POLICY RECOMMENDATION PAPER

Embracing technology, preserving data sovereignty

Farlina Said
Senior Analyst,
Institute of Strategic &
International Studies (ISIS)
Malaysia

Introduction

This paper is the result of the Huawei Technologies (Malaysia) Sdn Bhd (Huawei Malaysia), MyDIGITAL Corporation and the Institute of Strategic & International Studies (ISIS) Malaysia organised webinar, Digital age: embracing technology, preserving data sovereignty on 12 May 2022. The objective of the webinar was to raise awareness among the government, its agencies and the public about preserving data sovereignty while using digital technology, such as cloud, in the age of digital transformation.

Government cloud services are a new development at the intersection of electronic government and cloud computing, which promises more effective and efficient government services. While cloud transformation and enhanced connectivity are some of the most significant focus areas to accelerate the nation's digital economy building blocks, they have also triggered governments' concern for data sovereignty and security. The webinar addressed some of these issues, including cybersecurity as a critical component in building the digital ecosystem for Malaysia.

Participants included representatives from the Ministry of Communications and Multimedia Malaysia (K-KOMM), Malaysian Communications and Multimedia Commission (MCMC), MyDIGITAL Corporation, Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), National Cyber Security Agency (NACSA) and state governments. The webinar was held virtually and physically at the ISIS Malaysia headquarters.

In the keynote address, secretary-general of K-KOMM, Datuk Seri Mohammad Mentek highlighted that Malaysia is taking great efforts to protect its digital sovereignty, including introducing various policies and frameworks to enact controls and ensure organisations tighten their data security.

"As of 2021, about 100 countries have some form of existing data sovereignty laws. In Malaysia, the notion of data sovereignty is reflected in some of the existing legal and policy frameworks,"

Mohammad said, adding that "these policies encompass a comprehensive cross-sectoral framework to protect personal data in commercial transactions and play an important role in helping companies address data sovereignty issues, while at the same time ensuring information security, network reliability and integrity, and secure and resilient infrastructure".

MyDIGITAL Corporation CEO Fabian Bigar, in his welcome address, emphasised that threats can quickly outpace traditional approaches to data security, hence governments and organisations need to be proactive in creating and adapting systems to face these threats as the economy moves forward.

"One of the thrusts in the Malaysian Digital Economy Blueprint (MDEB) is to build a trusted, secure, and ethical digital environment. Today, there is a much greater urgency for our regulatory environment to be anchored on trust and digital-native policies which reflect the world we live in,"
he said.

Delivering the closing remarks, NACSA chief executive Rahamzan Hashim said retaining control over our data and leading with a security-first mindset must always be a priority. He emphasised the need for everyone to work together to protect cyberspace and to ensure that all data flows are protected and secure.

"Seamless cooperation between industries and public sectors must be strengthened and treasured in order to address challenges and opportunities present in this new journey towards embracing the new data-driven technology and digital transformation"
he said.

The panellists included Shamsul Izhan Abdul Majid (MCMC chief technology and innovation officer), Konesh Kochhal (director, industry ecosystem engagements, Huawei APAC), Raja Azrina Raja Othman (chief information security officer, group information security, TM), Nur Hidayah Abdullah (ICT consultant – information security, MAMPU) and Dr Moonyati Yatid (senior manager, corporate strategy & research, Malaysia Petroleum Resources Corporation).

1. Background

Data is a vital component of the future economy, especially as the fuel for key technologies, such as artificial intelligence or cloud computing, which are the bases for developments in the Fourth Industrial Revolution. Data stimulates the economy and industries where the collection, analysis and transfer of data can lead to greater adoption of tools and technology that could solve community and societal issues. MyDIGITAL highlights the potential of data, where between 2021 and 2025, the data-focused approaches look into public sector modernisation, personal data protection legislation and cross-border data flows. This initiative will complement the national development policies, such as the Twelfth Malaysia Plan (12MP) and the Shared Prosperity Vision 2030 (WKB 2030).

Globally, digital lifestyles can create up to 2.5 quintillion bytes of data daily.[1] Data created include information, such as identities, user behaviours, interactions and experiences. Digital transformation will accelerate data creation where technologies will automate data creation, information processing and produce metadata which will contain identifiable information. This means the security of information created, collected, processed and transferred would require the due diligence of the data controller or processor to ensure that the minimum standards in data management are met.[2]

In an interconnected and hyperactive data-generating environment, the protection of data would have to consider the entire data lifecycle. From the moment of creation to its destruction, controls must be in place to determine protection and access. For instance, there can be technological solutions to automate the classification of data, which would enable protection for documents or information even in transit. Additionally, coding specifications can be introduced at the point of data production, which would limit its ability to be distributed. As data travels from point A to point B, the entire ecosystem would need to uphold standards, rules and regulations.

2. Sovereignty and the obligation of states

The principle of sovereignty in international law includes the right of authority within a territory,[3] the equality of standing between states[4] and the justification for response should sovereignty be violated. *Tallinn Manual 2.0* discusses the rules of sovereignty,[5] including internal sovereignty and external sovereignty. Internal sovereignty touches on jurisdiction and responsibilities of the state within the jurisdiction while external sovereignty is derived from the United Nations Charter for states to comply with their international obligations.

Among such obligations are the 11 norms of responsible state behaviour adopted in UN Resolution A/RES/70/237.[6] These articulate the responsibility of the state to carry out due diligence measures to increase stability of cyber space. These are inclusive of prevention measures against malicious attacks throughout the supply chain, conducting assessments and reasonable steps to ensure that the territory is not being used for internationally wrongful acts and to consider all relevant information in the event of cyberattacks. Operationalising the norms of responsible state behaviour means that governments would need to build investigative capacities, legal measures and infrastructure resilience to fulfil the obligations articulated across the norms.

3. Data sovereignty

Exploring the sovereignty of data can present interesting questions. For one, data holds information related to populations in specific territories. Such data can be transferred, reside in other territories or produce metadata related to the population whose ownership may be unclear. The application of sovereignty principles to data may also require explorations of a state's capabilities and priorities to fulfil international obligations in data management. Thus, among a state's obligations as stated in the 11 norms is to protect data and uphold practices of privacy with respect to human rights.

As defined by Mohammad at the Huawei, MyDIGITAL and ISIS Malaysia webinar, Embracing technology, preserving data sovereignty, data sovereignty is to protect data from vulnerabilities and unwanted access. Elaborating on the concept, Bigar stated that data sovereignty is the idea that data is subjected to the rules and laws and governance of the nation the data is collected. The guidelines for the management of information security through cloud computing in the public sector released in 2021 by the Chief Government Security Office (CGSO) caution on the placement or processing of data outside of the control and jurisdiction of the Malaysian government. Such concerns are inclusive of the location where the supplier is registered and headquartered (if outside of Malaysia) or if a cloud-service provider (CSP) uses third-party vendors to deliver services. The emphasis of the guidelines is on the laws and regulations data would be subjected to, where the preference is for public sector data to be processed in Malaysia territory, especially if the data is classified as restricted, confidential, secret and top secret under the Official Secrets Act 1972.

To protect data, the state would introduce laws governing the ecosystem and the data's treatment. Generally, the ecosystem surrounding cyber security is regulated by the Communications and Multimedia Act 1998 (CMA 1998) and National Cyber Security Policy (NCSP) 2006. CMA 1998 regulates the communications and multimedia industries, setting out the offences and penalties for the misuse of network facilities in addition to outlining roles and responsibilities for compliance.

Cyber security processes are also elaborated in NCSP, especially for the operators of critical national information infrastructure (CNII) where the policy streamlines standards, certifications and channels of communication for critical sectors in Malaysia. Further, the Personal Data Protection Act (PDPA) 2010 regulates the processing of personal data by requiring data users to comply with obligations and rights accorded to data subjects.[7]

However, existing instruments such as CMA does not identify specific provisions for data sovereignty and protection. Newer technologies may challenge areas not covered by the existing laws.

For instance, the physical and digital architecture of cloud crosses different geographic locations. In Malaysia, cloud services is regulated with the light touch approach by MCMC, where cloud service providers can be registered as a class licensee. This places MCMC in a position to ensure the protection of consumer data. However, this licensee approach is effective if the provider is locally incorporated and may differ for foreign companies providing services in Malaysia. Further compliance to data protection for industries is under the PDPA.[8]

The European Union's general data protection regulation (GDPR), for instance, specifies that data collected from its citizens are subjected to the GDPR, regardless of where it is stored.[9]

The laws and guidelines governing those data are a core component of data sovereignty, especially if digital adoption means utilising services without great emphasis on geographic location.

4. Keeping data within borders

Enforcing extra-jurisdictional laws and setting standards may require resources, international collaboration and a sizeable market to ensure compliance by players. The mechanism would require multiple negotiations.

An alternative to stringent enforcement is strict data localisation requirements. Such requirements may introduce obligations for the entire data lifecycle, from storing, transmission and processing, to occur domestically. Thus, data must remain in the locality where it is created. Data within territorial borders would allow greater security controls over physical and digital architecture. Such control would also ensure that investigations for breaches could be conducted within national capacities without having to resort to mutual legal assistance treaties and letters rogatory.

Vietnam and China introduced data localisation requirements for online firms with the purpose of data or content control that could impact on security concerns. Cory and Dascoli articulate three kinds of data localisation and five rationales for its implementation.[10]

The different kinds of no data localisation are (i) the restriction in the transfer of data outside of borders, such as personal data, health and genomic data or geospatial data; (ii) the classification of data in accordance to sensitivity and national security; and (iii) making data transfers complicated, costly and uncertain.[11] The first is articulated by Malaysia's PDPA while the second is the approach of the public sector in managing data. The third form of data localisation or data protectionism is being discussed in France, South Korea and India, pertaining to licensing requirements and practices that could exclude or burden foreign firms. The rationales offered for data localisation are (i) to protect data stored within a country's borders; (ii) data protectionism – to wrest back control of data from foreign firms; (iii) for censorship and surveillance; (iv) for law enforcement and regulatory oversight; and (v) concerns over international financial sanctions.

While mandatory data localisation may hold advantages for law enforcement and regulatory oversight, keeping data within the country is not a guarantee of no data breaches, privacy or economic stimulation. Data localisation would need to be complemented by enforcement of cybersecurity standards, awareness and secure data practices to ensure safeguards against data breaches. Data in Malaysia can be as equally at risk in other jurisdictions if cyber hygiene and data management practices within the territory do not meet the necessary standards.

Additionally, lessons learned from the conflict in Europe indicate that concentrating data centres in centralised and specific locations may impact on a government's ability to deliver services in times of conflict. Estonia experienced such an attack in 2007, which forced the digital nation offline for nearly a month.[12] Estonia, following the attack that had taken 58 Estonian websites offline, including government, newspapers and banks, introduced "data embassies" where a bilateral agreement is signed for the establishment of data centres outside of the territory with the same rights and immunity of a physical embassy.[13] The embassies would reside in "friendly countries" where the Estonian government could use as external databases in times of crisis.[14] Further, the practice of storing data over several centres[15] could build resilience in an organisation or agency's data management. The location of such data centres may be in accordance with the risk appetite and compliance measures of the respective organisation and agency.

Another measure lighter than data localisation is data residency. Data residency focuses on controlling the location of data, most frequently "sensitive" data.[16] An interpretation of data residency laws would require companies to process data in a territory although copies of the data can be transferred abroad as long as a local copy is available to the local government for inspection.[17]

Other practices would include stringent standards for those collecting and processing data, knowing the geolocations of data flows and monitoring the cybersecurity practices along the entire supply chain. The difference between data localisation and data residency is that data localisation would require all data to be territory bound while data residency could tolerate transfers of data to other locations with the most sensitive kept within a nation's jurisdiction. Data residency policies could utilise international relations or extra-jurisdictional legislation to strengthen government control over data. However, the approach may not be effective for the private sector which hopes to grow business in different markets.

As data sovereignty is a concept in flux, the following table aims to articulate possible elaborations and distinctions between data sovereignty, data localisation and data residency.

Concept	Elaboration	Benefit	Risk	Considerations
Data sovereignty	Extension of sovereign rights of a state towards data with the expectation of fulfilling domestic and international purposes.	Galvanises existing practices and introduces baselines for data management.	Without transparency mechanisms, data sovereignty can be misconstrued with protectionist measures for the misuse of law.	Mitigation measures for increasing distrust in cyber space would include greater communication, stakeholder engagements and transparency.
Data localisation	Data must stay within the locality where it is created. This would be inclusive of processing and management.	Sovereign control over data and information. Would ease forensics and cybercrime investigative capabilities.	Need to be complemented by strong domestic cybersecurity practices. Would impact on competition and foreign investors' access to market.	Countries may adopt different levels of data localisation requirements. Some may require storage, transmission and processing within territory.
Data residency	A geo-location focused approach, where practices focus on controlling the location of data matched with its appropriate classification. The approach may not mandate data localisation requirements.	Control over regulatory concerns, which would include implementing national laws, introducing tax implications and governing privacy values treated onto data without absolute restriction and control of flows.	As a geo-location and data classification-centric approach distributes responsibilities across various stakeholders, the data residency approach needs heavy monitoring, especially for cybersecurity considerations.	Requires legislative and policy approaches to ensure compliance. Should be supported by international cooperation strategies that could harmonise approaches to cybercrime and national security concerns.

Source: Emily Wu, Belfer Centre,[18] Google[19] and InCountry.[20]

Data sovereignty is a developing concept, with various interpretations of its meaning resulting in practices, such as data localisation and data residency approaches.

Data localisation could stifle open data flows, which can impact on innovation that can further digital economy development and increase distrust in cyber space. However, responsibilities and laws for data sovereignty is clearer for on-premise infrastructure, especially because IT workloads and the business itself operate out of the same location, with a common set of laws applying to both. In the cloud infrastructure environment, where a business can store its data in any number of different geographic regions regardless of where the business itself is based, data sovereignty can be more complicated.

Comparatively, data residency could classify data to a hybrid approach that could suit the risk appetite of the departments. There are amalgamations of data localisation and residency approaches where copies of the data could be kept in local servers or centres abroad. Other restrictions can also be in the form of controls where data can only be transferred with approved destinations of specific authorities or with legal mechanisms facilitating the relationship. With sufficient legislation, it is possible for data stored in other parts of the world to be subjected to a nation's laws with examples inclusive of the US' Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and EU's GDPR. Both data localisation or data residency approaches require Malaysia's cyber environment to practise high standards of data management and security.

There is a need to define the data sovereignty requirements and comprehensive guidelines to support all deployment scenarios. High standards of cybersecurity would also build greater trust in Malaysia's digital economy ecosystem. Thus, developing ways forward should be complemented by sufficient legislation, compliance and enforcement mechanisms.

5. Current scenario

MyDIGITAL is targeting 80% usage of cloud storage across the government and incorporating cloud computing for businesses to procure services as well as offering a majority of end-to-end government services online by 2025 without having to own and maintain assets. The public sector is under great pressure to increase the pace of digitalisation. Cloud computing would utilise physical and digital architecture, where the data could be processed, transferred or stored outside of Malaysia's jurisdiction. This opens conversations on data hosting strategies.

In 2021, more than 100 countries introduced legislation to control the mechanisms for data security. India introduced mechanisms to address improper disclosure of personal information, compliance requirements for all forms of personal data and mandates data localisation requirements for certain forms of sensitive data. China's data governance laws also extend to the transfer of data outside the country, where firms would have to adhere to strict rules, including getting permission from China's government prior to transfers. Vietnam's cybersecurity laws and decrees require foreign providers of online services to store their data in Vietnam, in addition to setting up offices of local representation. Regulations can also be limited to public sectors, such as those discussed in Indonesia. These approaches are determined by national economic policies and the risk appetite of the nations. Among the concerns of data crossing borders are the different legislations applicable to the data. Such legislations could allow access to the data processed or treat data with different thresholds of rights.

In Malaysia, data sovereignty refers to the government's absolute rights over the data, which is inclusive of control in the management of such data.[21] The guidelines for the management of information security through cloud computing in the public sector by the CGSO favours data storage within Malaysian territory as data stored, processed or transferred abroad may be outside of the government's jurisdiction and control.[22] The concern of jurisdiction and control is also applicable to vendors registered outside of Malaysia, where risk is perceived as higher if vendors are registered outside Malaysian jurisdiction. Despite sharing concerns and risks, the guidelines do allow respective agencies to determine the appropriate residential status of the data in accordance to data classifications.

There are five data classifications in the guidelines which classify data against national security concerns. These are open, restricted, confidential, secret and top secret. Confidential data is information that could jeopardise the duties of government agencies or impact on the image of the Malaysian government. Secret data can endanger national security while top secret is information if leaked could lead to catastrophic consequences. The personal information of the population managed by the government would fall among these categories of classifications. Of the five classifications, only data categorised as secret and top secret cannot be placed on cloud. Restricted and confidential data are able to be stored on cloud computing services, although they must be placed in cloud facilities within the legislation and jurisdiction of the Malaysian government.[23] The facility can be developed and built by local or foreign cloud service providers. The safety and confidentiality of data will be held by legal agreements plus oversight measures.

Thus, to strengthen data security practices, the guidelines recommend that government agencies consider (i) the management and stakeholders in the government departments; (ii) data security; (iii) geographic location and physical residency of the data; (iv) the rules, procedures and laws; (v) security risks; (vi) data classifications; (vii) ownership of the data; and (viii) data flows in the steps to embrace cloud computing. CGSO and the related agencies would audit the data management system to ensure responsibilities are upheld. Enforcement will be conducted by CGSO and the Royal Malaysia Police as these are the two entities empowered with enforcement capabilities and jurisdiction.

Further, the Official Secrets Act 1972 does mention the possibilities of safeguarding against leaks with Section 9(1)(f) mentioning possession without the authority of the public service as punishable with a fine not exceeding RM10,000 or imprisonment not exceeding seven years, or both. The same section also states that any person who allows any other person to have possession of any official document would be guilty of an offence punishable up to seven years of imprisonment.[24] However, the barriers to gather evidence and place responsibilities may be high. There are no known statements of data leaks linked to government systems investigated under the Act.

6. Benchmarking Malaysia to regional data sovereignty approaches

While data sovereignty can seem synonymous with data localisation, international practices display a range of tools for the purpose of exerting rights over data for greater security. Examples, such as EU's GDPR, include obligations to comply to detailed mechanisms for the management of data, such as signing a data processing agreement with vendors that act as data processors[25] and providing users with the option to wipe or delete any information in full to uphold the rights of data owners.[26] The GDPR is applicable to all providers of services which manage data of EU citizens. The American CLOUD Act is an agreement to increase the capacity for obtaining evidence to combat cybercrime. Partner countries are able to use their own domestic legal processes to acquire data from providers with the purpose of addressing serious crimes.[27] Participation in the CLOUD Act would require fulfilling requirements stipulated, inclusive of high privacy standards.

The development of data sovereignty should take into account cybersecurity and cyber hygiene practices within Malaysia, especially for data centres located within the territory. For consideration, Malaysia ranked fifth in ITU's 2020 Global Cybersecurity Index.[28] However, despite maturity in internet access and the legal environment, vulnerabilities in Malaysia's cyber environment still exist. Since late 2021, the availability of data sets supposedly sourced from government agencies have raised concerns over the security of data practices by the government. Data sets for sale and leakages due to undiscovered system vulnerabilities display the challenges of data management practices. For data sovereignty practices, the availability of the data sets should be a concern and measures need to be fortified to safeguard the supply chain.

At the national level, protecting data throughout the entirety of the lifecycle would require technological solutions, legal-compliance mechanisms, regular security assessments and audits, access controls as well as public-private partnerships. There are talks of an Omnibus Act that governs the digital ecosystem, an approach that would be necessary to prepare the government for a data-sharing framework between government bodies and agencies. Additionally, as data can be managed by the private sector in critical sectors, vendors or third-party players in the supply chain, the approach should ensure compliance to security standards. The Act could seek to govern processes and encourage leadership to secure data generated and shared in the public sector.

7. Recommendations

- As data sovereignty requires assessment of data classification for data residency, understanding the data generated and flows would be necessary to ensure security practices are appropriate for the data produced. Data can be treated differently across borders and may also differ as it is processed by various applications. Mapping the data generated, in addition to understanding the intrinsic value and classification of data would be useful to ensure the appropriate data meets adequate security protection. Classifying data can be aided by technology, which can improve efficiencies of technological adoption.

- The burden for the public sector differs from industry players. However, as the list of CNII expands with the National Cyber Security Strategy 2020-2024, organisations, institutions and companies participating in the data flow cycle would need to ensure responsibilities are shared to build resilient data systems. This would require greater coordination between the public and private sectors, with regular aggressive audits. Creating an ecosystem that could consistently discover, test and introduce solutions to vulnerabilities would be useful. Empowering one body to have oversight on data sovereignty would help streamline processes. Agencies, such as CGSO and MAMPU, are vital players for the public sector's data security practices. Further conversations with stakeholders, ministries and relevant agencies to empower one body could strengthen and improve oversight mechanisms.

- Despite the set of laws and robust guidelines, there are grey areas which could be clarified for improved and healthier data practices. Among them are to refine roles and responsibilities for data security, such as increasing cybersecurity practices for the network, enhancing privacy at the data points and building ethics in the system. Additionally, conversations and awareness programmes would also need to be held with stakeholders, such as the operators of critical sectors and the private sector.

- Conversations between industry, critical sectors, government officials, think-tanks, academics and civil society on gaps, issues and appetite for greater controls over data flows should be held. The MCMC Network Security Division and International Affairs can be consulted, with NACSA and CGSO with regards to cross border data approaches and regulation. Data sovereignty practices would have to be scaled from the synergy of Malaysia's policies and economic direction. Thus, data sovereignty would have to consider the priorities articulated in these documents, the economic sectors producing and managing the data, as well as the public and government bodies whose data is used to improve and introduce services.

8. Conclusion and the way forward

Data sovereignty is identified in Malaysia's policies though it is mainly for the public sector. However, data sovereignty practices are specific for the public sector when a definition of data sovereignty would include rights over the population's data even if managed by the private sector in other territories. Considerations to operationalise data sovereignty are also anchored on increasing data security practices within Malaysia. For the public sector, this would mean improving mechanisms for compliance.

The government is in the unique position of being a regulator, user, owner and collector. Hosting, storing and processing data of various security risks, the modernisation of the Malaysian government would have to weigh digital adoption against government functions and national security concerns. In an interconnected environment, data can travel across jurisdictions, thus subjecting the information to different standards, rules and regulations. This could impact on efforts to gather evidence for forensics, to ensure data is managed in accordance with guidelines, laws and values as well as narrow opportunities to develop and stimulate local digital economies that would rely on data to improve services. Unless a country or region chooses to enforce extra-territorial regulations like the EU's GDPR, the treatment towards data can differ in each territory.

Further, as data sovereignty practices may be necessary for national levels of cybersecurity, businesses may have to face a tradeoff between data sovereignty requirements and costs, while balancing performance goals. It will be hard to achieve the simplest cloud data sovereignty while optimising performance and costs. To operators in the critical sectors, different measures will require exerting relative levels of control and technological adoption while scrutinising data security practices and location.

Data sovereignty issues have not traditionally been a major focus when the private and public sectors plan cloud strategies, but it is likely to become more and more significant as the regulatory landscape grows more complex. Hence, the definition of data sovereignty for Malaysia needs to be considered via the local context and national priorities. Increasing data security using data sovereignty practices may require building safeguards along the entirety of the data cycle. Thus, for strategic ways forward, the scope of data sovereignty should include (i) establishing laws or standards for the way data should be treated; (ii) increasing mechanisms for international collaborations that reflect domestic data security practices; (iii) enforcing compliance measures through a structured ecosystem as well as enhancing data security practices; and (iv) ensuring cloud storage systems used ensure data sovereignty.

Endnotes

[1] DOMO. (2017). *Data never sleeps 5.0* [Infographic]. https://www.domo.com/learn/infographic/data-never-sleeps-5

[2] Chia, J. (2021, June). *Malaysia – data protection overview*. OneTrust Data Guidance. https://www.dataguidance.com/notes/malaysia-data-protection-overview

[3] Besson, S. (2011, April). *Sovereignty*. Oxford Public International Law. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472

[4] United Nations. (n.d.). *United Nations charter – Article 2(1)*. https://www.un.org/en/about-us/un-charter/full-text

[5] Schmitt, M. N., & Vihul, L. (Eds.). (2017). *Tallinn manual 2.0 on the international law appliable to cyber operations* (2nd ed.). New York: Cambridge University Press, p. 11.

[6] United Nations General Assembly. (2015, December 30). *Developments in the field of information and telecommunications in the context of international security* (Resolution A/RES/70/237). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement

[7] Chia, *Malaysia data protection overview*.

[8] Malaysian Communications and Multimedia Commission. (2021, December 17). *Information paper on regulating cloud services.* https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/Info-Paper-Regulating-Cloud-Service.pdf

[9] Official Journal of the European Union. (2016, April 27). *Regulations*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[10] Cory, N., & Dascoli, L. (2021, July 19). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. ITIF. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

[11] Ibid.

[12] Reynolds, M. (2016, October 17). *'Land is so yesterday': e-residents and 'digital embassies' could replace country borders*. WIRED. https://www.wired.co.uk/article/taavi-kotka-estonian-government

[13] E-estonia. (n.d.) *Data embassy*. https://e-estonia.com/wp-content/uploads/aug2019-facts-a4-data-embassy.pdf

[14] Reynolds, *'Land is so yesterday'*.

[15] Cory, & Dascoli. *How barriers to cross-border data flows are spreading globally*.

[16] InCountry. (2022, March 8). *What is data residency-as-a-service*. https://incountry.com/blog/what-is-data-residency-as-a-service/

[17] Determann, L. (2020, June 9). *How data residency laws can harm privacy, commerce and innovation – and do little for national security*. World Economic Forum. https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/

[18] Wu, E. (2021, July). *Sovereignty and data localization*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/sovereignty-and-data-localization

[19] Google. (n.d.). *Implement data residency and sovereignty requirements*. Google Cloud. https://cloud.google.com/architecture/framework/security/data-residency-sovereignty

[20] InCountry, *What is data residency-as-a-service*.

[21] Prime Minister's Department. (2021, August 9). *Garis panduan pengurusan keselamatan maklumat melalui pengkomputeran awan (cloud computing) dalam perkhidmatan awam* [Surat Pekeliling Am Bil 2 Tahun 2021]. https://www.cgso.gov.my/wp-content/uploads/2021/11/SPA-Bil.2–2021-Garis-Panduan-Pengurusan-Keselamatan-Maklumat-Melalui-Pengkomputeran-Awan-Cloud-Computing-Dalam-Perkhidmatan-Awam.pdf

[22] Ibid.

[23] Ibid.

[24] Official Secrets Act 1972. (2006, January 1). http://mpsegamat.gov.my/sites/default/files/akta09_-_akta_rahsia_rasmi_1972_akta_88_-_bm_bi.pdf

[25] Wolford, B. (n.d.). *What is a GDPR data processing agreement?*. GDPR.eu. https://gdpr.eu/what-is-data-processing-agreement/

[26] Official Journal of the European Union, *Regulations*.

[27] Department of Justice. (n.d.) *Frequently asked questions*. https://www.justice.gov/dag/page/file/1153466/download

[28] ITU. (2022). *Global cybersecurity index 2020*. ITU Publications. https://www.itu.int/epublications/publication/D-STR-GCI.01–2021-HTM-E