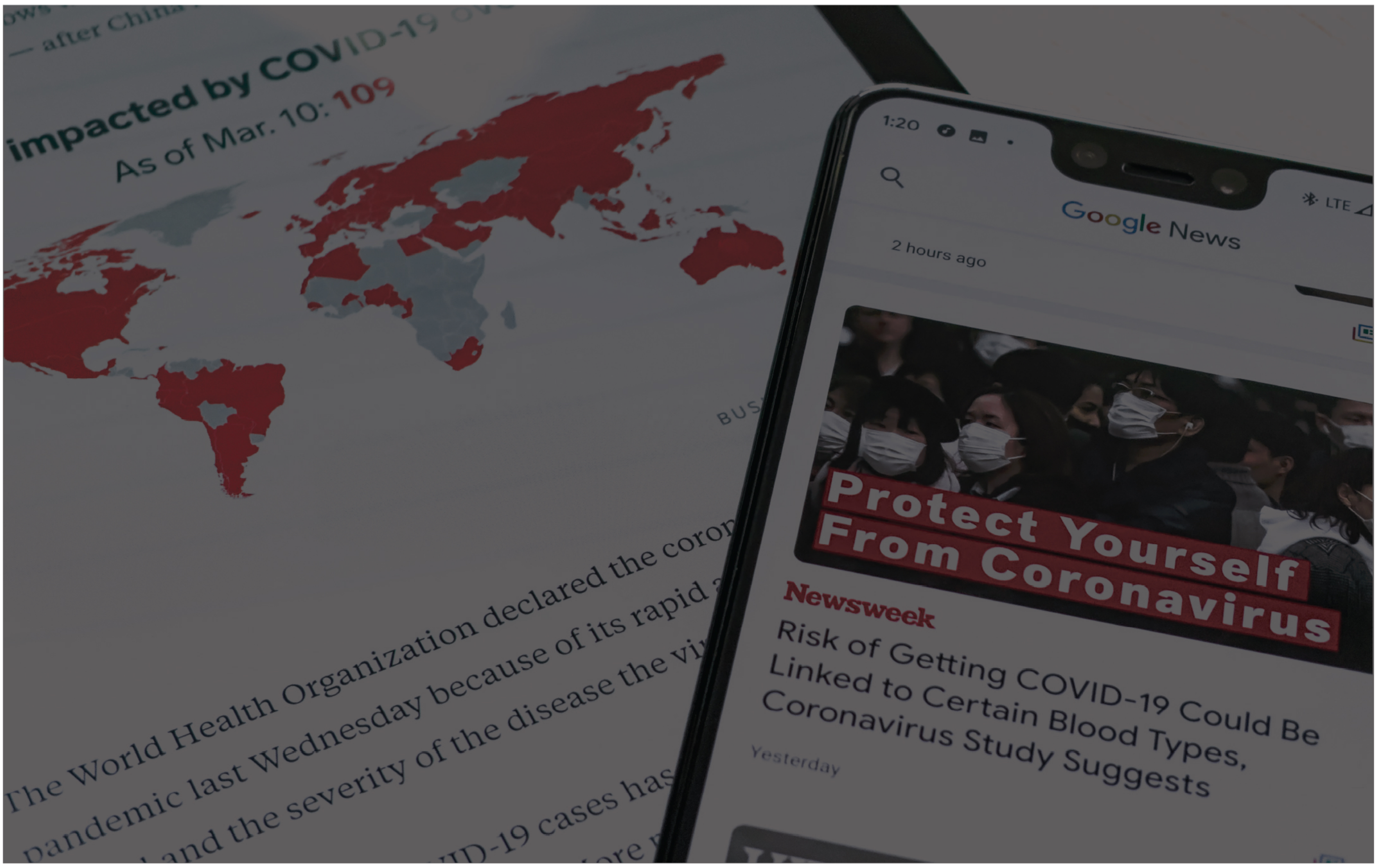
SERI
SOCIAL & ECONOMIC
RESEARCH INITIATIVE

From Digital First to Digital Native

COVID-19 EXIT STRATEGY TO THE NEW (NOW) NORMAL

Digital Infrastructure : a digital native policy paradigm; anchored on technology, powered by trust.

Nabila Hussain
October 2020
www.seri.my


impacted by COVID-19
As of Mar. 10: 109
The World Health Organization declared the coron
pandemic last Wednesday because of its rapid
and the severity of the disease the vi
1:20
Google News
2 hours ago
Protect Yourself From Coronavirus
Newsweek
Risk of Getting COVID-19 Could Be Linked to Certain Blood Types, Coronavirus Study Suggests
Yesterday

A Policy Imperative for Social and Economic Resilience

The COVID-19 pandemic has created an extraordinary health and economic crisis for countries around the world. As digital technology and data have become indispensable tools for governments to combat the virus, digital support has become critical for the world's first responders. As we have seen in the past months, digital infrastructure (mobile networks, broadband, TV whitespace[1] and cloud computing) has become one of the foremost essential services to ensure continuity of business, education, healthcare, and citizen services.

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[2] 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 in policymaking as technology moves forward.

[1] *TV Whitespace is a communications technology that simplifies the use of unutilized (licensed or un-licensed) TV and radio bands to provide wireless broadband services to unserved areas cost-effectively. This has worked well in rural areas, but has not been implemented in Malaysia.*

[2] *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.*

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 national digital infrastructure are evenly shared, and that challenges facing society are identified early and practical solutions applied.

A trusted, responsible, and inclusive digital strategy will form the foundation necessary to meaningfully unlock potential, build resilience, and develop the digital economy. There is much to be done at local, national, and regional levels, and the journey is just beginning, as we strive to amplify human ingenuity and create economic opportunities in the new normal.

Digital Infrastructure : *A Digital-Native Policy Paradigm – Anchored on technology, powered by trust*

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.

> **" Digital Infrastructure "**
> **The system connecting people to digital information, products, and services.**

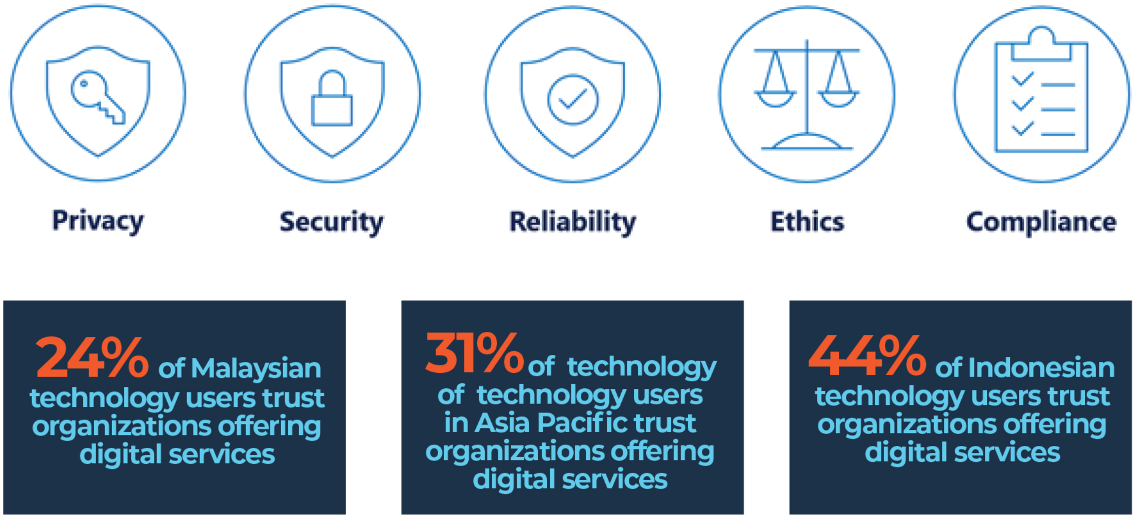
Although cost considerations may have diminished with technological advancements, the question of trust remains. Around the world, governments and business face an increasing trust deficit, particularly where technology is involved.

A 2019 study from IDC Asia-Pacific, Understanding Consumer Trust in Digital Services in Asia Pacific[3] 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.

[3] *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.*

Digital Infrastructure powered by Trust



24% of Malaysian technology users trust organizations offering digital services

31% of technology 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)

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.

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 in:

- Unlocking potential within data estates
- Regulatory reform towards a competitive and resilient digital infrastructure for all

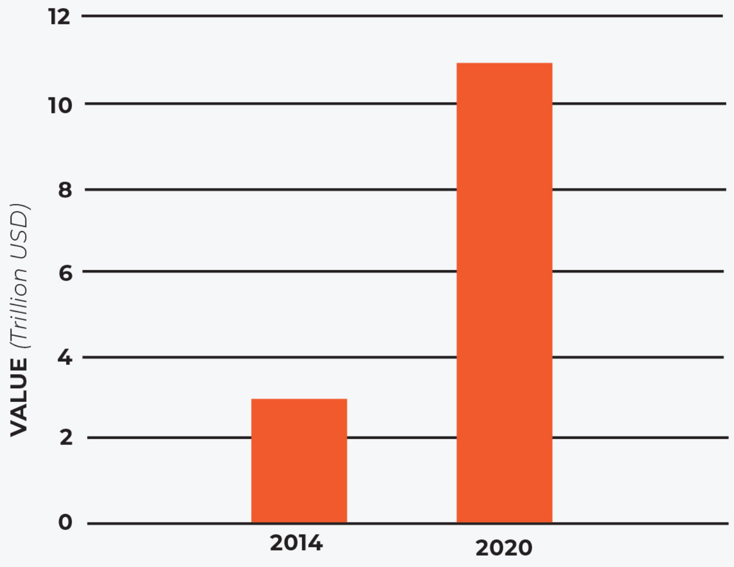
Digital : *an engine for global growth, fuelled by Data*

It has taken less than two decades for the internet to go from the computer science laboratory to the engine of global economic growth. Data is the oil of this engine, and similar to conventional fuel, it is only valuable once refined. Unlike fuel, data is not finite[4]. The use of data does not diminish the data or the value attached thereto. Data is not a finite resource and fuels innovation from product cycles to preventing outbreaks.

" Data estate "
The infrastructure or framework which allows organizations to manage all their data. Within 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.

Based on World Economic Forum data, 2014 and 2020 have seen 2.8 trillion USD and 11 trillion USD in global information flow, respectively.



$ 2.8 trillion
in information flow
of data in **2014**

$ 11 trillion
in information flow
of data in **2020**

Figure 2: Global information flows of data (World Economic Forum, 2020)

Data is the differentiator for governments and businesses seeking to reap the benefits of today's digital economy. It 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.

[4] *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)*

[5] *https://www.weforum.org/events/world-economic-forum-annual-meeting-2020/sessions/building-trust-in-data-flows*

Questions to ask[6]:

- **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?**

The Digital Infrastructure Potential for ASEAN

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[7], 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. ASEAN member countries rank from top to 160th on the global Digital Adoption Index (DAI) published[8] by the World Bank[9].

The Asean Digital Divide

There is a big gap in internet and fixed broadband (FB) penetration.
FB is prohobitively expensive in many countries.

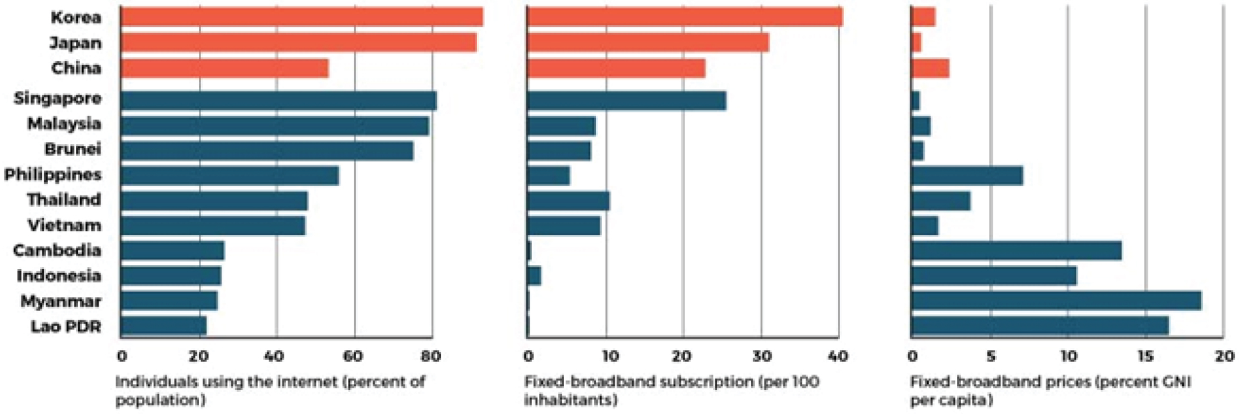


Figure 3: The ASEAN Digital Divide (International Telecommunications Union and World Bank, 2019)[10]

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).

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

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

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

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

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

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[11]. 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.

Digital ASEAN

Regional economic resilience can be bolstered by developing a genuine single market with free flow of data. ASEAN has 669 million citizens[12] 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.[13] 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.

But many significant roadblocks stand in the way of realizing this 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.[14]

Learnings from the European Union

If effectively implemented, the ASEAN Economic Community will allow for free movement of goods, services, and investment, but falls short of enabling the free movement of data. The European Union (EU), the world's largest economic bloc, in comparison, 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%)[15], the European Union offers some learnings and ways forward in the development of a coherent regional data economy for South East Asia.

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

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

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

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

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

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[16], the GDPR regulates the processing of personal data relating to individuals in the EU, by an individual, a company or an organization[17]. The GDPR has been hailed as the gold standard for personal data privacy, and has resulted in three main outcomes: legal certainty, providing citizens with more control over their data, and providing businesses across Europe with a level playing field.

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[18]. 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.

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[19], while the non-personal data will be covered by the regulation on free flow of data[20]. 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.[21] 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.[22]

The Cost of Data Localisation

With data being widely accepted as fuel 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 localization.

Data localisation refers to measures restricting data flows and can take several forms. From least restrictive to most restrictive, these measures include[23]:

> **“ Data localization ”**
> **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.**

- **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 localisation is a costly response to what is perceived to be loss of digital sovereignty. Data localisation requirements set digital economy back, 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.

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

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

[19] *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*

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

[21] *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/*

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

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

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[24]: 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.[25] 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.

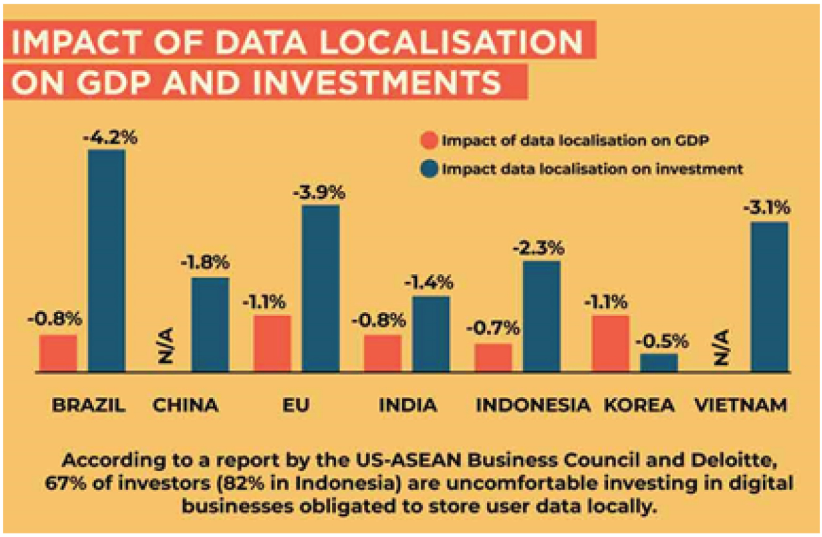


Figure 4: Impact of Data Localisation on GDP and Investments (ASEAN Post, 2019)[26]

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.[27]

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 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.

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

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

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

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

Determining What Data Lives in the Cloud

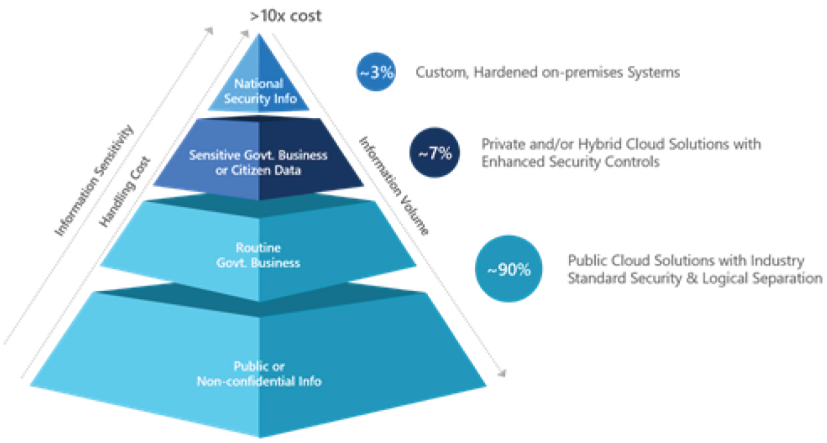

>10x cost
National Security Info
Sensitive Govt. Business or Citizen Data
Routine Govt. Business
Public or Non-confidential Info
Information Sensitivity
Handling Cost
Information Volume
~3%
Custom, Hardened on-premises Systems
~7%
Private and/or Hybrid Cloud Solutions with Enhanced Security Controls
~90%
Public Cloud Solutions with Industry Standard Security & Logical Separation

Figure 5: Determining What Data Lives in the Cloud

Figure 5 brings together many of the variables that governments typically consider in the context of classifying data in anticipation of moving to the cloud.

It is intended to convey rough relative values, and while this may differ from country to country, here are some interesting trends:

“ 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.

- **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.**
- **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[28] much that security might cost.**
- **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 costs savings.**

As data owners, businesses and 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?

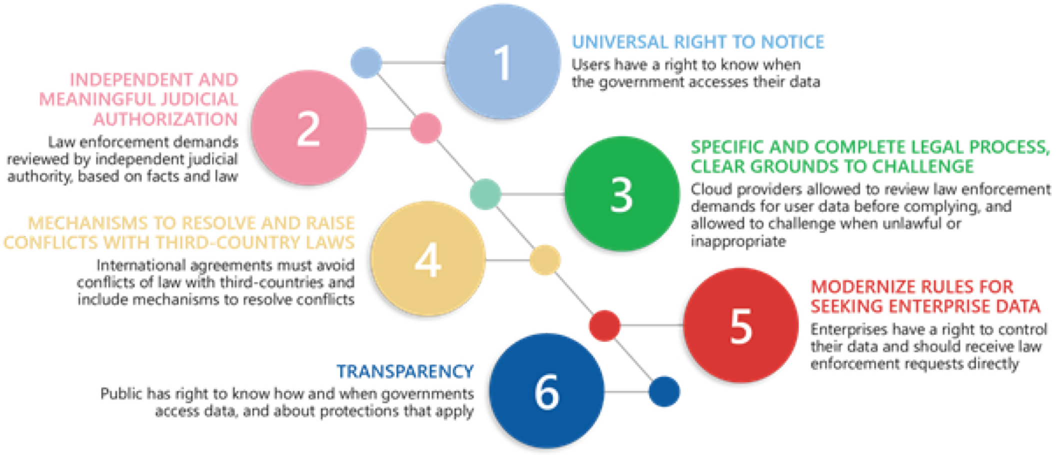
[28] *Cloud resources (e.g. servers and storage) are delivered over the Internet for the data owner, by a third-party cloud service provider. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud service provider.*

Law Enforcement Access

Another often cited reason for data localisation is the concern that law enforcement will not have access to data stored abroad. Regulators should note that conventional search and seizure rules do not apply to cloud computing. Removing a server from a data center would not equate to having access to data as the data stored on servers are encrypted both at rest and in transit.

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. 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



1 UNIVERSAL RIGHT TO NOTICE
Users have a right to know when the government accesses their data

2 INDEPENDENT AND MEANINGFUL JUDICIAL AUTHORIZATION
Law enforcement demands reviewed by independent judicial authority, based on facts and law

3 SPECIFIC AND COMPLETE LEGAL PROCESS, CLEAR GROUNDS TO CHALLENGE
Cloud providers allowed to review law enforcement demands for user data before complying, and allowed to challenge when unlawful or inappropriate

4 MECHANISMS TO RESOLVE AND RAISE CONFLICTS WITH THIRD-COUNTRY LAWS
International agreements must avoid conflicts of law with third-countries and include mechanisms to resolve conflicts

5 MODERNIZE RULES FOR SEEKING ENTERPRISE DATA
Enterprises have a right to control their data and should receive law enforcement requests directly

6 TRANSPARENCY
Public has right to know how and when governments access data, and about protections that apply

Allowing the free movement of data would open Malaysia up to a market of 669 million people, compared to its population of 32 million. A digital single market would allow entities to be regional from their inception, and digital by default. Malaysians would be able to provide digital goods and services to ASEAN and the world, not limited by geographical physical borders.

Malaysia has the opportunity to demonstrate leadership and become a regional datacentre hub, especially if it is able to introduce a legislation that will ensure businesses, enterprises, and regional governments that data hosted in Malaysia is safe and all access requests have to be made to the data owners and not the cloud service providers (CSPs), as CSPs are merely the data processors and not owners. The follow-on effect is also the opportunity to encourage the thriving start-up community to select Malaysia as their headquarters.

Policy Recommendations

- **Increase effective use of technology, powered by hyperscale public cloud.**[29]
  This would allow 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 and enable a single view of the citizen and/or customer:**
  - 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.

[29] *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.*

- **Democratization of access to technology.**
  Expand access in rural and remote areas to connect everyone, leveraging new technologies such as TV White Space.
- **Promote competition and remove barriers to investment to boost connectivity.**
  Telekom Malaysia controls 92% of fixed broadband subscriptions, making the Malaysian market more concentrated than that of other ASEAN or OECD countries.[30]
- All new trade routes are digital. **Enable cross-border data flow** to promote competitiveness, international trade, and economic growth.
- **Enhance legal certainty** by implementing a rules-based principled approach governing law enforcement access to data.

Conclusion

Malaysia has done well in the region, and globally, taking quick and effective action to stem the spread of COVID-19, but there remains much work to be done in unlocking the potential of data estates, enabling digital infrastructure, and bridging the opportunity divide. Resilient digital infrastructure must be coupled with stable water and electricity supply to enable economic and societal growth as we rebuild Malaysia. While the balancing act between saving lives and livelihoods has certainly been challenging to navigate, policymakers and regulators have demonstrated the ability to be innovative, decisive, and forward-looking; traits which will serve us well as we continue the journey towards creating a resilient digital infrastructure for improved societal and economic outcomes in post-pandemic Malaysia. Malaysia has the opportunity to lead change for the region in cohesive policy-making that addresses cross-cutting issues with leading-edge technology, providing solutions to not only exit the pandemic, but also recover, build resilience, and increase competitiveness.

[30] *https://www.worldbank.org/en/country/malaysia/publication/malaysias-digital-economy-a-new-driver-of-development*