests under Section 12. Public sector agencies are required to periodically report data sharing activities to the Director General under Section 21, thereby supporting transparency and accountability.

[35]Section 14.

THE LEGAL FRAMEWORK ON DATA SHARING IN OTHER COUNTRIES: A COMPARATIVE OVERVIEW

This part explores the practices in three countries, namely, the European Union, the United Kingdom, Ireland and Australia, to understand the legislation and best practices to be considered as far as the legal framework on data sharing is concerned. Unlike data protection regimes, these three countries were selected on the basis that they each possess data sharing frameworks, in the form of statutes, policies, and guidelines, which are not common among many countries worldwide. We will begin the analysis with the United Kingdom as follows.

The European Union (EU)

The EU develops legislation and policies aimed at ensuring the free movement of people, goods, services, and capital within its internal market. In the context of data sharing, EU legislation highlights the crucial role of data access and reuse across various economic and scientific sectors, promoting shared benefits such as mobility transition, digitalisation, and climate crisis management. The EU Data Governance Act 2022 (DGA), adopted by the European Parliament on April 6, 2022, entered into force on June 23, 2022, and became applicable on September 24, 2023, after a transitional period of 15 months. The Act establishes a comprehensive legal framework for data sharing within the EU's single market, ensuring neutral access to data, interoperability, and preventing lock-in effects. As an EU Regulation, the DGA directly applies across all EU member states without requiring further enactment at the nation-state level.

The DGA addresses key areas, including the reuse of public-sector data that might involve third-party rights, facilitating data sharing among businesses (with or without remuneration), permitting the use of personal data through regulated data intermediaries, and encouraging data altruism (voluntary data sharing for the public good). It complements Directive (EU) 2019/1024 on open data by specifically covering data not addressed by that directive. The DGA emphasises trust in data intermediaries and draws inspiration from FAIR principles (Findable, Accessible, Interoperable, and Reusable), promoting efficient and secure data use.

Currently, specific sectoral legislation exists in industries like automotive, payment services, electricity grids, intelligent transport systems, environmental information, spatial data, and healthcare. In the financial sector, the Payment Services Directive 2 (Directive (EU) 2015/2366) mandates open banking, requiring banks to provide third-party providers with secure access to customer data upon consent. In the spatial and environmental domains, the INSPIRE Directive (Directive 2007/2/EC) creates a legal structure for interoperable spatial data sharing across Member States. Similarly, in the healthcare sector, the European Health Data Space Regulation (Regulation (EU) 2025/327) and the Directive on Patients' Rights in Cross-border Healthcare (Directive 2011/24/EU) ensure that health data can be accessed, exchanged, and reused for both clinical and research purposes, thereby promoting cross-border interoperability in healthcare services.

Other sectors are also governed by dedicated frameworks that embed data-sharing obligations. The electricity and energy industries, for instance, operate under EU network codes and transparency rules that require grid operators to share data essential for system balancing and market efficiency. The Intelligent Transport Systems (ITS) Directive (Directive 2010/40/EU) ensures data interoperability and accessibility in transport and mobility services, while ongoing initiatives in the automotive industry aim to regulate fair access to in-vehicle data and connected systems. Collectively, these legislative instruments illustrate the EU's commitment to a harmonised data ecosystem that supports innovation, competition, and cross-sectoral integration within its single market.

The DGA supports existing data use regulations without modifying current sector-specific rules or creating new obligations. It respects EU competition laws and aligns with Articles 101 and 102 of the Treaty on the Functioning of the European Union, as well as the Directive on electronic commerce (2000/31/EC). The DGA was developed as part of the EU's 2020 Strategy to strengthen the single market for data, reducing risks of fragmented regulations by establishing harmonised governance structures for cross-border data flows.

Features of the EU Data Governance Act 2022

The DGA enables controlled data sharing through technical safeguards such as anonymisation, pseudonymization, and secure data environments. It defines rules for data intermediation services—such as data marketplaces—and data altruism, where individuals or companies voluntarily share data publicly. Public bodies can reuse data for purposes other than those originally intended, provided that privacy and confidentiality measures are in place, including conditions that must be transparent, fair, and non-discriminatory. Each EU member state must establish a supervisory authority as a central data-sharing hub and maintain a register of public-sector datasets. These supervisory bodies are overseen by the European Data Innovation Board (EDIB), which manages a central registry.[36]

The DGA limits exclusive data-sharing arrangements to a maximum duration of 12 months, with existing exclusive agreements terminating within three years of the Act's enforcement. It allows public bodies to charge reasonable fees for data access, which must be transparent and non-discriminatory. For data transfers outside the EU, the DGA mirrors EU General Data Protection Regulation (GDPR) mechanisms, requiring adequacy decisions to safeguard data transferred internationally.

The licensing regime ensures intermediaries operate independently, uphold data security, and maintain confidentiality. Once licensed, intermediaries can display an official compliance logo, charging reasonable fees without exploiting data for personal profit. Data intermediaries must remain neutral, structurally separate their services from other activities, and notify supervisory authorities about their operations. After notification, intermediaries are permitted to use the label 'recognised EU data intermediation service provider.' Examples include Deutsche Telekom's Data Intelligence Hub[37] and

[36]Jukka Ruohonen and Sini Mickelsson, "Reflections on the Data Governance Act", *Digital Society*, vol. 2, no. 1 (2023): 1–9.

[37]Fraunhofer Institute for Experimental Software Engineering IESE, "Deutsche Telekom AG Success Story – Secure Data - Fraunhofer IESE", Fraunhofer Institute for Experimental Software Engineering IESE, https://www.iese.fraunhofer.de/en/reference/deutsche-telekom-secure-data-marketplace (accessed 18 October, 2025).

Dawex,[38] a French company providing platforms to securely facilitate direct interactions between data providers and users, promoting transparency and neutrality. API-AGRO is another example, a neutral agricultural data-sharing platform leveraging Dawex's technology to foster transparent and efficient data use within the farming ecosystem.[39]

The DGA introduces the concept of 'data altruism', encouraging individuals and organisations to voluntarily share their data for public interest projects like scientific research or public service improvement. Participating organisations must register with national supervisory authorities and obtain explicit consent through specific data altruism forms for data processing activities.

The EDIB facilitates best-practice sharing and comprises representatives from national supervisory authorities, the European Data Protection Board, the European Data Protection Supervisor, the EU Cybersecurity Agency, the European Commission, SME representatives, and other relevant stakeholders. The EDIB operates through specialised sub-groups focused on authority coordination, technical discussions, and stakeholder engagement. It provides guidelines, such as those governing cross-border data transfers.[40]

The Data Act 2023, effective from January 11, 2024, complements the DGA by clarifying data access rights and promoting fair value distribution from data usage, especially in Internet of Things (IoT) environments. The Act specifies clear rules to prevent unfair contractual practices and facilitate equitable data sharing between private and public sectors, particularly during emergencies. It encourages innovation, job creation, and competitive pricing in IoT services, directly benefiting consumers and businesses alike.

[38]Dawex, "Data Exchange technology compliance | Dawex", Dawex, https://www.dawex.com/en/data-exchange-technology/compliance/ (accessed 18 October, 2025).

[39]Agdatahub, "Company – Agdatahub", Agdatahub, https://agdatahub.eu/entreprise/ (accessed 18 October, 2025).

[40]See Article 53-54 of the EU Data Governance Act, also referred to as Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724.

United Kingdom

In the United Kingdom, data sharing is administered under the Information Commissioner's Office. This office reports directly to the UK Parliament. The Digital Economy Act 2017 (DEA) includes provisions for public sector data sharing with the aim of encouraging the use of public sector data for research, innovation, and public service improvement while ensuring appropriate protections for privacy and security.

Part 5 of the DEA focuses on digital government, providing a gateway that allows certain public authorities to share data with each other. Some of these gateways allow the sharing of personal data, while others allow the sharing of non-identifying data. The objectives and purposes of data sharing under the authority of the DEA are strictly defined.

Section 5 of the DEA expressly states that all information processed under the DEA's authority must comply with data protection laws and prohibits the disclosure of information where it would violate data protection laws. The authority to share information under Part 5 of the DEA is authorised if it coincides with a statutory code of practice (DEA code) that must be consistent with the data sharing code of practice.

There are also provisions that facilitate the sharing of data by and with the Statistical Board to enable the production of statistics, the disclosure of information by public registration officers, and the Revenue Authority,[41] and the sharing of data for research purposes.[42] The DEA does not currently cover data sharing related to health care and social care provision.

In addition, anyone who discloses information under the authority of DEA Part 5 must also take into account other codes of practice issued by the Information Commissioner. This includes identifying elements that mitigate the privacy risk of any information disclosure and how the information collected from them will be used.

[41]Section 78-79.
[42]Section 64.

Section 35 of the UK DEA outlines the process of disclosing information to improve public service delivery. It includes the following key points:

1. One can share relevant information to perform the statutory duties of an agency.
2. The relevant authorities must consider security measures regarding the information collected and should comply with the relevant code of practice.
3. The disclosure of such information shall be to achieve a "Specific objective" referring to the objective defined by the regulations established by the relevant national authority. The objective is to improve or target public services for individuals or households or facilitate the provision of benefits to individuals or households, whether in financial form or otherwise.

Personal information shared by the Revenue and Customs Department under certain sections 35, 36, or 38 may not be further disclosed by the recipient of such information. In other words, the recipient must not share or disclose this information to the public. An exception exists if the disclosure is made with the consent of the Commissioner of Revenue and Customs. Such consent can be general or specific. If a person is charged with an offence under subsection (3), they can defend themselves by proving that they reasonably believe whether the disclosure is lawful or that the information has been lawfully made available to the public.

The DEA enables the sharing of personal information received by the Department of Revenue and Customs and specifies the conditions under which such disclosure is allowed. Violations of these restrictions may result in criminal charges against the person with whom the data was shared unless he or she can prove a reasonable belief that his or her actions were lawful or that the information was already publicly available. The DEA has disclosure-related provisions to address public sector debt and outlines the rules and conditions for such disclosures. Debts incurred by public authorities or the government include the amount of unpaid money still outstanding after the maturity date of the debt. Actions can be taken on these debts, including identifying, collecting, initiating civil proceedings, and taking administrative steps.

Ireland

Ireland has also embraced digital transformation to enhance public services and governance in recent years. The Chief Government Information Officer (CIO) spearheads the government-wide digital agenda, collaborating with departments and agencies to implement shared services, digital identification, and data-driven initiatives. This effort aligns with the Digital EU 2030 strategy, positioning Ireland as a leader in digital innovation. The CIO also supports the implementation of EU laws and regulations, providing strategic input to ministers and participating in national and international working groups.

A cornerstone of Ireland's digital strategy is the Public Service Data Strategy 2019-2023, which aims to transform data management across the public sector. The strategy envisions a cohesive data ecosystem that improves service delivery, policy formulation, and data transparency. Key objectives include providing integrated digital services, enhancing data protection, and reducing the need for citizens and businesses to repeatedly provide the same information. The strategy builds on existing initiatives like the National Data Infrastructure (NDI) and emphasises data governance, security, and reuse.

To implement this strategy, the Data Governance Unit (DGU) was established in 2020 under the Office of the Chief Government Information Officer (OGCIO).[43] The DGU supports the Minister for Public Expenditure and Reform in fulfilling responsibilities under the Data Sharing and Governance Act 2019 (DSGA). It comprises three teams: Data Policy, Data Governance Support, and Data Analytics. The Data Policy team designs standards and guidelines for data management, while the Data Governance Support Team oversees the review process for data sharing agreements. The strategy's implementation is modular and incremental, with each action contributing to the broader goal of a secure, transparent, and efficient data ecosystem.[44]

[43]Office of the Government Chief Information Officer, "Data Governance - ogcio.gov.ie", Data Governance, https://www.ogcio.gov.ie/en/corporate-pages/policy/data-governance/ (accessed 18 October, 2025).

[44]Office of the Government Chief Information Officer, "Data Governance - ogcio.gov.ie",id.

The DSGA, enacted in March 2019, complements the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018. It provides a legal framework for sharing personal data between public bodies while safeguarding individual rights. Section 64 of the DSGA empowers the Minister for Public Expenditure and Reform to introduce data management standards, establish a Basic Registry, and create a Data Governance Board. The Basic Registry ensures consistent and accurate information across public bodies, reducing duplication and improving efficiency. The Data Governance Board, established under Section 45 of the Data Sharing and Governance Act 2019, advises the Minister on data sharing rules, monitors compliance, and reviews data sharing agreements. It comprises six to twelve members, appointed based on their expertise in data protection and governance.

Section 21 of the DSGA also introduces the concept of a 'lead agency' in data sharing agreements. This agency is responsible for updating agreements, notifying parties of changes, and addressing requests from individuals regarding their data rights under the GDPR. Additionally, the DSGA mandates the creation of a Data Sharing Agreement Register, which catalogues all agreements and withdrawals, ensuring transparency and accountability. The DGU maintains this register, providing secretariat support to the Minister.[45]

The Public Service Data Strategy and the DSGA reflect Ireland's commitment to ethical data governance and digital innovation. These initiatives aim to improve service delivery, enhance data protection, and promote transparency by fostering collaboration across public bodies.[46] The strategy's guiding principles emphasise data security, governance standards, and the reuse of data for public benefit. It also empowers citizens by enabling them to access information about how their data is processed, fostering trust in public institutions.

[45]This Data Sharing Agreement Register (the Register) fulfils the obligation under Section 60(3) of the DSGA, which states that the Minister for Public Expenditure, NDP Delivery and Reform (the Minister) will publish a list of data sharing agreements, accession agreements or withdrawals received under the DSGA.

[46]Office of the Government Chief Information Officer, Data Governance - ogcio.gov.ie.

Australia

The Data Availability and Transparency Act 2022 (DATA Act) is a landmark legislation that authorises and regulates access to data held by the Australian Government.[47] DATA Act overrides Commonwealth, State, or Territory laws that would otherwise prohibit data sharing, collection, and use, provided appropriate safeguards are in place.[48]

The DATA Act is founded upon the Five Safes Framework, which includes Safe Projects, Safe People, Safe Data, Safe Settings, and Safe Outputs. These principles ensure that data sharing is conducted in a manner that balances public benefit with privacy and security[49]. For example, Safe Projects requires that data-sharing projects be evaluated for public benefit, while Safe People ensures that data recipients are trained and equipped to handle data securely. Safe Data emphasises the importance of de-identification, and Safe Settings require that data be stored and accessed in secure environments[50]. Finally, Safe Outputs ensure that the results of data analysis are reviewed to prevent the disclosure of sensitive information.[51]

Section 16A provides that the DATA Act does not override the Privacy Act 1988, ensuring that data sharing complies with privacy protections. The DATA Act establishes the DATA Scheme, a framework for sharing public sector data, supported by strong safeguards and efficient processes (Chapter 2). It empowers data custodians to share data,[52] accredited users to collect and use data,[53] and accredited data service providers (ADSPs) to act as intermediaries.[54]

The DATA Act initially allowed data sharing with private sector organisations, but this provision was removed to allow the DATA Scheme to mature, with a review scheduled within three years.[55] This decision reflects the government's cautious approach to balancing the

[47]Section 3 of Data Availability and Transparency Act 2022 (Data Act).
[48]Section 23 DATA Act.
[49]Section 18(2)(b).
[50]Section 33.
[51]Section 19.
[52]Section 13.
[53]Section 13A.
[54]Section 13B.
[55]Section 142.

benefits of data sharing with the risks of misuse or breaches, particularly in the private sector. The data sharing scheme involves three types of participants: data providers (Commonwealth Government bodies that regulate public sector data), accredited users (Commonwealth, state, and territory government bodies, as well as Australian universities), and accredited data service providers (entities that provide data integration, de-identification, and secure access services).[56] Foreign entities and certain Australian Government bodies are excluded from participating in the scheme.[57] This exclusion ensures that sensitive data remains within Australia's jurisdiction, reducing the risk of unauthorised access or misuse by foreign entities.

The Act's objectives include promoting the availability of public sector data, enhancing transparency and integrity in data sharing, and building public confidence in data use.[58] Data sharing under the scheme must be for permitted purposes,[59] comply with data sharing principles Section 16, and be governed by a data sharing agreement.[60] The permitted purposes include government service delivery (Section 15(1)(a)), informing government policies and programs (Section 15(1)(b)), and research and development (Section 15(1)(c)). However, any request for the sharing of data relating to law enforcement or national security purposes is explicitly prohibited, which reflects the government's commitment to protecting individual rights and privacy.[61]

As far as data governance is concerned, the DATA Act establishes the National Data Commissioner (NDC) as the regulator of the scheme[62]. The NDC is responsible for accrediting participants,[63] ensuring compliance with privacy and security safeguards,[64] and reporting on data sharing activities.[65] The DATA Act also establishes the National Data Advisory Council to advise the NDC on data sharing

[56](Section 11A (3)).
[57](Section 11(3).
[58](Section 3(a)), (Section 3(c)), (Section 3(d)).
[59]Section 15.
[60]Section 18.
[61]Section 15(2).
[62]Section 41.
[63]Section 74.
[64]Section 16A-16F.
[65]Section 138.

practices.[66] This dual structure ensures that data sharing is both regulated and informed by expert advice, fostering a balanced approach to governance.

Key safeguards under the DATA Act include accreditation (only accredited entities can participate),[67] permissions (consent requirements for data sharing) [68], privacy (compliance with the Privacy Act), and oversight (the NDC ensures accountability).[69] The DATA Act imposes significant penalties for unauthorised data sharing, collection, or use, including fines and imprisonment for serious breaches.[70] These penalties serve as a deterrent against misuse and reinforce the importance of responsible data handling.

The DATA Act also emphasises the importance of data management and governance. Organisations receiving data under the scheme must have appropriate policies (Section 77B), appoint a Chief Data Officer (Section 77B), ensure staff are trained in data handling (Section 16E), and implement secure access and de-identification processes through an Accredited Data Service Provider (ADSP) or qualified data custodian (Section 16C). These requirements align with international standards like the ISO/IEC 27001 framework, ensuring that Australia's data sharing practices meet global best practices.

Data sharing legislation has also been enacted at the state level in Australia. For example, in Victoria, the Victorian Data Sharing Act 2017 (VDS Act) promotes the sharing and use of public sector data to inform policymaking and service planning.[71] Section 7 of the VDS Act establishes a framework for data sharing and gives the Chief Data Officer (CDO) a central role in leading data integration and analysis. The CDO is responsible for building data analytics capabilities across the public sector and coordinating data sharing on behalf of Victoria.

On the other hand, South Australia's Public Sector (Data Sharing) Act 2016 (PSDSA) facilitates data sharing between public sector agencies and other entities to improve policymaking, program

[66]Section 61 DATA Act.
[67]Section 74.
[68]Section 16B.
[69]Section 42.
[70]Sections 14-14A.
[71]Section 5.

management, and service delivery.[72] The Act establishes the Office for Data Analytics (ODA), which is responsible for facilitating data sharing, performing data analytics work, and advising on data sharing practices.

Australia's data sharing frameworks at the federal, Victorian, and South Australian levels share common goals, such as promoting transparency, accountability, and innovation while safeguarding privacy and security.[73] However, there are notable differences in their approaches. For example, the DATA Act focuses on creating a national framework for data sharing,[74] while the VDS Act and PSDSA address state-level needs.[75] The DATA Act also places greater emphasis on accreditation and oversight.[76] At the same time, the VDS Act and PSDSA prioritise the role of the Chief Data Officer[77] and Office for Data Analytics,[78] respectively.

Another key difference is the scope of data sharing. The DATA Act allows data sharing between Commonwealth, state, and territory governments, as well as Australian universities, while the VDS Act and PSDSA focus on data sharing within their respective states. This reflects the different priorities and challenges faced by federal and state governments in managing public sector data. Despite these differences, all three frameworks emphasise the importance of data security, privacy, and ethical use. They also highlight the need for collaboration between government agencies, industry partners, and research organisations to maximise the benefits of data sharing. The next part discusses recent developments in the Malaysian data sharing legal framework, which was formalised after the enactment of the Data Sharing Act 2025 [Act 864] in 2025.

---

[72]Preamble to the South Australia's Public Sector (Data Sharing) Act 2016 (PSDSA).

[73]Section 4.

[74]See Section 3,4, 13, 13B.

[75]See Section 1(b) & (c), which promotes data sharing for Victorian government purposes.

[76]See Sections 74–87. See also Section 45, which grants the National Data Commissioner regulatory powers, and s.41, which establishes the National Data Commissioner as an oversight authority.

[77]For example, Part 2 (Sections 6–7) establishes the Victorian Chief Data Officer (CDO) and sets functions.

[78]See Part 3 (Section 6) that establishes the Office for Data Analytics (ODA).

ANALYSES AND RECOMMENDATIONS

The governance of data sharing has evolved from being a mere administrative exercise into a vital driver of innovation, economic expansion, and transparency across all sectors of society. When researchers, businesses, and public institutions can exchange high-quality data within clear and reliable legal parameters, collaboration becomes practice, and the resulting benefits are extensive. The EU's General Data Protection Regulation (GDPR) demonstrates how robust safeguards can coexist with technological progress: by embedding privacy-by-design principles while permitting legitimate cross-border data flows, the GDPR has enabled Europe to become a global leader in fields such as precision medicine, biodiversity monitoring, and artificial intelligence research. This illustrates that stringent safeguards and rapid scientific discoveries are not conflicting objectives but mutually reinforcing ones.

Yet, the risks associated with poor governance are equally significant. The Cambridge Analytica scandal highlighted how ambiguous or careless handling of personal data can erode public trust and compromise democratic institutions.[79] This example portrays a critical reality: while data holds immense potential to generate societal value, the absence of enforceable accountability mechanisms

[79]The Cambridge Analytica scandal, which came to light in 2018, involved the unauthorized harvesting of personal data from over 87 million Facebook users through a personality quiz app developed by academic Aleksandr Kogan. The data was then used by the UK-based political consulting firm Cambridge Analytica to create psychological profiles and micro-target voters with political advertisements during major campaigns such as the 2016 U.S. Presidential Election and the Brexit referendum. The incident exposed serious flaws in Facebook's data governance practices, sparked global outrage over digital privacy violations, and led to regulatory actions including a $5 billion fine imposed on Facebook by the U.S. Federal Trade Commission (FTC). It also prompted broader discussions on ethical data use and the role of social media in democratic processes. See Joanne Hinds, Emma J Williams, and Adam N Joinson, "'It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal", *International Journal of Human-Computer Studies*, vol. 143 (2020): 102498; Margaret Hu, "Cambridge Analytica's black box", *Big Data & Society*, vol. 7, no. 2 (2020): 2053951720938091.

diminishes this value through reputational damage, legal disputes, and public backlash. Effective governance must therefore also serve a distributive purpose. In today's hyper-connected world, equitable access to reliable data empowers marginalised communities, enhances evidence-based policymaking, and helps to reduce structural inequality. For instance, Open Government Data initiatives have already spurred civic-tech innovation, expanded journalistic scrutiny, and supported targeted social programs by making non-sensitive datasets freely available. It is therefore indefensible to retain public data under excessive bureaucratic caution when transparency can so clearly drive socio-economic development.

The rapid spread of artificial intelligence, machine learning, and automation further intensifies the ethical stakes of data sharing. These technologies bring to light new risks, such as algorithmic bias, invasive surveillance, and the erosion of digital rights. The debate over facial recognition technology and its discriminatory effects exemplifies why ethical guidelines and enforceable safeguards must accompany any expansion in data-sharing practices.[80] In essence, technological progress must remain anchored in legal and ethical principles so that innovation does not come at the expense of justice or human dignity.[81]

Centralising responsibility within a lead agency is an operational necessity. Such agencies coordinate collaboration, ensure compliance, and incorporate privacy and security measures by default. The EU, Australia, and the United Kingdom offer three instructive—though context-specific—models of national data-sharing stewardship.

Under the EU's 2022 Data Governance Act, the European Data Innovation Board (EDIB) convenes regulators, cybersecurity authorities, standard-setting bodies, and civil society stakeholders to harmonise cross-sector data mediation, altruism schemes, and the release of non-open public data. By institutionalising multi-stakeholder dialogue, the EDIB demonstrates how strategic oversight can coexist with technical agility.

Australia's Data Availability and Transparency Act 2022 establishes a robust regulatory framework through the National Data

[80]Emilio Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies", *Sci*, vol. 6, no. 1 (2024).
[81]Emilio Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources.

Commissioner (NDC), supported operationally by the Office of the National Data Commissioner (ONDC). Together, they accredit data users, prosecute non-compliance, and develop best practices through guidance and education. The DATA Scheme's Five Safes framework is a layered set of controls that link project purpose, authorised personnel, secure environments, appropriately treated data, and vetted outputs. Crucially, the National Data Advisory Council injects ethical scrutiny as technical governance alone is insufficient without an explicit moral compass.

Benchmarking against these international examples reveals a menu of design choices, rather than a one-size-fits-all template. The EU's commitment to transnational data sharing, for example, is predicated on its supranational legal architecture—a reality that does not map neatly onto Malaysia's federal framework.

Nonetheless, three transferable insights stand out:

1. *Out-of-Territory Flexibility* – Europe's concept of lawful cross-border usage validates the importance of accommodating regional data flows that extend beyond national frontiers.
2. *Multi-Stakeholder Oversight* – An advisory entity with representation from high-impact ministries, technical experts, industry, and civil society ensures legitimacy and responsiveness.
3. *Interoperability by Design* – The EDIB's drive toward common standards demonstrates that technical coherence is as pivotal as legal clarity.

Malaysia should therefore consider a National Data Sharing Committee (NDSC) modelled on, but not identical to, the EU's board. Core ministries that steward large volumes of citizen data must secure permanent seats, while other ministries should participate ad hoc as policy issues dictate. National Data Sharing Committee members should also include representatives from the industry, given that data governance is typically managed by the private sector in most cases. This flexible architecture prevents capture while safeguarding expertise.

Currently, the membership of the National Data Sharing Committee primarily comprises representatives from the government sector. This indicates that the data sharing framework remains limited to public sector data. Moving forward, considering the evolution of

data sharing practices, data flows across the globe should not be confined to segregated domains of government and private sector management. In practice, the government depends significantly on the private sector to sustain the digital data ecosystem. Therefore, the governance of data sharing must incorporate and adapt to these dynamic interactions.

Conversely, the UK's Digital Economy Act 2017, overseen by the Information Commissioner's Office (ICO), demonstrates how statutory powers, parliamentary reporting, and strict privacy obligations can work together to enable public-sector data for research, service delivery, and operational improvements. The key point here is that easy access to non-sensitive datasets fosters innovation without risking personal privacy—so long as robust institutional firewalls are maintained.

In comparison to Malaysia's Data Sharing Act 2025, which mandates the National Data Sharing Committee to report to the Cabinet, the frequency of such reporting remains uncertain due to the absence of a legal obligation to submit reports to Parliament. Furthermore, the Minister overseeing the Data Sharing Act 2025 does not serve on the Committee, potentially raising concerns regarding the extent of reporting. The lack of involvement of external members from international counterparts or industry may also cast doubts on the transparency and openness of data governance practices. Additionally, selective reporting is foreseeable; in the event of a data breach, responsibility falls to a different agency, namely the Department of Personal Data Protection, which is responsible for initiating further actions under the Personal Data Protection Act 2010. Notably, the Malaysia Data Sharing Act 2025 does not impose any reporting obligations for data breaches. Given that this Act constitutes the sole binding legal framework on the Federal Government concerning public sector data governance, future deliberations should consider establishing mandatory reporting or data breach notification requirements for public sector data sharing.

On the other hand, Ireland's Data Sharing and Governance Act 2019 demonstrates yet another effective model. Led by a Chief Government Information Officer (CIO) and a dedicated Data Governance Unit, Ireland aligns its digital-service goals with strict GDPR compliance. Ministers have the authority to mandate data sharing, while an independent Data Governance Board enforces

standards, reviews agreements, and audits compliance—showing that executive leadership and independent oversight can work together rather than oppose each other.

Furthermore, the Australian framework for public sector data sharing is fascinating to observe. Beyond the federal level, Australia's sub-national statutes—Victoria's Data Sharing Act 2017 and South Australia's Public Sector Data Sharing Act 2016—extend the Five Safes principles through Chief Data Officers and Offices of Data Analytics. They mandate de-identification, rapid response timelines, and capacity-building functions, reinforcing the principle that privacy protection and data utility must advance in tandem.

In light of the overall analyses in this paper, the following institutional data governance for Malaysia is proposed as follows: -

1. Provide regulatory powers and functions to the National Digital Department under the Data Sharing Act 2025. The current practice is that only the Director General of the National Digital Department shoulders key responsibilities under the Data Sharing Act 2025. The absence of the role of a specific regulatory agency on data governance will mean that data governance will stay decentralised and repeat the problems stated in the earlier part of this paper. Establishing a specific data commission may also be considered as an option, given the growing need for data governance and regulation.
2. Extend the application of the Data Sharing Act 2025 to cover all states in Malaysia, since most data relating to the people is available at the state and local government levels. This should also include statutory bodies at the state level. Once the operationalisation of the data governance is stable, one should consider extending the application of the Data Sharing Act 2025 to cover private entities, such as companies having offices within or outside Malaysia, reflecting upon the practice in the EU.
3. Designate Chief Data Officers in every central ministry and agency to operationalise the directives issued by the National Data Sharing Committee, oversee compliance, and champion data-literacy initiatives. In light of current administrative practice, Chief Digital Officers were appointed from amongst the Deputy Chief Secretaries (*Timbalan Ketua Setiausaha*), who do not focus on data governance per se. Such broad responsibilities

may mean that data governance will not be taken seriously and attentively unless a specific role is dedicated to this subject.

4. Embed the Five Safes principles and require every data-sharing arrangement to be formalised through a publicly accessible registry as per the Australian experience.

By internalising these recommendations, Malaysia positions itself to harvest the full economic and social value of data while fortifying public trust. A purpose-built data governance framework—rooted in international best practice yet sensitised to domestic realities will supply the strategic leverage required to drive innovation, elevate public-service delivery, and confront complex societal challenges head-on.

CONCLUSION

The implementation of Malaysia's Data Sharing Act 2025 represents a significant advancement, aligning national practices with global standards. By incorporating robust oversight, compliance mechanisms, and coordinated national governance, the Act is designed to facilitate data sharing securely and responsibly. Drawing lessons from international frameworks, Malaysia's approach can enhance transparency and effectiveness in public services while ensuring individual privacy is preserved.

Benchmarking against best practices, the UK's emphasis on lawful data usage, reinforced by rigorous oversight from the Information Commissioner's Office (ICO), demonstrates how strong institutional controls can balance enhanced data accessibility with privacy considerations. Similarly, Ireland's approach of integrating GDPR compliance into its digital service delivery highlights the necessity of embedding public transparency and explicit data rights into any national data-sharing framework.

Australia's model offers further guidance through its Five Safes Framework, emphasising principles-based data management and staged approaches to broader data usage. Such structured frameworks, complemented by independent oversight and strict regulatory controls, including written agreements and penalties for misuse, provide essential protections against potential privacy infringements and data

misuse. Malaysia could substantially benefit by integrating these structured mechanisms into its existing governance practices.

Ultimately, Malaysia's challenge lies in striking a balance between the need for broader data accessibility for public benefit and the imperative to safeguard individual privacy rights. By adopting privacy-by-design principles, clear consent rules, and independent oversight structures such as a National Data Sharing Committee, Malaysia can cultivate public trust in its data governance strategies. Adhering to these comprehensive and adaptive practices ensures both the protection of personal data and the facilitation of responsible and beneficial data use.

REFERENCES

Agdatahub. "Company – Agdatahub." *Agdatahub*. https://agdatahub.eu/entreprise/ (accessed 18 October 2025).

Ahmad Shaharudin, Ahmad Ashraf. "Open Government Data in Malaysia: Landscape, Challenges and Aspirations." *Khazanah Research Institute* 3/21 (2021): 1–45.

Australian Research Data Commons. *Data Sharing Policy Development Guidelines*. https://zenodo.org/records/7553182/files/Data%20Sharing%20Policy%20Development%20Guidelines.pdf.

Bernama. "Data Commission Key to Strengthening Governance and Protection, Says Gobind." *Bernama*. https://theedgemalaysia.com/node/767318 (accessed 17 September 2025).

Capgemini. *Connecting the Dots: Data Sharing in the Public Sector*. Capgemini Research Institute, 2023. https://www.capgemini.com/insights/research-library/data-ecosystems-in-public-sector/

Council for International Organizations of Medical Sciences (CIOMS). *International Ethical Guidelines for Health-related Research Involving Humans*.

Dawex. "Data Exchange Technology Compliance | Dawex." *Dawex*. https://www.dawex.com/en/data-exchange-technology/compliance/ (accessed 18 October 2025).

Department of Digital Malaysia. "MyGDX | Malaysian Government Central Data Exchange." *Department of Digital Malaysia*. https://www.mygdx.gov.my/ms/landing-page/theme (accessed 2 March 2025).

European Data Portal. *Creating Value Through Open Data*. https://data.europa.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf.

Ferrara, Emilio. "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies." *Sci* 6, no. 1 (2024).

Fraunhofer Institute for Experimental Software Engineering IESE. "Deutsche Telekom AG Success Story – Secure Data." *Fraunhofer Institute for Experimental Software Engineering IESE*. https://www.iese.fraunhofer.de/en/reference/deutsche-telekom-secure-data-marketplace (accessed 18 October 2025).

Ganapati, Sukumar, and Christopher G. Reddick. "Prospects and Challenges of Sharing Economy for the Public Sector." *Government Information Quarterly* 35, no. 1 (2018): 77–87.

Government Central Data Exchange. "MyGDX | Malaysian Government Central Data Exchange." *Government Central Data Exchange*. https://www.mygdx.gov.my/ms/landing-page/architecture?theme=second-theme (accessed 17 October 2025).

Government of Malaysia. "What Is MySejahtera?": MySejahtera." https://helpdesk.mysejahtera.malaysia.gov.my/en/support/solutions/articles/51000293086-what-is-mysejahtera- (accessed 28 February 2025).

Government of Malaysia. "Malaysia's Official Open Data Portal." https://data.gov.my/ (accessed 2 March 2025).

Hinds, Joanne, Emma J. Williams, and Adam N. Joinson. "'It Wouldn't Happen to Me': Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal." *International Journal of Human-Computer Studies* 143 (2020): 102498.

Hu, Margaret. "Cambridge Analytica's Black Box." *Big Data & Society* 7, no. 2 (2020): 2053951720938091.

IBM Corporation. *Cost of a Data Breach Report 2024*. IBM Security. https://www.ibm.com/security/data-breach.

International Organization for Standardization (ISO). "Smart Farming: Data-Driven Agriculture." https://www.iso.org/smart-farming/smart-farming-data-driven.

Jussen, Ilka, Frederik Möller, Julia Schweihoff, Anna Gieß, Giulia Giussani, and Boris Otto. "Issues in Inter-organizational Data Sharing: Findings from Practice and Research Challenges." *Data & Knowledge Engineering* 150 (2024): 102280.

Máchová, Renáta, Miloslav Hub, and Martin Lnenicka. "Usability Evaluation of Open Data Portals." *Aslib Journal of Information Management* 70, no. 3 (2018): 252–268.

Microsoft Stories Asia. "Data Sharing Key to Solving Asia's Biggest Economic and Societal Challenges: Microsoft Asia Whitepaper." *Microsoft Stories Asia*. https://news.microsoft.com/apac/2021/09/28/data-sharing-key-to-solving-asias-biggest-economic-and-societal-challenges-microsoft-asia-whitepaper/ (accessed 28 February 2025).

Ministry of Health (MOH). *Focus Group Discussion on Data Sharing and the Medical Act 1971 [Act 50]*. National Digital Department, 17 November 2023.

Ministry of Youth and Sports (KBS). *Focus Group Discussion on Data Sharing and the Sports Development Act 1997 [Act 576]*. National Digital Department, 30–31 October 2023.

National Geospatial Centre. "About MyGDI | MyGeoportal." *National Geospatial Centre*. https://www.mygeoportal.gov.my/en/about-mygdi?utm_source=chatgpt.com (accessed 28 February 2025).

Organisation for Economic Co-operation and Development (OECD). *Enhancing Access to and Sharing of Data*. Paris: OECD Publishing, 2019. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/enhancing-access-to-and-sharing-of-data_070835df/276aaca8-en.pdf.

Organisation for Economic Co-operation and Development (OECD). *G20 Compendium on Data Access and Sharing Across the Public Sector and with the Private Sector for Public Interest*. Paris: OECD Publishing, 2023. https://www.oecd-ilibrary.org/governance/g20-compendium-on-data-access-and-sharing-across-the-public-sector-and-with-the-private-sector-for-public-interest_df1031a4-en.

Organisation for Economic Co-operation and Development (OECD). "OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem." https://www.oecd-ilibrary.org/education/oecd-digital-education-outlook-2023_c74f03de-en.

Pangkalan Data Utama (PADU). "Pangkalan Data Utama (PADU)." https://www.padu.gov.my/soalan-lazim (accessed 2 March 2025).

Parliament of Malaysia. *Dewan Rakyat Parlimen Kelima Belas Penggal Ketiga Mesyuarat Pertama, Rabu 27 Mac 2024*. Parliament of Malaysia.

Reuters. "From Field to the Cloud: How AI Is Helping Regenerative Agriculture to Grow." *Reuters*. https://www.reuters.com/sustainability/land-use-biodiversity/field-cloud-how-ai-is-helping-regenerative-agriculture-grow-2024-09-18.

Ruohonen, Jukka, and Sini Mickelsson. "Reflections on the Data Governance Act." *Digital Society* 2, no. 1 (2023): 1–9.

Strom, Kevin. *Research on the Impact of Technology on Policing Strategy in the 21st Century: Final Report*. Washington, DC: National Criminal Justice Reference Service, 2017.

United Nations Office for Disaster Risk Reduction. *Global Assessment Report on Disaster Risk Reduction 2019*. https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2019 (accessed 2 March 2025).

World Economic Forum. "Global Cybersecurity Outlook 2024." *World Economic Forum*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.

World Economic Forum. "How Can SMEs Become Data-Driven Enterprises?" *World Economic Forum*. https://www.weforum.org/stories/2023/06/how-can-smes-become-data-driven-enterprises/.

Wired. "Environmental Sensing Is Here, Tracking Everything from Forest Fires to Threatened Species." *Wired.com*. https://www.wired.com/story/environmental-sensing-is-here-tracking-everything-from-forest-fires-to-threatened-species.

Xiong, Wei, Bin Chen, Huanming Wang, and Dajian Zhu. "Public–Private Partnerships as a Governance Response to Sustainable Urbanization: Lessons from China." *Habitat International* 95 (2020): 102095.