SERI
SOCIAL & ECONOMIC RESEARCH INITIATIVE

Digital Regulatory Transformation as an Enabler for Socio-Economic Revitalisation and Growth

NOVEMBER 2021

Contents

Digital Regulatory Transformation as an Enabler for Socio-Economic Revitalisation and Growth

A. INTRODUCTION 01
Chapter 1: Creating a Trusted Environment for Digital Adoption and Growth: A Digital-Native Policy Paradigm 02

1.1 Digital: An engine for Global Growth, Fuelled by Data and Connectivity 04
1.2 The Digital Infrastructure Potential for Malaysia 05
1.2.1 Digital Malaysia – an opportunity to take the lead within ASEAN 07

Chapter 2: Digital Policies for the Digital Era: Proposed Licensing of Data Centres and Cloud Service Providers in Malaysia 08

2.1 Regulatory Clarity in Line with Global Best Practices 08
2.2 Impact on Digital Investment, Data Centre Industry, and the Growth of the Digital Economy 10
2.3 Operational Uncertainty 12
2.4 Licensing Fees & Contribution to Universal Services Provision (USP) Fund 13
2.5 Socio-Economic Impact to Micro, Small & Medium Enterprises 13
2.5.1 Malaysia's MSME Profile 14
2.5.2 MSME Technology Adoption: From Computerisation to Digitalisation 14
2.6 Shareholding 15
2.7 Impact to Talent Development 15

Chapter 3: Harnessing the Value of Data for Inclusive Growth 18

3.1 Balancing Privacy and Benefits from Data – Learnings from The European Union (EU) Approach 19
3.2 The Social and Economic Cost of Data Localisation 20
3.3 Determining What Government Data Lives in the Cloud 22
3.4 Open Data by Default 23
3.5 Responsible Data Sharing/ Data Collaboration Principles 26
3.5.1 Why are Data Collaboration Principles required? 26
3.5.2 Proposed Data Collaborative Principles 27
3.6 Selecting a Trusted Cloud Service Provider for Storing and Processing Data 28
3.7 Law Enforcement Access 28
3.8 Trusted Cloud Principles: a global rules-based approach to privacy and security 29
3.9 Policy Recommendations 31

Secure, trusted, and inclusive application of technology is more critical than ever in a nation's economic recovery. A trusted, responsible, and inclusive digital strategy will form the foundation necessary to meaningfully unlock potential, build resilience, and develop the digital economy. It is imperative that we identify and prioritise agile and timely implementation of key policies to leverage technology as an enabler in socio-economic revitalization and growth.

Today's trade routes are digital, and digital infrastructure forms the highways and railway tracks of the 21st century. Consequently, there is a need to develop future-proof policies and sustain enabling environments to advance the nation and region's economic competitiveness as governments unlock the potential of data estates and national digital infrastructure in building social and economic resilience. COVID-19 has created further impetus for governments around the world to accelerate technology adoption, and it is imperative that this is advanced both ethically and equitably.

To reap the full benefits from technological advances, partnerships, innovation, and resilience will be required in many areas, including information and communication technology, healthcare, trade, labor markets, human capital development, and education. While there is acknowledgement that evolution of technology policy was not happening at the speed of technology itself, there has been divergence, and a tendency for policymaking to occur in isolation of technological advancement. It is most important that there is convergence of policy and technology to avoid regression of policymaking in parallel with technological and societal advancements.

COVID-19 has been catalytic for accelerating digital transformation and technology adoption. This paper seeks to provide policy recommendations, with the objective of ensuring that the opportunities presented by the digital economy are evenly shared, with the challenges facing society identified early and practical solutions applied.

---

[1] *Data estate refers to the system which stores, prepares, models, serves, and visualizes data to identify insights, trends, and unforeseen relations between variables which can support, accelerate, and transform operations for organizations.*

A. Introduction

The COVID-19 pandemic has accelerated digitalisation, leading to a global surge in demand and access to connectivity, cloud services and data centres as governments and businesses move towards digitalization.

Malaysia continues to ride this wave of digitalisation through various efforts, notably the JENDELA fiberisation effort and the launch of the Malaysia Digital Economy Blueprint (MyDIGITAL) in February 2021.

The Malaysia Digital Economy Blueprint (MyDIGITAL), is a national initiative which identifies six strategic thrusts supported by 22 strategies, 48 national initiatives and 28 sectoral initiatives.

During the unveiling of MyDIGITAL, the Prime Minister shared the following :

- Between RM12 billion and RM15 billion will be invested by Cloud Service Provider (CSP) companies over the next five years.
- Conditional approvals have been provided to four Cloud Service Providers (CSPs), i.e., Microsoft, Google, Amazon Web Services, and Telekom Malaysia - to build and manage hyper-scale data centres and cloud services.
- In line with Malaysia's goal to strengthen the capabilities of local companies, three local technology companies have been appointed as Managed Service Providers (MSP) to partner the CSPs in servicing the public sector.

While the Blueprint outlines bold and progressive goals, objectives, and timelines, there appears to be a mismatch between the Government's aspirations and policy implementation.

This is particularly relevant in relation to digital infrastructure (data centres and submarine cables) development, which could put at risk Malaysia's efforts to project regulatory stability and a policy environment that is conducive to investors and foreign direct investment in the digital age.

Consequently, this paper will explore the following areas, in an effort to better understand the implications of current and proposed regulations on Malaysia's digital economy:

1. Regulatory Clarity
2. Investment and Growth of the Data Centre Industry and Digital Economy
3. Operational Uncertainty
4. Socio-economic Impact
    a. Impact to Micro, Small and Medium Enterprises (MSMEs)
5. Shareholding requirements
6. Impact to talent development

Chapter 1

Creating a Trusted Environment for Digital Adoption and Growth: A Digital-Native Policy Paradigm

The global pandemic has resulted in years of digital transformation taking place within months. Virtual meetings, lessons, gatherings, and conferences have increased reliance on digital infrastructure almost overnight, as governments, businesses, and educational institutions scramble to provide continuity for their stakeholders.

Digital infrastructure refers to the systems connecting people to digital information, products, and services. It serves as the backbone of the digital economy and includes both hard (physical) and soft (non-physical) digital infrastructure comprising connectivity, devices, data storage and processing, services, and applications. Similar to the way cables, wires, and generators provide for the electricity needs of citizens, digital infrastructure enables transmission of information and data, underpinning our social and economic lives.

While digital infrastructure once required large up-front investment in equipment such as fiber optics, satellites, and high-powered computing facilities, highly flexible and elastic on-demand cloud computing services have led to a shift from capital expenditure to operational expenditure, lowering the barrier to entry for individuals, businesses, and governments.

Although cost considerations may have diminished with technological advancements, the question of trust remains. Around the world, governments and businesses face an increasing trust deficit, particularly where technology is involved.

Digital Infrastucture powered by Trust

24% of Malaysian technology users trust organizations offering digital services

31% of technology users in Asia Pacific trust organizations offering digital services

44% of Indonesian technology users trust organizations offering digital services

Figure 1: The level of trust in digital services, according to consumers in Malaysia, Indonesia and Asia Pacific (IDC, 2019)

A 2019 study from IDC Asia-Pacific, Understanding Consumer Trust in Digital Services in Asia Pacific[2] revealed that only 24% of technology users in Malaysia, 31% in Asia Pacific and 44% in Indonesia believe their personal data will be treated in a trustworthy manner by organizations offering digital services.

Underpinning leading-edge technological advancements and 21st century digital infrastructure are timeless values such as security, reliability, ethics, privacy, and compliance.

Privacy and Security: As more and more of our lives are captured in digital form, the question of how to preserve our privacy and secure our personal data is becoming more important and more complicated. Trust needs to be incorporated by design, not as an afterthought. While protecting privacy and security and building trust are important to all technology development, recent advances require that we pay even closer attention to these issues to create the levels of trust needed to realize the full benefits of emerging technologies such as artificial intelligence and quantum computing. Like other technologies, digital infrastructure of the 21st century must comply with privacy laws that require transparency about the collection, use and storage of data, and mandate that consumers have appropriate controls so that they can choose how their data is used.

[2] *About the Study: Understanding Consumer Trust in Digital Services in Asia Pacific*

- *6,372 consumers across Asia Pacific participated in this study.*
- *A total of 453 consumers were surveyed in Malaysia, an almost equal ratio of males and females were surveyed: 43% male; 57% female.*
- *Consumers were from four different age groups: Gen Z – 15 years old to 25 years old (20%); Gen Y – 26 years old to 40 years old (30%); Gen X – 41 years old to 55 years old (30%); and Baby Boomers – 56 years old to 75 years old (20%).*
- *All respondents come from a broad spectrum of occupations, from management, professionals to students and home makers.*
- *14 APAC markets involved: Australia, China, Hong Kong, Indonesia, India, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, Thailand, and Vietnam.*
- *An important qualifier for the Study is that these consumers needed to be digitally active in their daily lives, where they regularly perform online activities such as banking, shopping and had social media engagements in the last 90 days.*

Reliability: The complexity of emerging technologies has fuelled fears that systems may cause harm in the face of unforeseen circumstances, or that they can be manipulated to act in harmful ways. As is true for any tool, trust will ultimately depend on whether systems can be operated reliably, safely, and consistently — not only under normal circumstances but also in unexpected conditions or when they are under attack.

As policymakers adapt to unprecedented technological advancement, we have observed a global shift from digital-first to digital-native policymaking, which recognizes the ever-present influence of technology in our lives and livelihoods. Linkages between technology and traditional infrastructure are being mutually reinforced by digital transformation in areas of social and economic importance, e.g., water, education, healthcare, and financial services.

In today's digital-native world, how do we develop an enabling environment for Malaysian digital infrastructure anchored on technology, powered by trust? This paper recognizes the centrality of trust in technology adoption across sectors, and calls for concerted effort unlocking potential within data, and regulatory reform towards a competitive and resilient digital economy for all.

1.1 Digital: An engine for Global Growth, Fuelled by Data and Connectivity

It has taken less than two decades for the internet to go from the computer science laboratory to the engine of global economic growth. Some have deemed data to be the "oil" of this engine, but unlike fuel, data is not finite – there is no scarcity of data, and new data is being produced all the time[3]. The use of data does not diminish the data or the value attached thereto. Data fuels innovation from product cycles to preventing outbreaks.

Data Estate

the infrastructure or framework which allows organizations to manage all their data. Within a data estate, organizations can store and analyse data across all systems in one place.

With the proliferation of data and devices, governments across the Association of Southeast Asian Nations (ASEAN) preside over sprawling data estates. A data estate refers to the system which stores, prepares, models, serves, and visualizes data to identify insights, trends, and unforeseen relations between variables which can support, accelerate, and transform operations for governments and businesses.

Data is the differentiator for governments and businesses seeking to reap the benefits of today's digital economy. IDC predicts the exponential growth of data to be from 18 zettabytes in 2018 to 175 zettabytes by 2025 (one zettabyte is equal to a trillion gigabytes)[4].

[3] *While data is infinite, data centers are not. Consequently. carbon neutral operations and renewable energy use become important considerations in engaging cloud service providers (CSPs).*

[4] *https://bernardmarr.com/default.asp?contentID=1846*

Data is one of the most valuable assets of a nation and serves as the foundation and driver of digital transformation.

As demands on networks are growing due to more people, services, objects, and activities going online, network capacity lags behind in rural parts of the country. To enhance access to networks, services, and data, governments may want to consider promoting competition in the provision of digital services, simplifying administrative procedures, and boosting connectivity in rural and remote areas.

Governments should also review existing frameworks that impact technology with a view to ensuring they assist with the development and deployment of new technologies in a way that is trusted, responsible and inclusive. Conflicting requirements increase compliance costs. Regulatory requirements may need to be updated to provide consistency and clarity in light of the use of emerging technologies.

Questions to ask[5]:

- Which regulations and policies are not ready for the digital age, presenting risks to inclusive growth?
- Which past approaches have been particularly successful/unsuccessful in facilitating innovation, investment and data flows through digital technologies?
- How can policy/regulatory approaches and institutions be transformed to deliver intended outcomes?
- What regulatory reform processes have worked in the past? What is likely to block progress now?

1.2 The Digital Infrastructure Potential for Malaysia

As part of ASEAN, Malaysia could be part of a digital economy 20 times the size of its population. Asia is already leading the world in terms of producing data, in part due to the large amount of industrial robotics in the region[6], and ASEAN is set to become the world's fourth largest economy by 2030; a transition that will be championed by an increasingly tech-savvy younger population which is rapidly scaling the socio-economic ladder. ASEAN's digital economy is expected to expand 6.4 times from US$31 billion in 2015 to US$197 billion by 2025 according to the Economic Research Institute for ASEAN and East Asia (ERIA).

As a region, the general quality of digital infrastructure in ASEAN looks satisfactory compared with that of the world average. However, the development of technology-related infrastructure, between and within countries, is uneven[7]. ASEAN member countries rank from top to 160th on the global Digital Adoption Index (DAI) published by the World Bank.[8]

[5] *https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/Digital_Economy_Kit_JAN_2020.pdf*

[6] *https://www.researchandmarkets.com/reports/4769146/asia-pacific-industrial-robotics-market-by*

[7] *https://www.eria.org/uploads/media/policy-brief/Improving-Digital-Connectivity-Policy-Priority-for-ASEAN-Digital.pdf*

[8] *https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index*

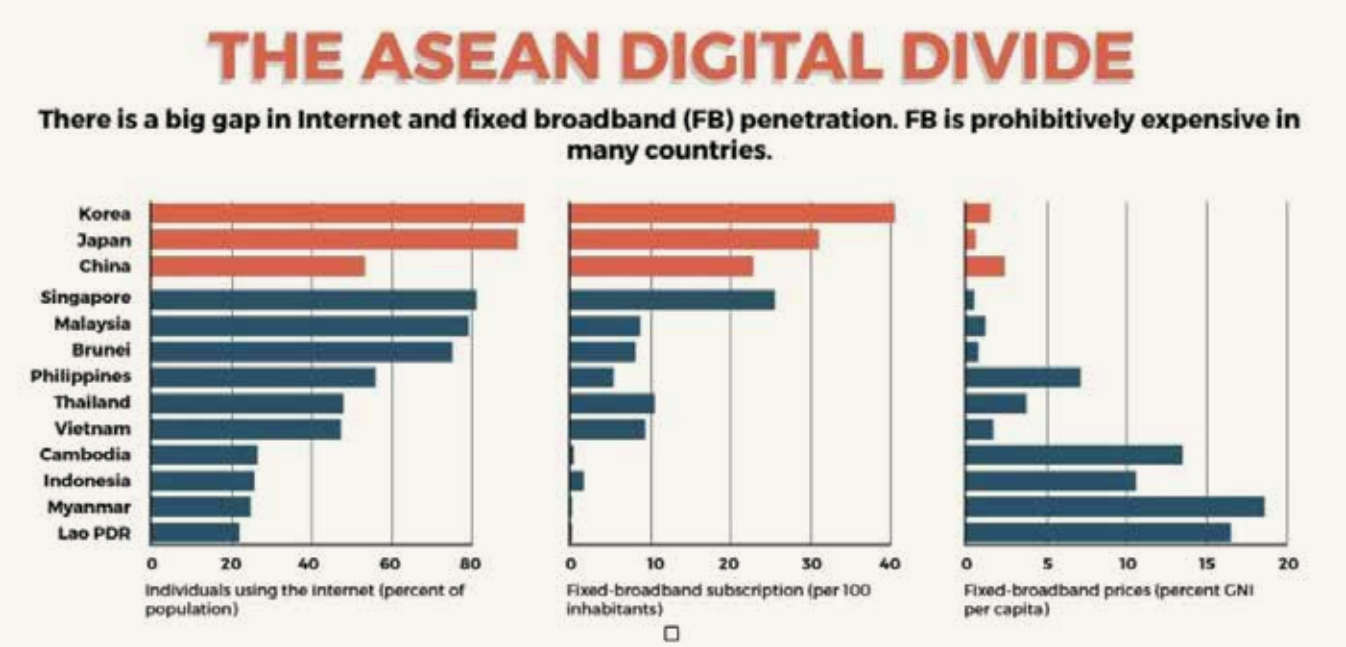


Figure 2: The ASEAN Digital Divide
(International Telecommunications Union and World Bank, 2019) [9]

Singapore tops the ranking at 1st place followed by Malaysia in a distant 41st place; Brunei (58); Thailand (61); Vietnam (91); Philippines (101); Indonesia (109); Cambodia (123); Lao PDR (159) and Myanmar (160).

The Internet has reached most people in Brunei Darussalam, Malaysia, and Singapore, but more than 70 percent of Cambodia, Indonesia, Lao P.D.R., and Myanmar remain offline and do not fully participate in the digital economy. Development of 4G networks and access to electricity continue to be critical issues.

In Malaysia, the digital divide remains wide between urban and rural areas, ranging from high-speed 4G internet to tree-climbing in order to write exams.[10] With the global pandemic forcing the world online, there are both social and economic imperatives for Malaysia and ASEAN member states to further develop digital infrastructure in order to reap the gains of the digital economy, and ensure its people are not left behind.

Policy barriers continue to impede digital transformation as policies made for the analogue world have increasingly become irrelevant or have become a blocker for rapid adoption and accelerated digital transformation. In today's world, transformation requires modernized policies and data platforms that break down silos to unleash data's full potential. Policy barriers have not only become an impediment but in some instances have led to the regression of digital transformation and adoption.

[9] *https://theaseanpost.com/article/digital-asean-everyone*

[10] *https://www.malaymail.com/news/life/2020/06/17/sabah-university-student-spends-24-hours-on-top-of-a-tree-for-better-intern/1876231*

1.2.1 Digital Malaysia – an opportunity to take the lead within ASEAN

Being part of ASEAN presents Malaysia with a unique opportunity to strengthen regional partnerships and take the lead, but this must be centered on efforts to bolster regional economic by developing a genuine single market with free flow of data.

ASEAN has 669 million citizens[11] with rapidly rising spending power. Full implementation of the ASEAN Economic Community will be critical in allowing ASEAN to determine its own economic future, rather than relying on demand from external markets, and providing improved insulation against potential shocks, particularly exacerbated protectionism as a result of COVID-19.

As an economic bloc, ASEAN is the fifth largest economy in the world and the third largest population trailing China and India. With 125,000 new users coming onto the Internet every day, the ASEAN digital economy is projected to add an estimated $1 trillion to regional GDP over the next ten years.[12] Creating a single market for services will be crucial. ASEAN member states must respond to the opportunities and challenges of the Fourth Industrial Revolution coupled with a global pandemic, tackling issues such as harmonization of rules governing the use of data. Emerging technologies – including digital platforms, big-data analytics, and cloud-based services – do not recognize national borders and function best when they operate at scale. With a single digital market, ASEAN can develop truly pan-regional services in finance, healthcare, education, and e-commerce.

Malaysia has made many efforts, such as being one of the early ASEAN adopters of Personal Data Protection legislation, but many significant roadblocks still stand in the way of realizing Malaysia and ASEAN's full potential. ASEAN has developed important policy measures and frameworks, including the ASEAN Economic Community Blueprint 2025, Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement, to address these roadblocks. These ambitious goals will demand detailed research, visionary policy-making, and substantial commitment from regional stakeholders.[13]

With Brunei as current ASEAN chair (2021), Malaysia has an opportunity to leverage its strong bilateral relations with Brunei to provide recommendations and present best practice approaches towards advancing not only Digital Malaysia, but also Digital ASEAN.

[11] *https://www.worldometers.info/world-population/south-eastern-asia-population/*

[12] *https://www.weforum.org/projects/digital-asean*

[13] *https://www.weforum.org/projects/digital-asean*

Chapter 2

Digital Policies for the Digital Era: Proposed Licensing of Data Centres and Cloud Service Providers in Malaysia

While the bold aspirations laid out in the Malaysia Digital Economy Blueprint (MyDIGITAL) certainly promise to propel Malaysia forward, there have been some recent policy decisions resulting in great concern across the technology industry. One such decision is the Malaysian Communications and Multimedia Commission (MCMC)'s intent to subject data centres and cloud services providers to the licensing obligations of the Communications and Multimedia Act 1998 (CMA 1998).

The following section explores some perspectives as shared by local and international members of the technology industry, representing data centre providers, technology companies, cloud service providers, web hosters, and internet users:

2.1 Regulatory Clarity in Line with Global Best Practices

The 'global by default' nature of the digital economy requires public sector and private sector to jointly chart the path forward in the best interests of the nation. While the Malaysian Communications and Multimedia Commission (MCMC) undoubtedly has certain rationale and justifications for the decision to impose licensing, the proposed introduction of a licensing scheme contrary to international best practices would put at risk Malaysia's efforts to project regulatory stability and a policy environment that is conducive to investors and foreign direct investment in the digital age.

A look at the international regulatory landscape for data centre and cloud computing shows that China, with its 1.4 billion population, remains the only jurisdiction in the world which subjects cloud services to its telecommunications licensing regime.

	Licensing Policy	Data Protection Policies
Malaysia	Licensing planned to commence on 1st January 2022	Personal Data Protection Act (PDPA)
Singapore	No licensing requirement	Personal data protection laws apply to data centres (equivalent to our PDPA)
Indonesia	• No licensing requirement • Registration of service providers	Data residency requirements recently relaxed to allow use of foreign public cloud
Vietnam	No licensing requirement	Guidelines for e-government (equivalent to our own Cloud First Policy)
Australia	No licensing requirement	Data privacy act (equivalent to our PDPA)
China	"Value Added License" with foreign equity limitations	Strict laws on cross border data transfer
USA	No licensing requirement	Data privacy laws and law enforcement data disclosure processes under the CLOUD Act
EU	No licensing requirement	Data privacy laws (GDPR)

Figure 3: International Regulatory Landscape Relevant to Data Centre & Cloud Services

The European Union, the United States, and neighbouring countries such as Indonesia, Vietnam, and Singapore currently rely on international standards such as ISO/IEC 27001, 27017, 27018, Uptime Institute Tier III or IV, TIA 942D, and PCI DSS to provide trust and assurance.

In Malaysia, MCMC has previously released a voluntary Technical Code for Cloud Service Provider Selection while Bank Negara Malaysia and Securities Commission Malaysia have issued their own respective guidelines.

In a sector that relies on globally accepted standards, the introduction of its own licensing regime would hamper Malaysia's ability to further enhance its competitiveness and participate in digital economy free trade agreements.

The technology industry has expressed willingness to collaborate towards the development of policies to attract domestic and international investment; however, the introduction of a licensing scheme may be counterproductive towards efforts to decrease complexity and increase the ease of doing business in Malaysia.

Below are some thoughts from members of the technology industry:

"Malaysia is still at the nascent stage for DC & Cloud services (60MW market size in Malaysia vs 483MW market size in Singapore). The role of the country was clearly outlined in MyDigital where the government wants to grow data centres by building a stronger and more robust ecosystem."

"While other governments are signing digital economy agreements and focusing on open cross border data flows, this licensing can be construed as a non-tariff barrier to entry. Many countries are moving towards giving special status for Data Centre players as digital infrastructure providers to promote the sector while Malaysia may be seen to be going in the opposite direction."

2.2 Impact on Digital Investment, Data Centre Industry, and the Growth of the Digital Economy

Implementing a licensing framework on data centres and cloud service providers will reduce Malaysia's appeal and competitiveness as an investment destination, impacting broader socio-economic growth in the country. Multiple local and foreign data centre investments planned for 2022 are currently under immediate suspension and review pending this data centre licensing decision.

Data centre investment improves digital and physical infrastructure, creates employment opportunities, and increases the pool of skilled workers, impacting economic growth and competitiveness. Absent the implementation of this licensing proposal, the Malaysia data centre market is expected to grow at a CAGR of over 16% during the period 2021–2026. With a small but steadily growing market, it is an opportune time for Malaysia to introduce enabling policies and position itself as a technology investment hub.

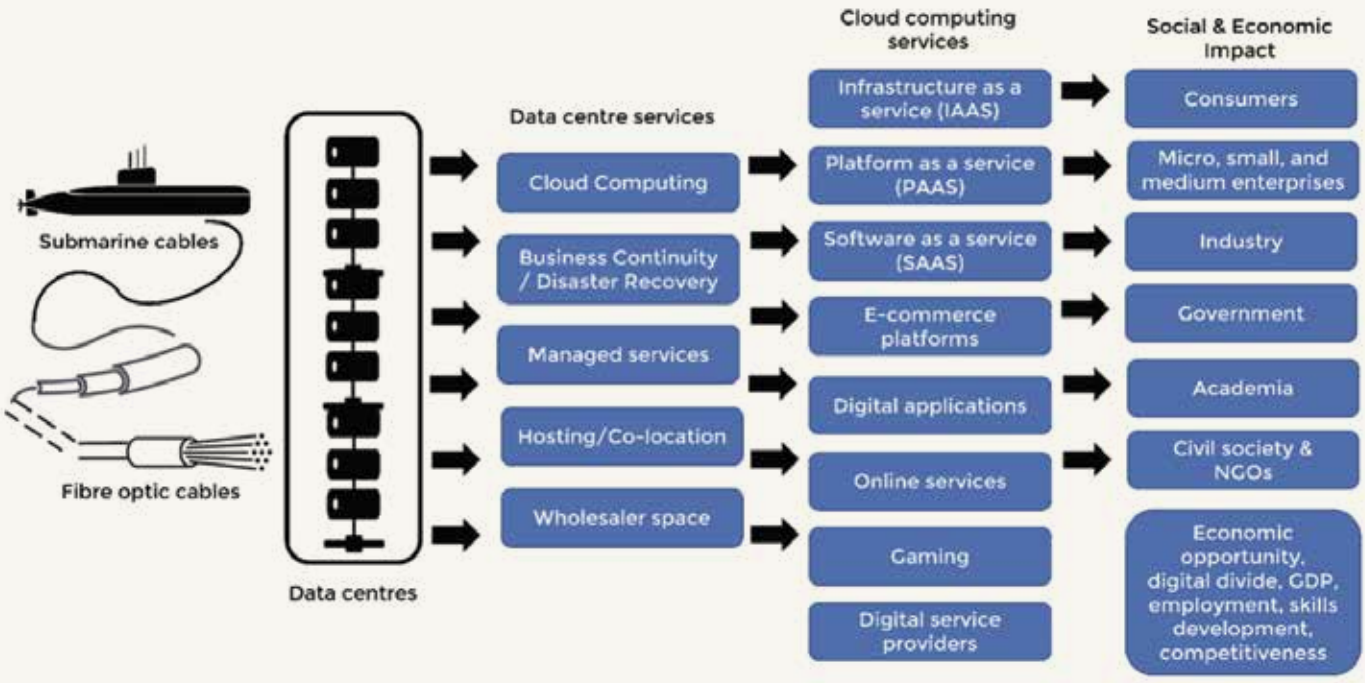


Figure 4: Digital Infrastructure Ecosystem

Members of the technology industry are concerned that Malaysia's ability to further enhance its competitiveness as a business-friendly digital economy will be hampered by the introduction of a licensing regime in a sector that relies on industry driven regulation in the form of globally accepted standards. The nation's ability to participate in digital economy free trade agreements would also be complicated by regulations that are deemed to be regressive and contradictory to efforts to promote a competitive and open data flow regime.

The industry welcomes progressive policies and regulations to attract investment, but these should not take the form of a licensing scheme which regulates cloud service providers and data centres as telecommunications services providers. The Ministry of Communications and Multimedia (KKMM)'s commitment to review the Personal Data Protection Act 2010 and extend its application beyond commercial transactions is one example of the Government's efforts to build trust and create an enabling policy environment, in line with global best practices. This will ensure that laws, practices, and enforcement regarding personal data protection and privacy are comprehensive and fit-for-purpose, in line with the needs of the digital age

Below are some thoughts from the technology industry:

"Any global company that wants to invest in Malaysia will make a comparison with other markets. No other country in Asian region is introducing this licensing regime where there's also a financial impact. Singapore has imposed a moratorium on data centres and it might be lifted soon. This is the time to attract investments and not to put up more blockers and affect investment decisions."

"Access to digital infrastructure such as data centres and cloud is borderless so we are not just competing in Malaysia where we can control the pricing but we are competing with many other players in the region. Local players will be at a disadvantage in terms of cost and competitiveness. Licensing will add additional layers of hidden costs to the various providers and users within the ecosystem."

"What is the economic reverse impact of this regulation? How much foreign direct investment (FDI) will Malaysia potentially lose due to this? Post pandemic, can Malaysia afford to miss out on influx of foreign capital? Regulations will also almost guarantee capital flight from Malaysia to neighbouring countries. The Cloud industry is very agile and service providers can easily move to other countries."

2.3 Operational Uncertainty

The CMA 1998 was drawn up to regulate telecommunications services, and 'data centre and cloud services' are not explicitly defined in the Act. The new licensing proposal thus risks exceeding the CMA's legal remit. The far-reaching implications of the proposed licensing scheme will also impact end users such as micro, small, and medium enterprises (MSMEs) who are increasingly reliant on cloud-based digital platforms to reach their customers. Their ability to survive will be severely impacted by the rising costs of digitalisation as the Universal Services Provision Fund fee will be passed on to them. Additionally, only 44% of Malaysian SMEs use cloud computing compared to 85% of SMEs in Singapore.

With the licensing scheme threatening to create additional multiple layers of cost and complexity, MSMEs, enterprises, customers, and end users will almost certainly look to migrate hosting and use of cloud services outside Malaysia.

Industry views are as follows:

> ***"The proposed regulation is likely to kill the industry instead of helping it to grow. It will add a lot of uncertainty and complexity in terms of operation and force a lot more players to operate outside the country."***

> ***"Licensing regime for the telcos cannot be simply applied to data centre and Cloud services without taking into account the differences of the services offered and the customers they serve."***

While the CMA has served us well since it was drafted in 1998, we must recognise that it was not made with 21st century technology in mind. As the technology environment has evolved exponentially, perhaps it is time for Malaysia to reconsider existing regulation in partnership with industry and civil society, to avoid laws and policies being force-fitted or retro-fitted into scenarios which may not have been envisioned at the time of drafting.

2.4 Licensing Fees & Contribution to Universal Services Provision (USP) Fund

Based on the initially proposed licensing scheme, all licensees must contribute 6% of revenue to the USP Fund once they reach the minimum revenue threshold of RM2 million. This requirement is unprecedented and unheard of anywhere else in the world. It would be detrimental to the growth of small-to-medium sized Malaysian technology companies and would increase costs to licensees and end users by 20% to 40%. This would not only impact research, development, and innovation efforts, but would also be viewed as a non-tariff barrier that would decrease market opportunities and reduce Malaysia's appeal and competitiveness as an investment destination. It is certainly encouraging that the government has considered the industry's feedback in this regard, and opted for a different approach that does not include a USP Fund contribution. Nonetheless, further clarity is still being sought by members of the technology industry.

With the borderless nature of cloud hosting services, local cloud providers and technology companies could be encouraged to redomicile to neighbouring countries, with less costly, less complex regulations, impacting MyDIGITAL's aim to create 5,000 start-ups and 500,000 jobs by 2025.

Below are views shared by members of the technology industry:

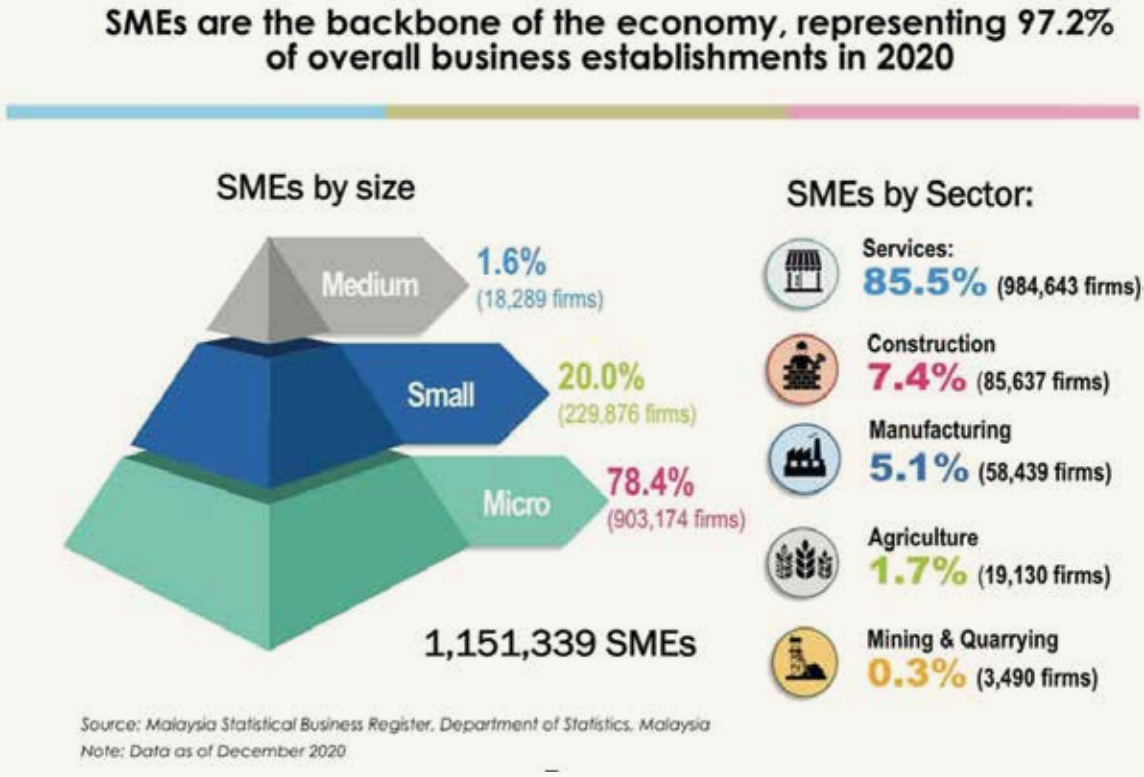
> ***"The USP requirement is perceived as a double taxation scheme by potential customers and investors. This is likely to make Malaysian data centre players less attractive and competitive."***

2.5 Socio-Economic Impact to Micro, Small & Medium Enterprises

> ***"In the context of the USP fund, telecommunications providers require extensive infrastructure to provide service across the country so that the citizens will benefit from that infrastructure rollout and choose from various telecommunications service providers to subscribe. It is not possible to apply that concept to cloud service providers and data centres because individual consumers do not buy data centre (DC) or Cloud services. There is no correlation of how the USP contribution would benefit the greater society and the DC and Cloud industry."***

2.5.1 Malaysia's MSME Profile

Based on the Department of Statistics, Malaysia (DOSM), the total number of SMEs in Malaysia in 2020 was 1,151,339 or 97.2% of total business establishments. On average, number of SMEs increased by 4.9% every year since 2015, with micro enterprises accounting for 78.4% (903,174), as the largest share of SMEs.[14]



2.5.2 MSME Technology Adoption: From Computerisation to Digitalisation

With greater recognition of technology's role in not only enabling productivity for MSMEs, but also acting as a critical competitive advantage and growth catalyst, governments in ASEAN and around the world are developing incentives and policies to ease the transition from computerisation to digitalisation. Two examples are as follows:

- Singapore: SMEs Go Digital programme by the Infocomm Media Development Authority (IMDA) aims to make going digital simple for SMEs via grants and sector-specific roadmaps for digital adoption.[15]

- Thailand: a 200% tax deduction for the purchase of smart devices, digital services, robotics and Internet of Things (IoT) devices by small and medium-sized enterprises (SMEs), in addition to software, starting in 2020 [16]

[14] *SME Corporation Malaysia - Profile of SMEs in Malaysia*

[15] *Factsheet.pdf (imda.gov.sg)*

[16] *Thai gov introduces tax perks to help SMEs go digital – OpenGov Asia*

During the pandemic, the Malaysian government worked hard to provide economic relief and enable digitalization of small businesses. Efforts included the SME digitalization grant via an allocation of RM 100 million where each SME received a RM 5000 matching grant. SMEs were also onboarded to established digital commerce platforms, enabling their access to customers across the country.

While this certainly demonstrated the Malaysian Government's commitment to partnering MSMEs and ensuring they remain afloat, the proposed licensing of data centres and cloud service providers could potentially undo the progress and benefits gained by previous efforts to digitalise MSMEs.

According to a study conducted in 2018,[17] only 44% of SMEs use cloud computing, mostly for online storage capabilities. Only 35% of these organisations (out of the 44%) use cloud business applications, illustrating the large opportunity that remains untapped in relation to MSME digitalisation.

2.6 Shareholding

The Government's effort to allow Multimedia Super Corridor (MSC) status companies to hold 100% foreign shareholding has been well received across the technology ecosystem; however, there is great concern regarding Bumiputera and foreign shareholding conditions related to Individual licensees. With the cross-border and global nature of the digital economy, countries around the world are opening up their economies, welcoming foreign investment and innovation anchored on digital cross-border trade. Malaysia cannot afford to move in the opposite direction implementing discretionary Ministerial powers and added layers of complexity is akin to Malaysia closing its doors when the world is now open for business. To ensure Malaysia can continue attracting global technology investment, full foreign shareholding needs to be allowed across all licence categories.

2.7 Impact to Talent Development

Developing a global digital workforce will depend on an inclusive and accessible talent ecosystem. Skills and talent development fit for the digital era, anchored on reskilling, upskilling life-long learning.

According to a survey conducted by the Strategic Change Management Office (SCMO)[18] and the Social & Economic Research Initiative (SERI) in July 2021,[19] on average, only 4.8% of private sector organisations surveyed felt that the existing labour market is able to fully meet their digital talent needs. Even among the top 5 technologies for which the labour market was able to meet talent needs, the degree to which the needs were met was low, with e-commerce and digital trade topping the list at 58%.

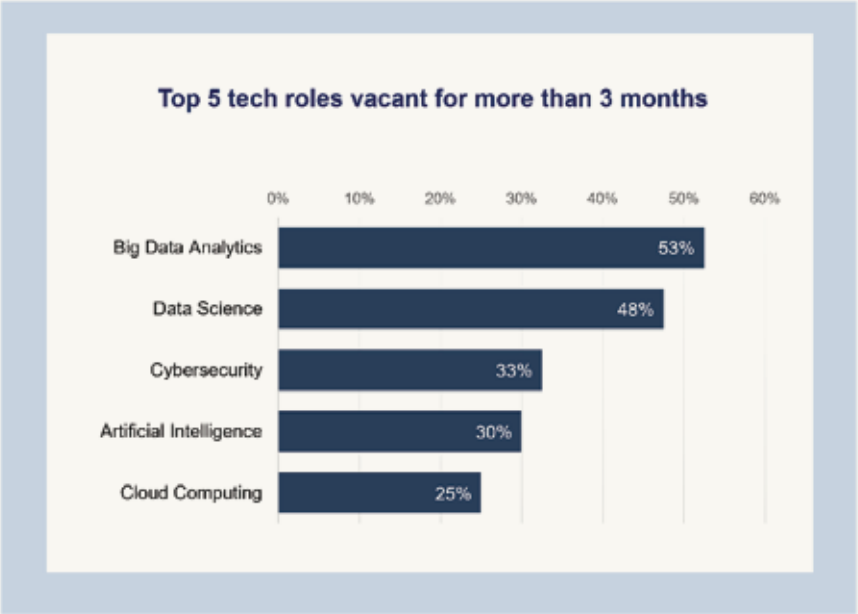
---

[17] *the-state-of-smes-ict-adoption-in-malaysia (huawei.com)*

[18] *The SCMO is an agency within the Economic Planning Unit entrusted to ensure the delivery of the initiatives spelled out in the Malaysia Digital Economic Blueprint and the National 4IR Policy.*

[19] *Digital Talent in Malaysia: Challenges, Opportunities and Trends*

Tech roles that are challenging to fill



"Lack of capable local skills that is affordable"

"Lack of highly skilled local talents with experience"

"Low budget allocation to attract quality talents"

"Unable to match salary offered by larger technology companies"

Figure 6: Technology roles that are challenging to fill (Digital Talent Survey 2021)

The survey identified the costs of digitalisation and adoption of latest technologies as a challenge to effective digital adoption – this included the costs of the talent required to adopt technology. Given the competitiveness of the labour market for digital talent, the survey found that micro, small, and medium enterprises (MSMEs) face various limitations and require the government's support in order to sustain themselves. Below are some views shared by survey respondents:

Catching up with technology can be costly to businesses.

Despite ability to source local talent, operational expenditure is impacted by the need to offer salary structures that can compete with big organisations.

As a manufacturing company, the cost to transform our current facility with digital technology will require large financial investment due to the cost of the system, and customised automation for selected processes. This will increase our production cost and will require a long period for return on investment (ROI). Hiring of staff with the capability to maintain and troubleshoot the system is also expensive as most digital talents opt to be hired by multinational companies. For that matter, if government can consider providing grants or other incentives, this will help companies like ours adapt to digitalization.

In building a successful data centre and cloud computing ecosystem, there is a need for a good balance of value, profitability, and well served customers with speed, quality, capacity, and reliability. Our assessment of successful data centre and cloud service provider ecosystems clearly shows that these markets are industry-regulated and do not require or rely on licensing schemes. Regulations for the digital era should reflect agile policymaking and increase the ease of doing business – increased costs will increase the barrier to entry, resulting in an unlevel playing field particularly for smaller businesses.

The digital economy may be seemingly borderless but Malaysia's ability to participate and grow its revenue is dependent on our policy and regulatory landscape. Licensing of data centres and cloud service providers is not in line with global best practice and will not directly translate to increased trust, clarity, or data protection as intended by MCMC.

Malaysia's data centre industry is growing positively as demand continues to surge. At the same time, there is significant competition among key ASEAN countries where progressive regulatory environments, attractive incentive packages, continuous upgrading of infrastructure and bigger demand continue to attract global players. With the current window of opportunity for Malaysia, both the government and private sector must collaborate and focus on building the ecosystem and creating an enabling environment, to ensure that we do not stunt the growth of the industry.

Chapter 3

Harnessing the Value of Data for Inclusive Growth

With data providing the fuel for today's digital economy, enabling responsible access to data is essential as nations around the world undergo digital transformation. A modern and pragmatic approach to open data will drive innovation and agile policymaking. This can only be enabled with progressive and modernised regulation, similar to banking laws and confidentiality provisions which were introduced when banking regulations were first developed. Today's regulatory frameworks have to be built on the premise that we live in a digital-native world.

Open data frameworks and cross-border data flow have become integral to the global digital economy and Malaysia's ability to reap the benefits of digitalisation. However, despite the growing need for access to data and evidence of its economic and social benefits, data access and sharing remains below its potential. Compared to data, there is far greater regulatory clarity in relation to cross-border access to goods or funds.

Opening up access to government data would bring us closer towards data-driven research, journalism, and policymaking. Smart cities, for example, are built on both technology and data. While technology may enable transport systems or waste management facilities to be connected, it is data collection and analysis that will make them 'smart', allowing for trends to be examined, and resources to be optimised.

Although there have been efforts such as the Malaysia Open Data Portal (data.gov.my), we can certainly do more. For instance, although the national budget provides allocations for software and hardware procurement, we must also include technology budget line items for data cleaning, data organisation, and skills development.

According to the 12th Malaysia Plan, in an effort to strengthen open data governance, a national data governance framework will be established to bolster data sharing among the public and private sectors. The framework will incorporate policies, guidelines, legal and investment measures. In addition to enabling the development of a comprehensive database to identify and address socio-economic issues in a targeted and personalised manner, this initiative demonstrates a clear recognition for the need to increase digitalisation and technology investments, in line with Malaysia's target to boost investments from the private and public sectors to RM258 billion and RM80 billion, respectively, by 2025.

3.1 Balancing Privacy and Benefits from Data – Learnings from The European Union (EU) Approach

ASEAN has taken strong steps to facilitate the flow of data across borders within the region, including the ASEAN Framework on Digital Data Governance adopted in 2018. Similarly, the European Union (EU), the world's largest economic bloc, has successfully enabled free movement of goods, services, people, and data. Besides being the second-highest source of foreign-direct investment in ASEAN at 18.6% (after intra-ASEAN trade at 19.4%),[20] the European Union offers some learnings and ways forward in the development of a coherent regional data economy for South East Asia.

In May 2018, the General Data Protection Regulation (GDPR) came into force, as part of a regional effort to make Europe fit for the digital age. As more than 90% of Europeans say they want the same data protection rights across the EU regardless of where their data is processed,[21] the GDPR regulates the processing of personal data relating to individuals in the EU, by an individual, a company or an organization.[22] The GDPR has been used as a model for personal data privacy laws, and has resulted in three main outcomes: legal certainty, providing citizens with more control over their data, and providing businesses across Europe a common standard of data protection.

In June 2018, the EU boosted its data economy by introducing a regulatory reform which created a single market for data storage and processing services for both personal data and non-personal data. The regulatory reform complemented the GDPR by removing all restrictions imposed by member states' public authorities on the geographical location for storing or processing of non-personal data unless such restrictions are justified on grounds of public security. Important sources of non-personal data include the rapidly expanding Internet of Things, artificial intelligence, and machine learning. Current uses of aggregated and anonymized sets of non-personal data include big data analytics and precision farming.[23]

If a data set contains both personal and non-personal data, the EU General Data Protection Regulation will apply to the personal data within the set,[24] while the non-personal data[25] will be covered by the regulation on free flow of data. The freedom to choose a technology service provider anywhere in Europe has led to more innovative data-driven services and more competitive prices for businesses, consumers, and public administrations.[26] Removing data localisation restrictions has been considered a key factor in ensuring that the European data economy can achieve its full potential and double its contribution to 4% of European GDP in 2020.[27]

---

[20] *https://www.imf.org/external/pubs/ft/fandd/2018/09/asean-digital-economy-infographic-feng.htm*

[21] *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en*

[22] *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en*

[23] *https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data*

[24] *The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. Article 1(3), General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN*

[25] *https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data*

[26] *https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/eu-to-ban-data-localisation-restrictions-as-ambassadors-approve-deal-on-free-flow-of-data/*

[27] *http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf*

Recent court actions in the EU - notably the Court of Justice's ruling in the so-called "Schrems 2" case - have highlighted the vulnerability of GDPR's prescriptive limitations on transfers of personal data. The "Schrems 2" case established a new requirement for transfers of personal data to consider the equivalence of the national security laws and judicial redress provisions in a third country with those codified under European Union treaties. While there remains much confusion over how this ruling will impact data transfers over time, assessing national security laws of third countries, as well as rights for EU citizens in third-country courts presents a key consideration in navigating the free flow of personal data & expansion of digital trade.

3.2 The Social and Economic Cost of Data Localisation

With data being widely accepted as the lifeblood for the digital economy, we continue to observe tensions between the free flow of data for innovation and economic growth, and the protection of personal data. One result of this tension is data localisation.

Data localisation refers to measures restricting data flows and can take several forms. From least restrictive to most restrictive, these measures include:[28]

- Prior consent before data is transferred outside national borders.
- One copy of data must reside within national borders, and copies can be transferred abroad.
- Data must be stored in servers located within a country's borders and cannot be transferred outside national borders

Data Isolation

In its most restrictive form, data localisation requires any entity that processes the data of a given country to store that data on servers within said country's borders.

Data localisation is a costly response to what is perceived to be loss of digital sovereignty. Data localisation requirements are a setback for the digital economy, as start-ups and scale-ups will have to pay for the prohibitive cost of compliance, and will not be able to utilise regional or global services which may have servers abroad.

The European Center for International Political Economy found that enacted or proposed data localisation policies in China, for instance, would cost 1.1% of its GDP:[29] reducing domestic investment by 1.8%, exports by 1.7%, and welfare (economic cost to citizens) by the equivalent of 13% of each citizen's salary. Empirical evidence shows that data localisation and other barriers to data flows impose significant costs, reducing India's GDP, for example, by 0.1-0.7 percent.[30] In the European Union, data localisation costs would add up to 0.4% of its GDP, reduce investment by 3.9%, and result in welfare costs up to $193 billion.

[28] *https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf*

[29] *http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf*

[30] *https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf*

Figure 7: Impact of Data Localisation on GDP and Investments (ASEAN Post, 2019)[31]

Data localisation is a costly response to what is perceived to be loss of digital sovereignty. Data localisation requirements are a setback for the digital economy, as start-ups and scale-ups will have to pay for the prohibitive cost of compliance, and will not be able to utilise regional or global services which may have servers abroad.

The European Center for International Political Economy found that enacted or proposed data localisation policies in China, for instance, would cost 1.1% of its GDP: reducing domestic investment by 1.8%, exports by 1.7%, and welfare (economic cost to citizens) by the equivalent of 13% of each citizen's salary. Empirical evidence shows that data localisation and other barriers to data flows impose significant costs, reducing India's GDP, for example, by 0.1-0.7 percent. In the European Union, data localisation costs would add up to 0.4% of its GDP, reduce investment by 3.9%, and result in welfare costs up to $193 billion.

Restrictions on the free movement of data tend to arise from concerns over privacy, security, and lack of control. Governments implement data localisation with the justification of protecting citizens, preserving national security, allowing law enforcement to have rapid access to data, and improving economic growth or competitiveness, while also achieving the underlying objective of prioritising local firms while excluding foreign competitors. However, data protectionism has proved to be counterproductive in today's digital economy, causing lower domestic economic growth and reduced exports.[32]

[31] *https://theaseanpost.com/article/southeast-asias-data-localisation*

[32] *https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf*

Security is often the main concern when discussing cross-border data flow, and the use of cloud computing systems which store and process data outside national borders. While there is a widely held perception that servers under one's roof are safer than servers stored abroad, there is little evidence to support the contention that data is safer when stored domestically. Data localisation requirements do not enhance security; they merely enhance the perception of control.

Control over data is not lost when storing data in the cloud. Cloud technology providers are held to global privacy and security standards and compliance requirements, with some cloud providers extending the protection afforded by the EU GDPR to technology users around the world.

As regulators continue the important work of protecting national interests, it is important to note that cloud computing does not employ an 'all-or-nothing' approach. With the cloud evolving to support the diverse needs of businesses and governments, data classification and the availability of hybrid options provide organizations with the option to determine which information remains onshore and which data is stored in the cloud.

3.3 Determining What Government Data Lives in the Cloud

While there has been broad adoption of cloud by the private sector, businesses and organisations driven by the economics, agility and security, the public sector has been more cautious and reserved.[33] This is largely due to legacy policies that were designed for physical documents, and the lack of appreciation on how far cloud service providers have matured in safeguarding the privacy of data through strong security and contractual obligations.

Proper, risk-based data classification of government data ensures that data is handled based on the potential impact to national security in the event that data is compromised or lost. Unfortunately, it is observed that many government agencies default to classifying their data as Official Secrets unnecessarily. Overclassifying and overprotecting data has serious implications for cost and overall efficiency as each increased level of classification results in:

1. **Increase in infrastructure cost:** data classified as Official Secrets will not be able to leverage on the economics of the hyperscale cloud. The cost of compliant on-premise or private cloud computing and storage may be up to 10 times more expensive than the public hyperscale cloud.
2. **Security costs:** the additional security requirements for the on-premise or private infrastructure will add significant software, hardware and implementation costs. These features would typically be available out of the box through configuration in hyperscale cloud.
3. **Information management overheads:** the additional controls include special personnel such as the data classification officer and the registrar to manage the whole life cycle of the electronic records.

[33] *https://www.forbes.com/sites/forbestechcouncil/2019/04/19/government-in-the-cloud-adoption-has-become-safer-and-smarter/?sh=48380e427323*

4 **Inconvenient and restrictive:** at every step of the life cycle, the data stakeholders will need to record the creation, updates, sharing, archiving and deleting of Official Records. Further,other than managing the lifecycle of electronic documents (such as Word documents, PowerPoints etc), these requirements may be impractical for systems that process electronic records associated with transactional systems**.**

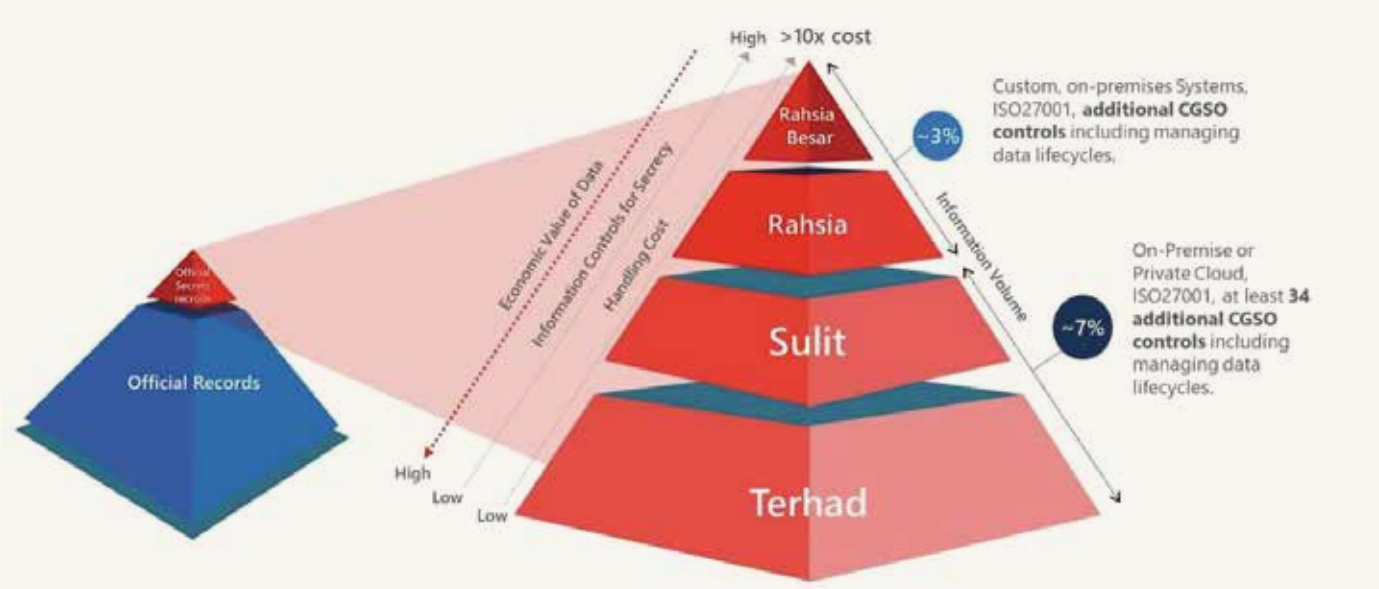


Figure 8: Classification for Official Secret Records

Given that emerging technologies such as artificial intelligence and data science are data and processing intensive, a cloud first strategy would be required. This can only be achieved if data is classified as an Official Record by default rather than an Official Secret.

3.4 Open Data by Default

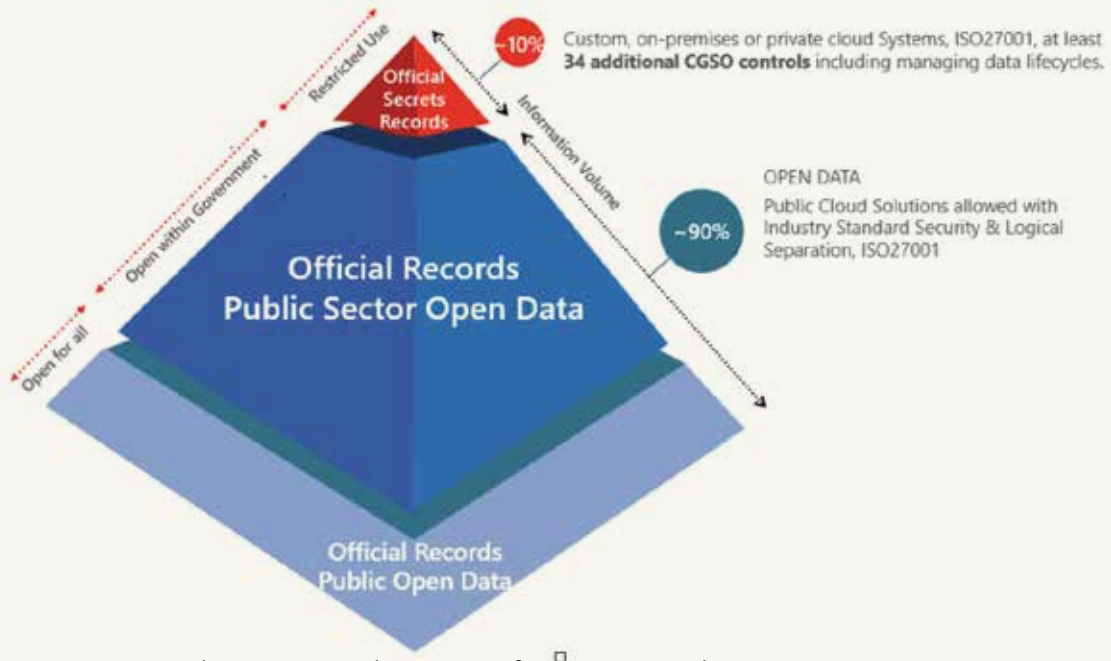


Figure 9: Mapping types of government data to Open Data

The value of data can only be harnessed through technology if democratised by making it open for sharing. This is difficult if classified as Official Secret, but if government data is made Official by default, then in general most of the data could be made Open. As shown in Figure 10 above, there are two types of Open Data:

1. **Public Sector Open Data:** these are Official records that can be shared within government agencies for any purpose-driven collaboration for government workloads.
2. **Public Open Data:** these are Official records that have been made publicly available to anyone. This allows the larger ecosystem to benefit from government data.

The percentage of Open Data shown in figure 10 is intended to convey rough relative values, and while this may differ from country to country, here are some interesting trends:

- Governments create a lot of data, but most of it is of low sensitivity. There is an increasing recognition by governments that they have large amounts of non-sensitive data which allows for consideration of the use of public cloud.[34]

- At the other end of the spectrum, there is no doubt that countries create some of the most sensitive information on the planet, and that such information will be subject to the most stringent security, regardless of how much that security might cost.

Public Cloud

The most common way of deploying cloud computing. Computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. They may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume.

- The key point is that while these high security costs make incredibly good sense for the most sensitive information, this applies to a very small percentage of government data. Needlessly applying those high security requirements to all government data results in loss of significant potential cost savings.

It is important to note that all public sector data has the same level of sensitivity. The majority of data is not highly classified (i.e., unauthorized disclosure would not present a serious threat to national security) and should be able to move to public cloud which provides cost savings and better security compared to conventional on-premises options.

Placing Government Data by default under the protection of the Official Secrets Act results in costlier technology infrastructure due to higher costs for security and data protection. This is in part due to existing infrastructure and processes being designed for analogue systems.

[34] *Cloud resources (e.g., servers and storage) are delivered over the Internet for the data owner, by a third-party cloud service provider. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud service provider.*

Consequently, procedures related to the Official Secrets Act (OSA) tend to be more labour and time intensive. For example, amendment or deletion of Official Secret data requires physical registration of the proposed amendment with an officer, who will then process the request. The requested amendment/deletion can only be made once approval has been obtained. This is not just inefficient but entirely unsuitable for the purposes of maintaining databases.

Besides time and cost considerations, a "closed by default" or "OSA by default" policy also intensifies the challenge of data sharing.

In some cases, new legislation may need to be developed to replace laws from a different era. E.g., modernisation of law enforcements access to data, and proper risk-based data classification of government data to ensure that data is handled based on the potential impact to national security if data is compromised or lost.

While the current practice is such that the majority of Government data is classified as Official Secret, the Chief Government Security Officer (CGSO) expects that more than 80% of government data is non-OSA data. Based on this assessment, the below diagram illustrates the estimated breakdown of OSA data:

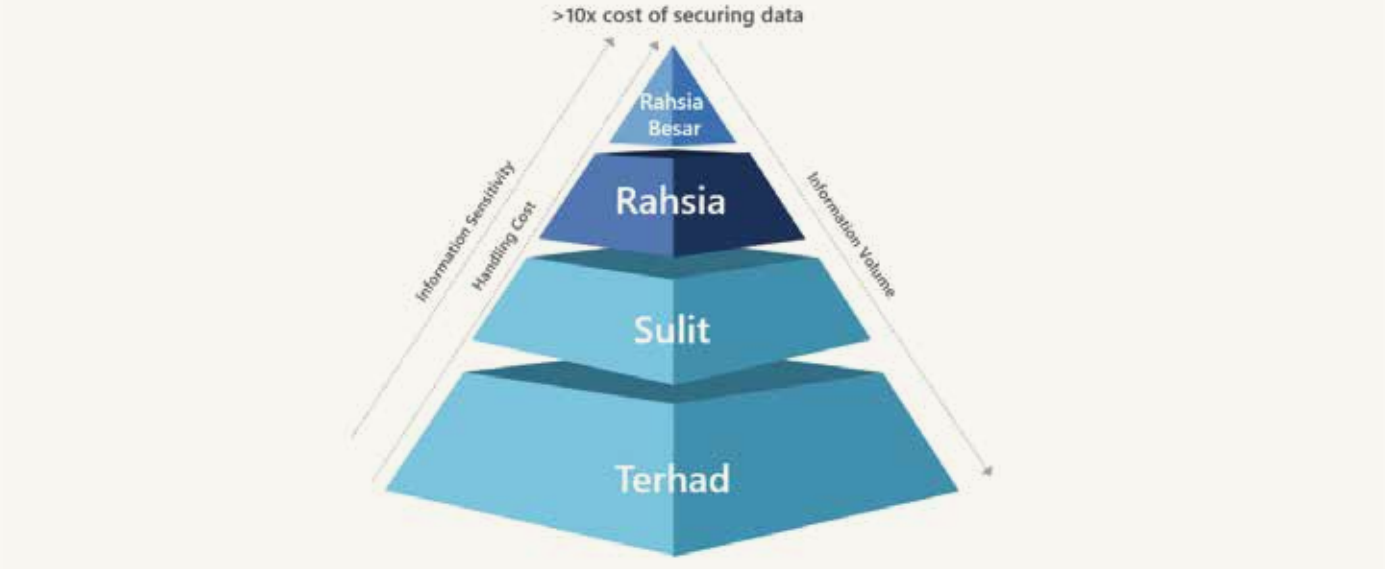


Figure 10: Estimated breakdown of OSA Data based on the 4 categories (Rahsia Besar, Rahsia, Sulit, and Terhad)

As part of an effective cloud-first and digital-native policy, a clear data classification policy for public sector data should be in place that identifies categories of sensitivity of data, and allows the vast majority of data to move to public cloud.

Given the accelerated development of technology, policies and regulations related to data governance must be reviewed and revised to ensure Malaysia's policy environment enables innovation, competitiveness, and greater economic growth. Forcibly applying analogue policies to circumstances requiring digital-native policies will not bode well for Malaysia's development.

In addition to the use of public cloud as the default option, private cloud deployment models should only be an option for the most sensitive data where its unauthorized disclosure would present a serious threat to national security.

The classification policy should provide for a harmonised approach across government, while allowing individual agencies to go through their own process of identifying which data falls into which category. This should be part of each Ministry's information management policy. The Government should also consider having a designated officer per Ministry, who would oversee and be ultimately accountable for the Ministry's data classification decisions. This would also facilitate the creation of standards for data classification across the different parts of government.

3.5 Responsible Data Sharing/ Data Collaboration Principles

3.5.1 Why are Data Collaboration Principles required?

1. **Enable Collaboration for innovation:** partnerships and data collaboration will enrich the insights and value which can be extracted from data. This will help fuel rapid innovation.
2. **Enable Value Extraction:** Organisations must enable the extraction of economic and strategic value through processing of raw data.
3. **Economic Sustainability:** Managing the data lifecycle incurs huge cost considerations. This includes creation, management, storage of data. Value extraction via data collaborative efforts will enable greater returns on investment, and consequently fuel further data creation and value extraction initiatives.
4. **Balance Challenges, Risks, and Opportunities:** Sharing of Data involves balancing considerations such as privacy, competitive advantage, and compliance.
5. **Move from Closed by Default to Open by Default:** Present norms usually result in Closed Data, which restricts the ability to harness the benefits of data. An Open by Default approach would allow organisations to gain insights and make data-driven decisions.
6. **Addressing FUD:** At present, there is a great amount of Fear, Uncertainty, and Doubt which is inhibiting data sharing and value extraction from data within departments, agencies, and organisations.

3.5.2 Proposed Data Collaborative Principles

1. **Open by Default:** By default, all data should be made open by the data owners to all data collaborative stakeholders.
2. **Security and Privacy by Design:** Best practices for security and privacy must be implemented in the data collaborative.
3. **Purpose-Driven Data Sharing:** Only data that is demanded by the problem should be shared by data owners. Data collaborative members should be able to request additional data if required, and approval will be subject to the data owners.
4. **Risk-based approach:** Data owners are responsible for identifying, assessing, evaluating, and mitigating risks involved, prior to, and during the sharing of data. Risks include compliance, strategic, operational, market, and financial risks. (ISO 31000)
5. **Compliance by default:** The use of data must be compliant with all relevant regulatory requirements.
6. **Address the FUD:** In cases where the data collaborative is impeded by Fear, Uncertainty, Doubt (FUD) in relation to the existing regulatory environment, the regulatory framework should support a regulatory sandbox providing collaborators with a space to test technology and policies, while remaining in adherence to the other data collaborative principles.

Based on The Open Data Inventory (ODIN) 2020/21, Malaysia ranks 78th out of 187 countries. ODIN assesses the coverage and openness of official statistics to identify gaps, promote open data policies, improve access, and encourage dialogue between national statistical offices (NSOs) and data users.

Improved data openness will unlock the value within data, enabling action and decisions to be made in an analytical and predictive manner. Open data can be a powerful force for public accountability, making information more accessible, and allowing for greater public scrutiny.

3.6 Selecting a Trusted Cloud Service Provider for Storing and Processing Data

As data owners, governments may want to ask the following questions when selecting a cloud service provider (CSP):

Where is the data stored? (Which region, country, and data center)

What does the CSP do with customer data?

How does the CSP protect the data?

How does the data owner have control over the data?

Does the CSP publish/make publicly available law enforcement access requests for data stored in its cloud?

3.7 Law Enforcement Access

Another often cited reason for data localisation is the concern that law enforcement will not have access to data stored abroad. To fight crime and protect public safety, governments have a clear and compelling interest in protecting the safety, security, and privacy of individuals and organizations that use global cloud services. Balancing that interest against citizens' expectation of due process, internationally-recognized rule of law, and human rights standards is essential to maintaining trust in technology.

Regulators around the world are developing new legal frameworks and principles for trusted government access to data held or processed by cloud service providers (CSPs). For example, conventional search and seizure rules do not apply to cloud computing, e.g., removing a server from a hyper-scale cloud data centre would not enable access to the information in the server, as data is encrypted both at rest and in transit.

This makes it a critical priority to craft modern laws that provide law enforcement and national security agencies with clear and transparent legal mechanisms to access digital information pursuant to lawful process. These laws should protect citizens' fundamental privacy rights, hold law enforcement accountable, and respect the sovereignty of other nations.

As the global data economy grows, a principled rules-based approach to law enforcement access would enhance legal certainty and increase investment opportunities, allowing countries to become data center hubs or innovation testbeds.

3.8 Trusted Cloud Principles: a global rules-based approach to privacy and security

To fight crime and protect public safety, governments have a clear and compelling need to access digital data. Balancing that interest against citizens' expectation of due process and the rule of law is essential to maintaining trust in technology. Regulators around the world are developing new legal frameworks and principles for trusted government access to data held or processed by cloud service providers (CSPs).

Some of the world's largest technology companies, including Amazon, Google, Microsoft, IBM, Salesforce, Slack, SAP, and Cisco have joined forces to establish the Trusted Cloud Principles as part of their commitment to work with governments to ensure the free flow of data, promote public safety, and protect privacy and data security in the cloud.

Anchored on the following principles, the Trusted Cloud Initiative seeks to partner with governments around the world to resolve international conflicts of law that impede innovation, security, and privacy, and to establish and ensure basic protections for organizations and businesses that store and process data in the cloud:

- Governments should engage data owners first, with only narrow exceptions. Governments should seek data directly from business or enterprise customers rather than cloud service providers, other than in exceptional circumstances.

- Customers should have a right to notice. Where governments seek to access business or enterprise data directly from cloud service providers, customers of those cloud service providers should have a right to advance notice of government access to their data, which only can be delayed in exceptional circumstances.

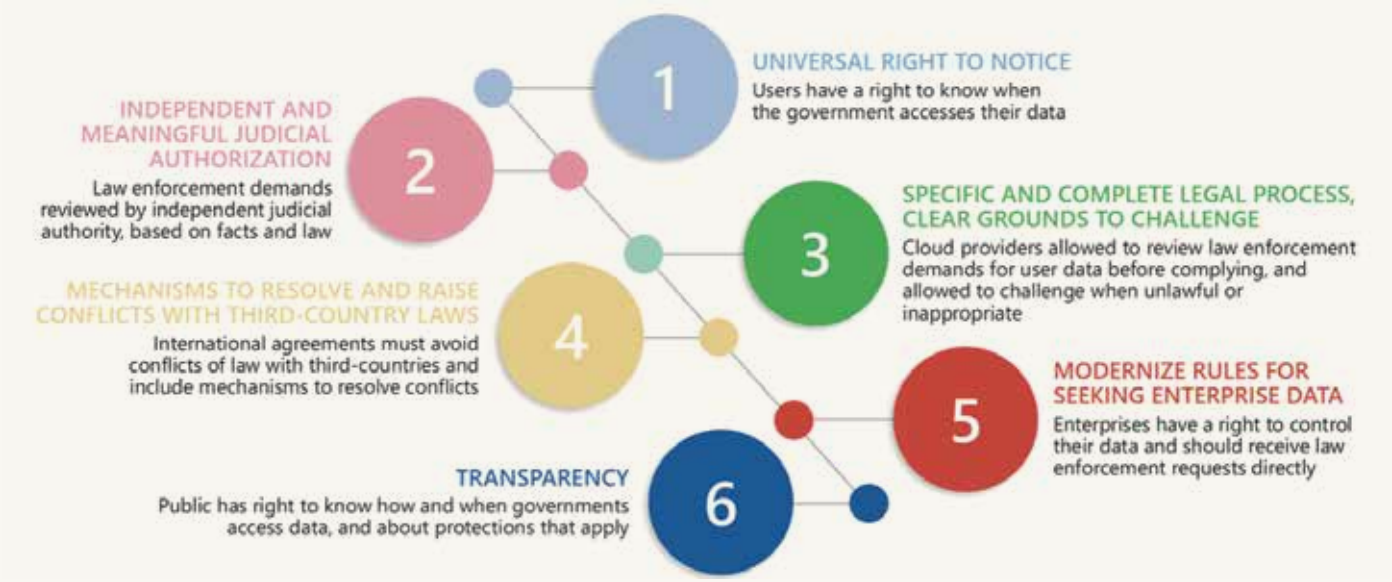
- Cloud service providers should have a right to protect their customers' interests. There should be a clear process for cloud service providers to challenge government access requests for their customers' data, including notifying relevant data protection authorities.

- Governments should address conflicts of law. Governments should create mechanisms to raise and resolve conflicts with each other such that cloud service providers' legal compliance in one country does not amount to a violation of law in another.

- Governments should support the cross-border flow of data as an engine of innovation, efficiency, and security, and avoid data residency requirements.

As Malaysia continues to develop its digital economy, this paper proposes the following framework for Law Enforcement Access to Data stored in the cloud:

Principles for Government Law Enforcement Access to Data



Government requests to access private sector data must be facilitated by a regulatory framework that respects ownership of data and due process while also addressing public safety needs.

Regulatory clarity and a common approach will not only increase investor confidence, but overall public trust in technology. Similar to the European Union, ASEAN has an opportunity to develop a unified approach, in line with the goals of Digital ASEAN and the ASEAN Digital Masterplan 2025.

3.9 Policy Recommendations

- **Increase effective use of technology, powered by hyperscale public cloud.**[35] Emerging technologies require high-speed internet and vast amounts of data and computing power. Hyperscale public cloud would provide the necessary computing power while also allowing for 'anytime anywhere' access, address the need for backups, and ensure compliance with global privacy and security standards.

- **Open Data platform to eliminate data silos,** enable a single view of the citizen and/or customer, and allow access to date for research and innovation:
  - With the ability to better connect data across an organization, governments and businesses can more easily use artificial intelligence and advanced analytics for real-time insights, leveraging critical data to increase efficiency across the organization.
  - In organizations working on critical national developmental areas, anonymized data should be made publicly available, for research and innovation.

- **Democratization of access to technology:** Expand access in rural and remote areas to connect everyone, leveraging new technologies such as TV White Spaces. This will ensure emerging technologies are democratized and its benefits are shared evenly, reducing the risk of the Fourth Industrial Revolution being perceived as 'elitist'.

- All new trade routes are digital. **Enable cross-border data flow** to promote competitiveness, international trade, and economic growth.

- **Enhance legal certainty** by ensuring that laws and policies around law enforcement access to data are substantially in line with the Trusted Cloud Principles.

- **Develop a policy and industry hub on emerging technologies.** This would bring together industry case studies, best practice policies, and serve as a platform for collaboration between private sector, public sector, academia, and civil society. This collaboration should also build upon existing principles of responsible technology already adopted by many countries in the region and hub members could offer knowledge sharing on how these principles can be translated into practice. Building trust in technology is instrumental to deliver the benefits of digitalisation widely across sectors and communities.

- **Accelerate skills development for all segments of society.** Developing a global digital workforce will depend on an inclusive and accessible talent ecosystem. Skills and talent development fit for the digital era, anchored on reskilling, upskilling life-long learning. For instance, although the national budget provides allocations for software and hardware procurement, we must also include technology budget line items for data cleaning, data organisation, and skills development.

[35] *The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. They may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume.*