Position Paper on Cross-Border Data Flow and Data Localization

We would like to express the private sector's concerns and strong opposition if there is a draft Executive Order proposing a data localization mandate in the Philippines. The country is progressing towards becoming a digital economy heavyweight in the region, with digital trade underpinning the growth of the digital economy. However, any shift away from the current open and enabling data policy regime, such as through regulation that will impose data localization requirements and impede data flows, could significantly alter this course.

Furthermore, if any proposed data localization or data residency mandate is put forward, this will stand directly at odds with the Philippines' international trade commitments, the government's policy approach of allowing data to flow across borders, and fundamentally impede the growth of the digital economy by hindering the ability of companies to offer cross-border services and discouraging investments into the local digital ecosystem.

Any proposal to issue such a mandate will require a deliberate, transparent, and consultative approach given the multitude of stakeholders – including, among others, aviation, cloud computing, cross-border e-payments, financial services, health services, and IT-BPM sectors – that will be affected and the potential negative consequences it could have on the country's digital economy ambitions.

Below are our general points on the imposition of a data localization mandate as well as comments on the rationale, scope, covered data, and data residency requirements in the supposed draft EO.

GENERAL POINTS

Data localization and restrictions on cross border data flows have a significant impact on overall economic activity. Data is the foundation of the modern digital economy and is a core input across all sectors. According to the OECD, the following types of data would be affected the most by restrictive policies: personal data (16%), business records (15%), financial (14%), public sector (12%), and telecommunications data (11%)[1].

Data localization will significantly increase costs for businesses operating in the Philippines, cause unnecessary disruption to business operations, and directly and negatively impact the competitiveness of the Philippine business sector. Data localization creates barriers for innovative products and services to enter the Philippines, hampering growth opportunities for the Philippine start-up ecosystem. Moreover, studies have shown that SMEs, start-ups, and gig-workers will suffer the biggest negative impacts of data localization.

---

[1] Ferencz, Janos. "The nature, evolution and potential implications of data localization measures". Presentation at the *Arangkada* Philippines Policy Discussion on Managing Cross-Border Data Flows: Regional/Global Experiences and Good Practices, virtual, August 16, 2023. https://www.arangkadaphilippines.com/video-arangkada-philippines-policy-discussion-on-managing-cross-border-data-flows-august-16-2023/

Consequently, data localization poses a hindrance in complying with international agreements that seek to promote the growth of the international digital economy. Localization constraints can also deter innovation and hurt local economies by limiting which services are available to them, or increase costs given there is a smaller number of service providers from which to choose.

Data localization measures would require re-evaluating and restructuring of global transactions. Such measures would limit the full trade benefits between firms, among firms, and agreements at the industry level. The imposition of data localization would severely affect transactions that occur across countries in the Asia Pacific region and beyond. Businesses including business process outsourcing (BPO) transactions will be affected by changes in policies. Moreover, small and medium business, including start-ups will not be able to comply with such mandate given the digital nature of their business, as well as the additional cost of complying with data residency mandates.

Data localization would impede the full benefits of cross-border flows. For instance, the ASEAN economic community allows for the free flow of services, goods, and skilled labor. Imposing data localization would hinder the leverage from the sectors previously mentioned. Aside from this, data localization would hinder the full use of Internet of Things applications (IoT) and Artificial Intelligence (AI), which are mostly processed offshore.

Data localization requirements create high barriers for both local and global providers of companies willing to expand business either domestically or internationally. The repercussions of data localization are especially felt by the financial and digital payment companies. The OECD's e-payment case study helps illustrate said impact[2].

Data localization would lead to fragmented markets. A cloud computing case study from the OECD revealed that smaller markets would tend to lose from data localization measures since higher costs for firms to enact facilities and securities[3]. In other words, market fragmentation across borders would undermine services offered to consumers. This would affect consumers in a smaller market.

A policy of mandating storage of consumer and business data within specific cloud containers risks decreasing consumer trust and confidence and negatively impacting the effectiveness of organizations' current privacy and security protocols. For certain industries such as the financial and payments industries, effective fraud tools are built on centralized global datasets, accuracy in detecting and preventing fraud increases in tandem with larger pools of data for fraud scoring. As such, data localization may lead to higher incidence of fraud incidents, resulting in higher financial losses to financial institutions and consumers. Such an outcome is also detrimental to the building of digital trust in the financial services sector.

Data localization will increase the cost of remitting money. Free data flows across borders is critical to ensuring the safe and secure provision of remittance services. Data localization requirements can directly increase the cost of remittances, formalize remittance flows, and empower Overseas Filipino Workers (OFW) who have supported the Philippines economy. OFW remittances in 2022 reached $32.54 billion or 9% of the country's gross

[2] *Ibid.*
[3] *Ibid.*

domestic product in 2022. GSMA, a group of mobile operators worldwide, published a report on the impact of data localization on mobile-money enabled remittances that confirm the same assertions[4].

The global slowdown is already expected to hurt remittance growth in the Philippines, according to the World Bank. In fact, in 2022, remittance only contributed 2.24% of the Philippine GDP, a big dip from 9.31% in 2020 and 9.64% in 2019 (The Global Economy). Behind these statistics are OFWs and their families.

Complying with a data localization mandate would mean creating new infrastructures, processes, resources, and systems which would snowball to increase overall operational overheads. This will eventually result in increased cost of remittance, at the expense of the OFWs and their families. Complying may not even be an option for international remittance or payment companies. For some, this requirement may be too costly, burdensome, and inconsistent with global trend that they may just opt to stop operating in the Philippines. This will further limit the access of Filipinos.

Data localization contradicts the Philippines commitments on international trade. The Philippines is a party to the Regional Comprehensive Economic Partnership Agreement, which contains a binding commitment that *"no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory."* Moreover, the Philippines has played a key role in championing cross-border data flow amid ongoing negotiations on the Indo-Pacific Economic Framework for Prosperity and ASEAN Digital Economy Framework Agreement (DEFA). The data localization proposal is a step backwards to the progressive digital policy that the Philippines has represented in these international trade negotiations.

Comparison with other Asia Pacific (APAC) jurisdictions:

- Data localization laws are not common in APAC given the position various countries in APAC have as commercial hubs with respect to world markets.
- Currently, China and Vietnam are two APAC countries with data localization laws pertaining to personal information. However, it is noteworthy that the Chinese law has a high threshold before data localization kicks in – mainly, information that is critical in nature – important data and national data. Even then, cross-border transfers are still permitted provided certain conditions are met. Similarly, the Vietnam cybersecurity legislation imposes data localization requirements under exceptional circumstances.
- It is also pertinent to note that the draft data privacy legislation for India had data localization requirements which have since been scrapped by virtue of a law – Digital Personal Data Protection Act 2023.

[4] GSMA. *The impact of data localisation requirements on the growth of mobile money-enabled remittances*. March 2019. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf

COMMENTS ON THE DRAFT EXECUTIVE ORDER

RATIONALE/ PURPOSE

1. **Ensure that personal information in ICT systems in the government and private sector are secured and protected.**

In a world where cyberthreats are dynamic, sophisticated, and driven by well-resourced threat actors, the cost, complexity and effort for data continues to increase. **Few organizations will have the expertise and the resources to keep abreast with this constantly evolving and challenging threat landscape.** With most systems in this digital world connected to the internet, data localization can reduce security, increase cost and complexity, as well as restrict innovation.

Fortunately, the hyper-scale cloud services around the world have not only democratized advanced computing services that enable digital transformation, but also security and compliance. The shared responsibility model means that the cloud service customer can off-load the security of the cloud to experts, and secure infrastructure provided by the cloud service provider. The security and privacy controls are based on global international standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 as well as industry standards such as SOC, PCI-DSS and others. Cloud service customers are assured that these controls are implemented by third-party audits and certifications.

Further, to assist cloud service customers to meet their responsibility in addressing cyberthreats and protecting confidential or sensitive data, the hyper-scale cloud service providers offer an extensive collection of security functionality. For example, cloud service providers (CSPs) have more than 300 security, compliance and governance services and features that can be readily configured to implement advanced security measures cost-effectively.

The security capabilities of cloud provide the ability for customers to take advantage of the best, most up-to-date technology while maintaining full control over their data with regard to the physical location of where it is stored. Hyperscale CSPs implement rigorous contractual, technical, and organizational measures to protect the confidentiality, integrity, and availability of customer data regardless of which location a customer selects.

Advanced security measures to counter the sophisticated cybersecurity challenges faced in this digital world are now within the reach of all entities in the Philippines, large or small, through hyper-scale cloud services. However, the economics and capabilities of these hyper-scale clouds are derived from global scale and distribution, where the actual data center may not be located within the geographical boundaries of a country.

Restricting the use of these global infrastructure by having data residency requirements will not only hinder business and digital transformation initiatives but may also weaken the security and privacy posture of organizations that cannot afford implementing on-shore secure infrastructure to resist the sophisticated cyber-attackers of today. The small to medium size entities will be most adversely affected by this.

Finally, unless the system is not connected to the internet, the mandated data localization controls will not enhance the security and privacy of data in any way.

The protection of personal information in any ICT systems, is dependent on the security protections that are in place. Government and private sector entities will have to invest and implement strong security mechanisms that involve people, process, and technology. With regulations that prohibit the use of off-shore hyper-scale cloud, implementing these advanced features in on-premises solutions, private cloud or limited-scale public infrastructure increase the cost and complexity of protecting personal information. The complexity of operations will typically deprioritize the efforts needed to address the people and process requirements in personal information protection.

2. Ensure the rights of individuals to privacy and confidentiality of their personal information.

Using hyper-scale cloud services, irrespective of the location of the infrastructure, will not hinder the cloud service users from meeting their privacy and confidentiality obligations of their, or their customers' information. "Out-of-the-box", privacy assurance of the cloud is provided through third party audit reports and certifications based on globally recognized standards. Examples such as compliance with ISO/IEC 27018 (Code of practice for PII in public clouds) and ISO/IEC 27701 (Privacy Information Management) as well as HIPPA and GDPR compliance.

Global hyper-scale cloud providers offer more than 300 security and compliance features that will enable cloud service users to readily configure their deployment to ensure the rights of individuals to privacy and confidentiality are met. Data localization requires these security capabilities to be acquired, deployed and managed in on-premise or local private cloud which could be prohibitive for many organizations.

Hyperscale cloud service providers have advanced encryption and key management services that customers can use to protect their content. We have industry leading encryption services that give our customers a range of options to encrypt data in-transit and at rest, and to manage encryption/decryption.

Furthermore, existing laws such as the Data Privacy Act already provide for holding the local counterpart of a multinational corporation accountable for data privacy violations even if the data has been processed overseas. The Data Privacy Act is a principles-based law that allows organizations to implement privacy protections in an adaptable way that accounts for actual risks. It is a technology- and business sector-neutral approach that allows organizations to implement common-sense business practices to comply with the law's requirements. The Philippines' National Privacy Commission (NPC) has in turn carefully and adequately balanced privacy rights and business needs with interoperability in ASEAN and privacy laws around the world. The Act is impactful— with significant penalties and the NPC as an active enforcer of privacy rights. Moreover, NPC affirmed its support for cross-border data flow in a public webinar organized by the Department of ICT in July 2023 on the subject of personal data protection in the context of cross-border data flow.

3. Ensure the security of critical ICT infrastructure, including information assets of the government, individuals, and businesses.

Protection of critical ICT infrastructure is important for the country as well as business. As such, it is

important that these are highly secure and resilient. For example, in the Financial Services Industry (FSI) sector, the catastrophic failure of a data center (DC) of a significant FSI entity will not only impact the company, but the country as a whole. Implementing a Disaster Recovery Plan (DRP) that includes investing in backup DC that is typically idle is not only costly, but wasteful.

Local data storage does not equal improved data security. Information is typically distributed among multiple systems rather than stored in a single location, not to mention the significant investments that these companies make in their cybersecurity capabilities. When it comes to data security, investment in infrastructure and maintenance is more critical than the physical location of data.

A typical hyper-scale cloud is made up of "regions" or clusters of data centers located in a particular geography. Each region consists of at least three separate DCs. Further, cloud service customers are able to leverage on more than one region to enhance resilience. With this, the FSIs, large or small, can readily implement DRP, as well as advanced security features on secure and resilient underlying ICT infrastructure in an optimal way.

Hyperscale CSPs leverage insights gained from our global footprint, applying lessons learned to improve security against cyber incidents throughout our infrastructure, including at the local level. After a customer picks the geographic region or regions in which they want to store their data, cloud infrastructure provides far greater resiliency and availability than organizations can achieve using on-premises infrastructure. In the cloud, rather than concentrating risk, data can be automatically distributed among multiple servers in the same location, and customers have the option to store their data in multiple locations.

The data localization can restrict the options for implementing robust security and resilient solutions by entities that operate critical ICT infrastructure. A recent real-world example of this risk was Ukraine's decision in 2022 to change its laws to permit backing-up computer servers and data centers to offshore cloud. Soon after the conflict with Russia began, many of those server farms were destroyed. However, with cloud backups enabled, the Ukrainian government was able to continue operations.

4. Address issues related to cybercrime, data privacy, cybersecurity, confidentiality of certain types of data in the possession of government and private entities.

Government restrictions on cross-border data transfers have typically been justified by citing concerns about personal data and national security. The common misconception is that the best way to address these concerns is to store data within a country's borders. **However, the security of data is not dependent on the physical location of its storage. Instead, data transfer restrictions and data localization requirements may counterintuitively pose a risk to cybersecurity.**

Data localizations or transfer restrictions impede integrated cybersecurity planning. These restrictions force organizations to adopt a siloed approach to data, restricting the location of certain types of data but not others. This is a differentiation that complicates data without adding any corresponding benefit to security, thus unnecessarily straining the people, processes, and technologies necessary for an organization to manage its cybersecurity risk. This approach also impedes the visibility of cybersecurity

risks across jurisdictions.

Restrictions like this also weaken coordinated network defense mechanisms by impeding cross-border collaboration and information sharing. This puts malicious actors who do not respect local legal requirements at a structural advantage over service providers who do. Cyber defenders themselves will lose access to threat indicators or cybersecurity data in certain jurisdictions, making it difficult for them to address malicious activity in other jurisdictions, ultimately impeding cybersecurity resilience.

The escalation of cybercrime in this connected digital world has increased the data privacy, cybersecurity and confidentiality risks of all data that has value to the threat actors. Regardless of the location of data, strong security and privacy measures are required to address these.

For example, for a healthcare organization to protect against security incidents, there is a need to establish an incident handling process that involves preparation, detection (identification), response (containment), mitigation (eradication), reporting, recovery, remediation and lessons learnt. Each of these stages involves people, process and technology. The shared responsibility model offered by hyper-scale cloud providers will help the healthcare entities to reduce the cost and complexity to implement this incident handling process necessary to address cybercrime issues in the real world, and focus more on their major business, providing healthcare services.

Requiring all sensitive data to be stored in a country may increase the cybersecurity risk especially if government and private entities are not able to mitigate cybersecurity risks due to affordability or lack of expertise to deal with the complexity of implementing these mitigating controls in on-shore ICT systems.

SCOPE

1. All national government agencies (NGAs) and their regional and provincial offices, government-owned or -controlled corporations (GOCCs), government financial institutions (GFIs), state universities and colleges (SUCs), local government units (LGUs), and other government instrumentalities.

Governments that are highly advanced in digitalization in Asia-Pacific such as Japan, Singapore, Australia, New Zealand have taken the exact opposite approach. Conscious of the costs and institutional capacity and resources that would be required to manage all data in-house or in-country, they have all adopted effective risk-based approaches to data classification and cross border data flows, and significantly limited the types of government data that must be stored or processed locally to all but the most sensitive/secret categories.

Requiring all national and local government agencies and other public sector bodies in the Philippines to manage all data on premises and/or in-country would make heavy demands on government/public sector agency budgets and staff resources for data management. It would delay the implementation of their digitalization plans and delivery of digital services to citizens and businesses.

It is also worth noting that the current digital infrastructure in many national and local government units remains vulnerable to hacking. These vulnerabilities in the digital infrastructure need to be addressed and not by data localization, which simply increases the risks.

Further, the actual benefits to these government/public sector agencies of mandatory data localization are not apparent.

2. Cloud Service providers, intermediaries, and other private entities with transactions, contracts, or data related to, in connection with, or arising from the rendition of cloud computing services:

- **A. For the Philippine Government**
- **B. For private entities processing sensitive personal information**
- **C. Healthcare providers; and**
- **D. Private entities processing personal information declared to be confidential in nature under existing laws**

A risk-based approach should be taken in evaluating cloud services by any of these entities, rather than a fixed and restrictive rule-based approach based on data location that may have unintended and even adverse consequences to economics, agility and security.

Furthermore, the proposed scope of covered entities is unduly broad given the objectives the EO seeks to achieve. For example, sub-paragraph (ii) is very broad as it essentially would cover all private entities who are employers as these firms would be processing sensitive personal information (such as social security number, marital status, age, education). Sub-paragraph (iii) is also very broad as a subscriber's information under the Cybercrime Prevention Act 2012 would include any information contained in the form of computer data or any other form that is held by a service provider, relating to the subscribers of its services other than traffic of content data and by which identity can be established.

TYPES OF DATA INCLUDED

1. Follows government data classifications - mandates that government entities classify their data according to 4 level classification from non-sensitive, sensitive, above-sensitive, and top-secret.

Data localization requirements across a wide range of sectors and workloads will severely restrict the choice for implementing digital solutions at a time when digital transformation is a key agenda for many countries, including the Philippines.

Implementing a narrow rule-based approach based on data location may have unintended and even adverse consequences to economics, agility and security. Instead, a risk-based approach in adopting cloud services where data location is one of the risks to be considered will help balance the benefits, and risks in a pragmatic and constructive manner which is aligned to the national agenda for socio-economic progress in this digital era.

2. All sensitive personal information processed by private entities which are also classified as confidential under existing laws are included under the mandate.

The private sector has to be more cost efficient and agile to be competitive and succeed in this connected digital world. The private sector already has obligations to protect PII under the Data Privacy Act of 2012, and to achieve this, they are already required to implement strong security and privacy measures. **Being heavily reliant on the internet to drive their business, the mandate for localization of data for the private sector does not bring additional protection to the security and privacy of data because cyber-attacks are location agnostic.**

For example, a web storefront for a small business based in the Philippines hosted in Singapore will face the same cyber-attack risk as a web site hosted in the Philippines. However, if the small business can readily implement enhanced security offered by the hyper-scale cloud provider in Singapore, but unable to do so in the Philippines due to significant cost difference when implemented in on-premise or private cloud solutions, the latter approach will expose the company to greater risk of loss of confidentiality.

The cost benefits, agility and enhanced security offered by hyper-scale cloud infrastructure can unnecessarily disrupt and disadvantage local companies, especially to small businesses.

DATA RESIDENCY

1. Only Non-Sensitive Government Data may be stored in off-shore infrastructure

---

This is a much more restricted approach to data residency requirements under the DICT Cloud First Policy, where only above sensitive and top-secret data are required to be stored within the Philippines' jurisdiction. Because of the high-cost implications of this proposed measure, before considering such a requirement we recommend the Government to commission an audit of the implementation experience of the CF policy to determine whether there has been any actual quantifiable impact on the security of government data under the current policy.

2. The following institutions must store data locally:

a. **Core operations of *Bangko Sentral ng Pilipinas* (Central Bank) Supervised Financial Institutions deployed on private cloud.**

Cloud computing has become an essential tool. Digital transformation of the economy, and financial services in particular, relies on the efficiency of public cloud computing and free flow of data. The opportunity to leapfrog legacy systems and catch up with the digital world by accessing economies of

scale in data storage, analysis, and cyber defense has emerged as a critical solution for the modernization of banking, insurance, payments, and asset management.

When data is mandated to stay inside national borders, it must temporarily be separated from a global data pool, creating more room for errors, as well as adding additional costs and slowing services. Data localization would require underlying data architecture of financial institutions' platforms to change which causes upstream and downstream impacts to other systems that may interface. This increases the potential for errors for support teams, technologists, and the business. Furthermore, control is not scalable in this case and would result in diminished and fragmented control.

Citizens expect faster payments, easy onboarding, open banking, and effective fraud prevention. All these rely on the falling cost of storing and processing data remotely along with high- speed global networks. In the area of payments as an example, more and more countries are introducing faster or instant payment schemes to meet these expectations. Regulators have also played a role in driving competition and innovation through fintech, which in turn has transformed financial service onboarding and verification of customers to meet KYC, KYB, and AML rules. Digital services in the cloud allow remote account opening and digital identity services for consumers and businesses. Ironically, data localization regulation creates new barriers to these other regulatory initiatives and citizen benefits.

Data localization could choke innovation. Financial institutions and fintech's alike rely on public cloud services to launch. It is a democratizing technology. It offers ventures of all sizes access to global cutting-edge platforms for development and operation, the ability to set-up instantly, and uses only the capacity they currently need while retaining the ability to rapidly scale.

Global cloud service providers offer advanced tools and solutions, incorporating AI and machine learning tools to achieve results in fraud prevention. The instant free flow of data is essential for delivering these service levels while meeting customer expectations for safe, secure, instant payment in the coffee shop line or walking through mass transit turnstiles.

Data localization undermines cybersecurity in FSI. The increasing threat landscape requires increasingly sophisticated and constantly evolving defense solutions. Global public cloud service providers (CSP) and cloud based cyber security firms have delivered incredibly valuable common solutions where the economies of scale, access to scarce talent resources, and the ability to monitor global networks in real time have provided an essential solution to enterprises trying to cope and to regulatory supervisors looking for workable solutions. Data localization would undermine these solutions and weaken common global defenses while breaking a best practice of cyber defense. Storing all data within one geographical region undermines the security of data by exposing it to physical threat and targeted cyberattacks. It mandates expansion of attack surfaces which heightens cybersecurity risks for FIs.

2. The following institutions must store data locally:

b. Health information systems of health service providers and insurers.

The *Benefits of cloud-enabled healthcare* report, prepared by Deloitte Access Economics included a meta-analysis of 66 existing use cases of cloud technology in healthcare across nine Asia-Pacific countries: In these use cases, cloud technology was a key enabler of digital technologies such as telehealth consultations, predicting patient outcomes and augmented reality for clinician training.

The use of these technologies will be critical as health care across the Asia-Pacific faces mounting challenges, with health expenditure per capita growing 80% in the region over the past decade to 2019 and sector workers facing burnout from the intense COVID-19 period. Public and private providers are searching for new ways to deliver quality care in an accessible and cost-efficient way, including by using digital technology.

The report finds that cloud technology can deliver significant benefits for healthcare organizations, the broader healthcare system and most importantly patients, including:

- $21.6 USD billion in cost savings if all hospitals in the nine countries transitioned to cloud, which is equivalent to $5,963 USD per hospital bed.
- 20% of total healthcare costs accounted for by health inequality which can be addressed by cloud identifying key populations and increasing accessibility to healthcare.
- 7.6% increase in diagnostic accuracy for cardiovascular diseases (one of the most prevalent chronic illnesses globally).
- 2.2 billion vaccines administered in India supported using the cloud-based platform, CoWIN.
- 1 million hours saved for manual entry for frontline COVID-19 healthcare workers in New South Wales, Australia in 2021.

The increase in costs incurred by private health service providers and insurers to host their systems in the Philippines would likely also be passed down to end customers, thereby making healthcare less affordable for the people.

Reference: Benefits of Cloud-Enabled Healthcare in Asia Pacific[5]

Cloud services enable data to be used faster and shared more readily across borders. **Healthcare authorities and policymakers should carefully balance the benefits of cross-border data sharing for greater access to medical services against security and localization requirements.** Requiring data to be hosted and processed locally can result in loss of certain cloud benefits, including the ability to scale quickly and dynamically, provide high levels of service, and cost-effectiveness. Strict localization may also impair both business and government continuity plans, resulting in critical government functions and institutions not being able to operate during a national emergency, such as war or major natural

[5] https://d1.awsstatic.com/institute/Deloitte-Access-Economics-AWSI-Benefits-of-cloud-enabled-healthcare-in-Asia-Pacific-2023.pdf

disasters. Data localization also may stifle innovation and research opportunities due to the requirement to have infrastructure located onshore and increase overall infrastructure costs.

Principles:

a. Avoid implementing broad data residency requirements to healthcare data that restrict access to healthcare services and technology. At an international level, there are multiple valid and effective ways to establish security and control over data.
b. Alternatives include allowing public sector data to be located offshore, subject to certain requirements, or "whitelisting" countries that provide a sufficient degree of protection for that data.
c. Consider utilizing privacy enhancing technologies to de-identify data and reduce risks arising from transfers. Certain privacy enhancing technologies allow data analytics to be carried out on the data without requiring data sharing or data leaving the environment.
d. Make requirements accountability-based rather than jurisdiction-based to promote free-flow of data across borders. This will ensure that the data owner is responsible for meeting requirements, regardless of where the data is physically stored.

Reference: Health Data Governance[6]

The restriction of health data with local cloud deployment will hinder the access of innovative healthcare solution for the Philippines population, preventing the effective deployment of latest development in AI, precision medicine, digital health/digital therapeutic solution, genomic and immunotherapy for critical illness like cancer treatment, rare disease and chronic disease management, and emergency collaboration for global pandemic readiness, clinical research, and innovation. This will prevent the Philippines from accessing the latest technology and advance the digital economy, with limited market access globally.

2. The following institutions must store data locally:

c. Subscriber information of service providers located in the Philippines;

While subscriber information may be considered as "Sensitive Data", a mandate to reside on-shore does not enhance the security and privacy protection unless the system is air-gapped (not connected to the internet) or there is an unacceptable level of jurisdictional risk associated with the location of the data.

Service providers operating in the Philippines should already protect subscriber data with strong security and privacy mechanisms. Subscriber data typically contain PII and hence the need to comply with the requirements of the Data Privacy Act 2012.

[6] https://d1.awsstatic.com/institute/Health-Data-Governance.pdf?did=psr_card&trk=psr_card

Service providers, such as telecommunications operators, cannot control cross-border data transfer. For example, if a Philippines mobile phone customer roams to another country, for roaming to work, data about the customer will need to flow out to another country for the service to work.

Data localization requirements for subscriber information may inadvertently introduce unforeseen challenges for service providers to operate, without enhancing data security.

3. All sensitive personal information processed by private entities which are also classified as confidential under existing laws

---

Most private entities today would have in place security and privacy mechanisms to comply with privacy requirements of the Philippines as well as others such as GDPR which demands a high bar protecting the security and privacy of data associated with EU data subjects.

Mandating private entities to have PII the process to reside in the country may require major changes that will involve people, process, and technology. For example, if a local company uses a cloud-based software-as-a-service ERP solution that suits their existing business processes, having to move the system in-country will highly likely require them to change this core business system, which in turn forces significant business process re-engineering.

Private entities may have to suffer major business disruption and prohibitive operational costs, impacting smaller players at a disproportionate scale, without improving the security posture in protecting the PII.

Furthermore, the imposition of data localization as a prescriptive technical requirement to achieve security of “sensitive personal information which are also classified as confidential under existing laws” is a slippery slope and is not in-line with the general trend of omnibus data privacy frameworks (GDPR and GAPP). For example, data protection laws (including the Data Privacy Act of 2012 (Republic Act No. 10173) and its implementing rules and regulations) generally leave it up to data controllers to decide and establish technical and organizational measures to ensure the appropriate level of security (see Section 25 of the IRRs of Data Privacy Act 2012) without specifying the actual technical means to achieve that goal.

APPENDIX:

Philippines Digital Trade Commitments:

Regional Comprehensive Economic Partnership Agreement – *entered into force for Philippines on 2 June 2023*

Article 12.14: Location of Computing Facilities

1. The Parties recognise that each Party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining:

   (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or

   (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

Article 12.15: Cross-border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. A Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining:

   (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or

(b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

Comprehensive and Progressive Trans-Pacific Partnership – *Philippines officially submitted interest to join on 25 March 2021; Pending formal accession process.*

Article 14.11: Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

Article 14.13: Location of Computing Facilities

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore – *signed on 16 November 2020*

In recognition of the importance of data connectivity in financial services, Bangko Sentral ng Pilipinas ("BSP") and The Monetary Authority of Singapore ("MAS") have agreed on and jointly issue the following statement of intent:

1. Introduction

1.1. BSP and MAS recognise that the ability to aggregate, store, process, and transmit data across borders is critical to the development of the financial sector. The expanding use of data in financial services and the increasing use of technology to supply financial services offer a range of benefits, including greater consumer choice, enhanced risk management capabilities, and increased efficiency. These developments also pose new and complex risks for markets and challenges for policymakers and regulators. BSP and MAS are committed to working together and with other countries and authorities to promote an environment in financial services that fosters the development of the global economy.

2. Promotion of data connectivity

2.1. Data localisation requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to data. Data mobility in financial services supports economic growth and the development of innovative financial services, and benefits risk management and compliance programs, by, amongst others, making it easier to detect cross-border money laundering, terrorist financing patterns, and proliferation financing; defend against cyberattacks; and manage and assess risk on a global basis.

2.2. Based on this shared understanding, the BSP and MAS intend to promote the adoption and implementation of policies and rules that facilitate the following goals with respect to the operation of banks and non-bank financial institutions falling within the jurisdiction of either BSP or MAS ("covered institutions"):

a. Covered institutions should be allowed to transfer data, including personal information, across borders by electronic means provided this activity is for the conduct of the business within the scope of their license, authorisation, or registration.

b. The location where covered institutions can store and process their data should not be restricted as long as BSP and MAS have full and timely access to the data necessary to fulfill their regulatory and supervisory mandate.

c. If BSP or MAS is unable to access the data as described in paragraph 2.2(b) above, covered institutions should have the opportunity to remediate such lack of access before being required to use or locate computing facilities locally.

2.3 BSP and MAS also intend to, as appropriate, encourage other authorities to adopt policies and rules which facilitate the goals set out in paragraph 2.2.

3. Information sharing

3.1. BSP and MAS also intend to share information on developments related to the adoption and implementation of the policies and rules referred to in paragraphs 2.2 and 2.3.