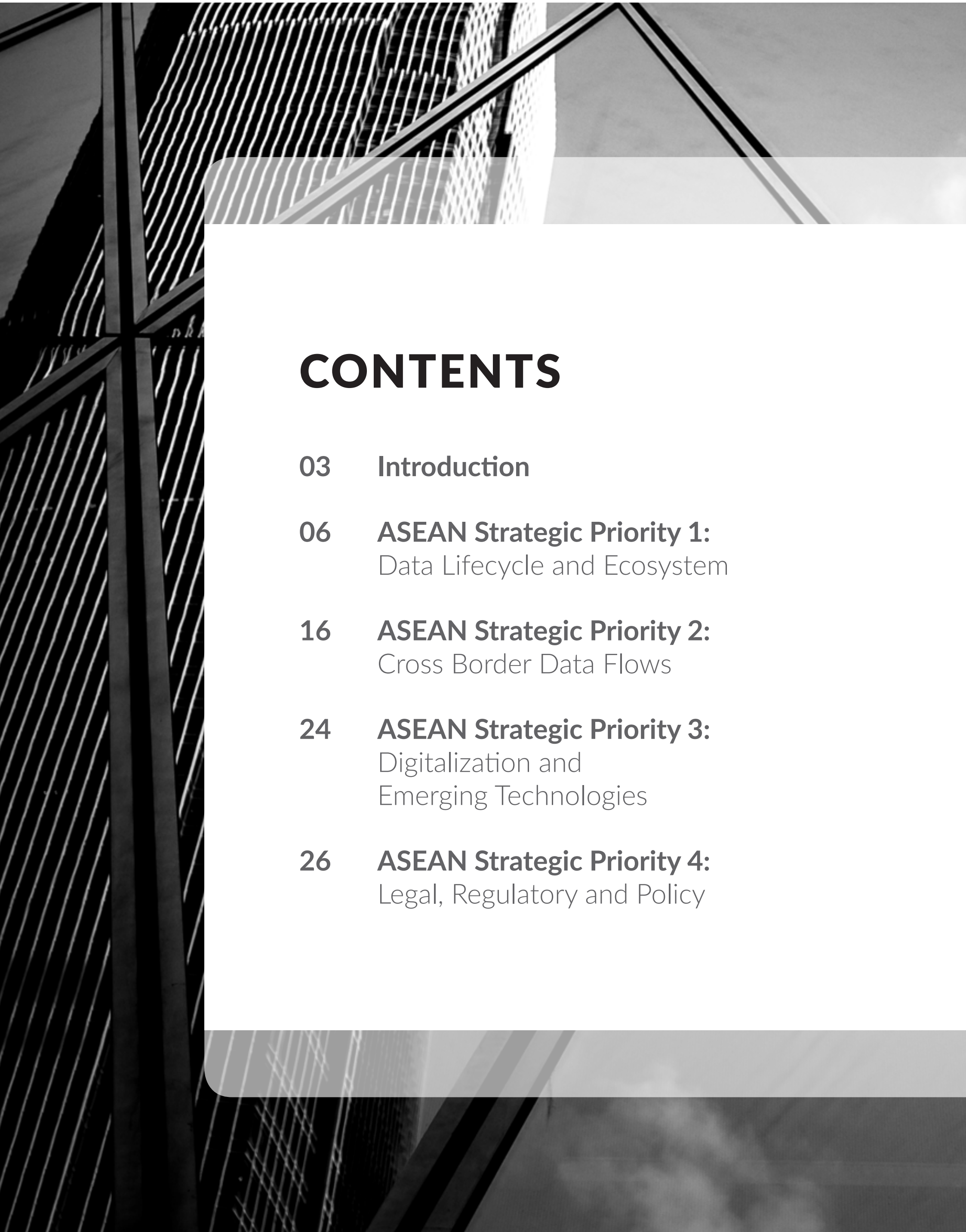
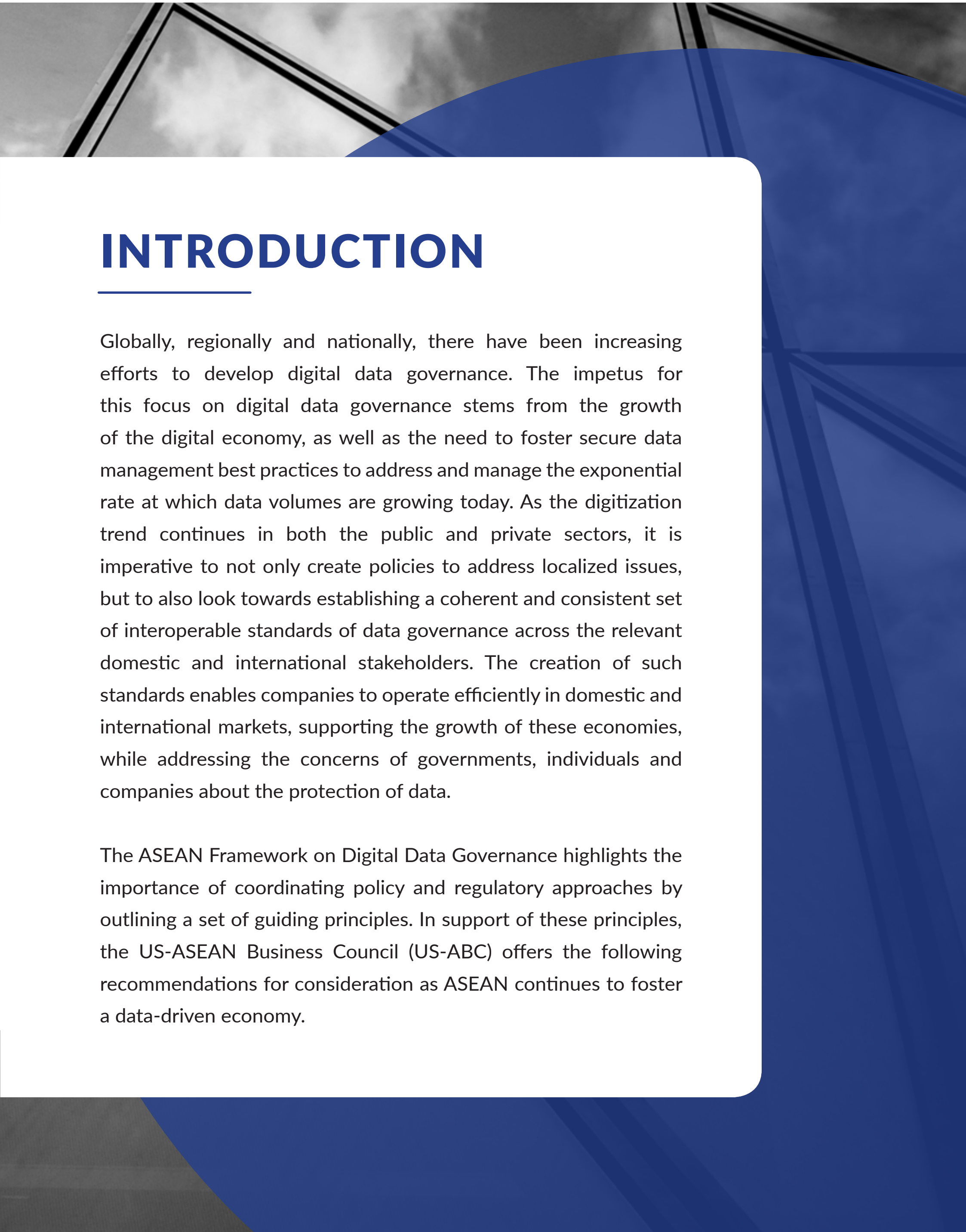
US-ASEAN
BUSINESS COUNCIL, INC.

DIGITAL DATA GOVERNANCE IN ASEAN

KEY ELEMENTS FOR A DATA-DRIVEN ECONOMY



CONTENTS



INTRODUCTION

Globally, regionally and nationally, there have been increasing efforts to develop digital data governance. The impetus for this focus on digital data governance stems from the growth of the digital economy, as well as the need to foster secure data management best practices to address and manage the exponential rate at which data volumes are growing today. As the digitization trend continues in both the public and private sectors, it is imperative to not only create policies to address localized issues, but to also look towards establishing a coherent and consistent set of interoperable standards of data governance across the relevant domestic and international stakeholders. The creation of such standards enables companies to operate efficiently in domestic and international markets, supporting the growth of these economies, while addressing the concerns of governments, individuals and companies about the protection of data.

The ASEAN Framework on Digital Data Governance highlights the importance of coordinating policy and regulatory approaches by outlining a set of guiding principles. In support of these principles, the US-ASEAN Business Council (US-ABC) offers the following recommendations for consideration as ASEAN continues to foster a data-driven economy.

OVERARCHING RECOMMENDATION:

The promotion of an interoperable data governance system is key to strengthening ASEAN's digital economy and data ecosystem

ASEAN Strategic Priority	ASEAN Guiding Principles	US-ASEAN Business Council Recommendations
Data Lifecycle and Ecosystem	• Data Integrity and Trustworthiness • Data Use and Access Control • Data Security	1.1 Promote Data Quality, Hygiene, Integrity, and Trustworthiness 1.2 Encourage Data Transparency and Accountability 1.3 Ensure Data Security at All Levels 1.4 Embrace a Risk-Based Approach towards the ASEAN Data Classification Framework
Cross Border Data Flows	• Cross Border Data Flows	2.1 Facilitate the Flow of Data Across Borders 2.2 Recognize the Importance of Cross Border Data Flows to the Digital Economy
Digitalization and Emerging Technologies	• Capacity Development	3.1 Leverage Public-Private Partnerships for Capacity Development 3.2 Support Global Standards and Policies Key to Emerging Technologies 3.3 Support Intellectual Property Rights to Drive Innovation
Legal, Regulatory and Policy	• Personal Data Protection and Privacy Regulation • Accountability • Development and Adoption of Best Practices	4.1 Align Data Protection and Privacy Regulations with International Best Practices 4.2 Coordinate Across Relevant Regulatory Bodies 4.3 Ensure Intra-ASEAN and International Transfers 4.4 Encourage Industry Self-Regulation 4.5 Engage with Private Sector Consistently and Collaboratively

The promotion of an interoperable data governance system is key to strengthening ASEAN's digital economy and data ecosystem. The adoption of internationally-recognized best practices support interoperability across the region and the globe. Where possible, general definitions should align with existing, broadly applicable examples, such as the ***OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, APEC Privacy Framework, and the EU General Data Protection Regulation (GDPR)***. This helps to enable a seamless integration between ASEAN and the global economy.

We further encourage ASEAN Member States to be mindful of some key distinctions when developing definitions for policies and regulations:

DATA CONTROLLERS AND DATA PROCESSORS

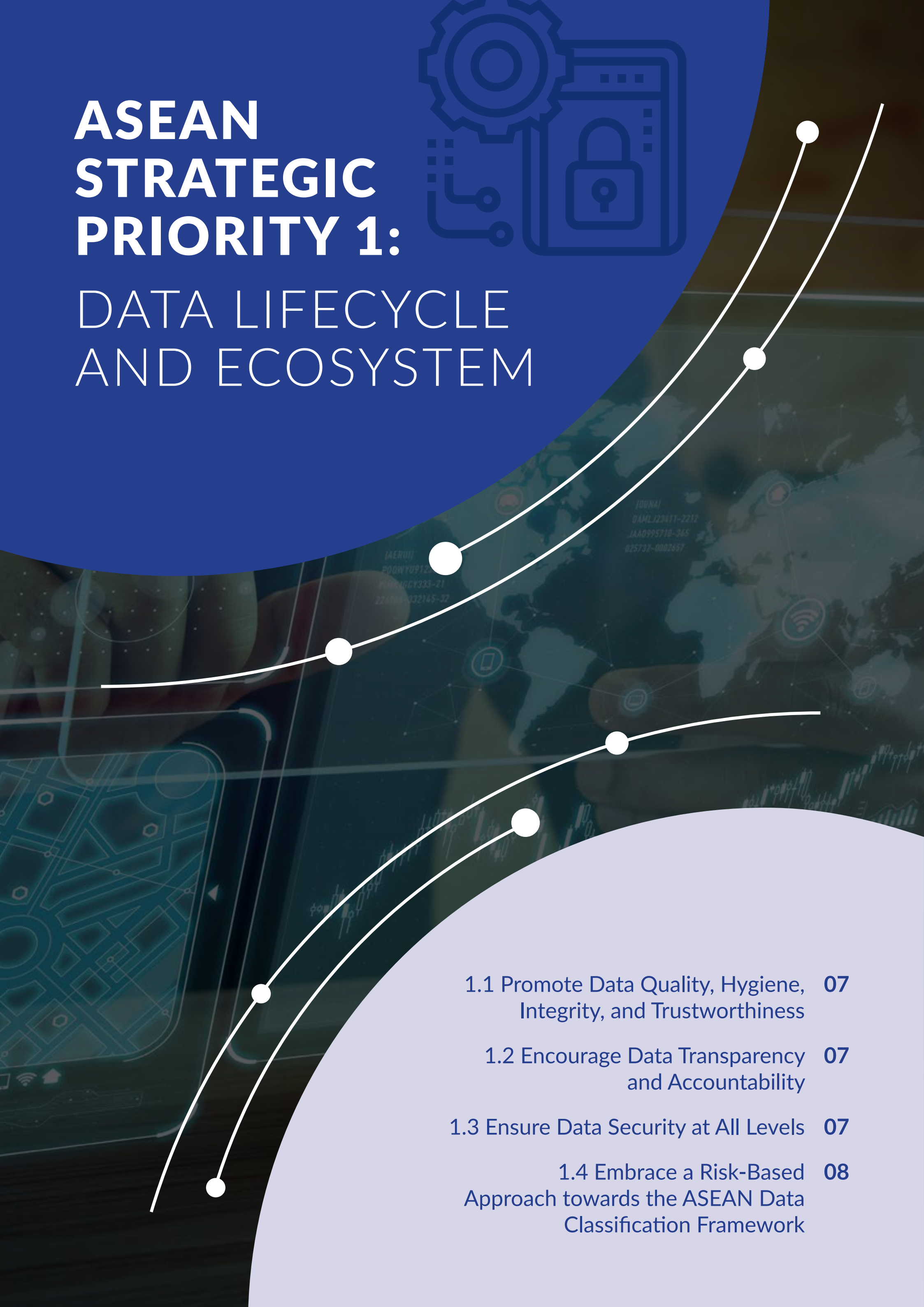
Data processors and data controllers have specific roles in the data lifecycle, with differing visibility and degrees of control over the decisions for collecting and processing consumers' personal data. Data controllers and data processors also have distinct and important responsibilities for meeting obligations under the law. Data processors process data on behalf of controllers rather than crafting or manipulating the data itself, and therefore lack the ability to make independent decisions on data usage. Processors should, however, also be encouraged to have proper risk-based systems in place to meet basic programmatic and security responsibilities and should be responsible for complying with the lawful instructions of the data controllers.

There are certain cases where a data processor may be a data controller vis-à-vis managing the data being processed on behalf of a data controller. As such, policies should recognize this by specifying the distinct obligations of controllers and processors, as well as for instances where organizations may hold dual responsibilities.

PERSONAL AND NON- PERSONAL DATA

Personal data should be defined as information which could be used to identify a specific natural individual (e.g. the data owner), directly or indirectly. Personal data should not include aggregated, encrypted, pseudonymized or otherwise anonymized or de-identified information which do not reasonably pose a risk of re-identification, all of which should be defined further in policies. Based on precedents in other existing personal data protection regimes globally, the definition of personal data should also exclude certain data collected or processed as part of an employment relationship (which excludes sensitive personal information), any business contact information or publicly available data.

ASEAN STRATEGIC PRIORITY 1:
DATA LIFECYCLE AND ECOSYSTEM



1.1 PROMOTE DATA QUALITY, HYGIENE, INTEGRITY AND TRUSTWORTHINESS

The US-ABC is supportive of the ASEAN Guiding Principles on Data Integrity and Trustworthiness, which recognizes the importance of access to accurate and reliable data. Personal data should be accurate, complete and up-to-date to the extent necessary for the purposes for which it is to be used.

1.2 ENCOURAGE DATA TRANSPARENCY AND ACCOUNTABILITY

The ASEAN Guiding Principle on Accountability supports the development and implementation of data protection and data management policies and promotes the continuous review of data protection and data management policies. We would also encourage data transparency on the types of personal data provided, purposes of collection, and how such personal data will be used or disclosed, particularly around using it to make decisions about the individual.

1.3 ENSURE DATA SECURITY AT ALL LEVELS

Data security starts with corporations and individuals taking responsibility to proactively protect data. We encourage governments to clearly articulate the objectives of data security regulations, as opposed to prescribing data security measures, which can rapidly become outdated with technological improvements and innovation to protect data. Data controllers and data processors should be encouraged to implement and maintain appropriate technical, procedural and physical safeguards to ensure the confidentiality, integrity and availability of data. Individuals should also be encouraged to proactively protect themselves, and to take further action to protect themselves when their data is compromised.

Data Breach Notification

To address data breaches promptly and effectively, policies should establish clear rules mandating the notification of breaches where it may cause material risks of significant harm to individuals, such as identity theft, fraud, or economic loss. This would exclude breaches of data which are not personal data, such as data which has been encrypted, or data which is pseudonymized, anonymized or otherwise de-identified, unless the encryption key or other data which may result in re-identification has also been breached.

Notification by data controllers to affected individuals should be encouraged without undue delay. Setting arbitrary deadlines for data breach notification is not ideal as the allotted period may not be commensurate to the time required for investigation and remediation of breaches, which vary in size, severity and complexity. If arbitrary deadlines are set, resources which could be used for investigating and remediating the breach may be diverted to dealing with breach notification requirements, which would not benefit the affected individuals.

Data Recovery and Remediation

Mechanisms for sharing data breach incidents through de-identified avenues should also be enabled to allow patching of potential vulnerabilities in the overall data ecosystem. Furthermore, preparation of contingency plans for disaster and data recovery should be encouraged as a best practice to ensure minimal disruption to overall trade flows and operations if and when data breaches occur.

1.4 EMBRACE A RISK-BASED APPROACH TOWARDS THE ASEAN DATA CLASSIFICATION FRAMEWORK

The US-ABC supports the promotion of sound data governance practices, in line with international standards, through the ASEAN Data Classification Framework. This approach would involve more than just classifying data, as organizations will need to discover the data they have; assign it with appropriate classification; protect it accordingly; monitor the data they hold; and comply with relevant regulations. Any regional framework should promote internationally-recognized best practices by organizations within ASEAN and allow ASEAN Member States and companies flexibility in classifying their own data, appropriate to their respective needs and sectors. Given that they serve different purposes, we would recommend that public sector data and commercial data also be classified separately. For commercial data classification, companies should be permitted take the lead in determining the appropriate classification levels for data under their control.

To that end, the US-ABC welcomes further discussion on the nature of the framework by elaborating best practices on: (i) data governance principles throughout the data lifecycle (e.g. collection, use, access, storage, disposal), and (ii) adequate protection of different types of data.

Data classification is one of many tools which public and private sector organizations use to ensure that their data is appropriately managed and protected. It works in conjunction with many other tools for appropriate management and protection of data, including authentication systems, access controls, encryption for data at rest and in transit, and physical security for data centers. As such, data classification should not be conflated with the need for further data localization requirements. Improved governance and protection, in alignment with international standards, will enable the goal of promoting the growth of trade and the flow of data among ASEAN Member States and their partners in the digital economy.

Within public sector data classification frameworks, there is typically a small percentage of highly-sensitive data where security concerns will outweigh competing considerations (e.g. cost of storage on premises or on cloud-based servers). Figure 1 provides a reference of how governments typically approach public sector data classification, with reference to applicable international standards under each classification.

Figure 1: Sample Reference Guide for Public Sector Data Classification

Data Classification	Data Examples	Possible Standards as Reference
Unclassified Data	Open Data, publicly available information including informational websites, terminology systems, standards, practitioner registries.	• Mapping Types of Information and Information Systems: National Institute of Standards and Technology (NIST) 800—60 • Global Quality Standard: International Standards Organization (ISO) 9001:2015 • Security Management Systems: ISO 27001 • Personal Data Protection: ISO 27018 • Standards for Security Categorization: NIST Federal Information Processing Standard (FIPS) 199 • Cybersecurity: NIST Cybersecurity Framework • Risk Management: NIST Risk Management Framework
Restricted Data	Sensitive government business or citizen data which may be shared with non-government entities, including Personally identifiable information (PII) such as identification numbers, biometric data or information on race or religion.	
Government Confidential Data	National security information or data dealing with matters of international negotiations, and military intelligence.	• Security Controls: NIST 800-53

In addition, the US-ABC encourages a flexible and outcome-oriented approach, and hopes to recommend some areas for consideration as ASEAN and its Member States may look to develop their data classification frameworks:

1.4.1 Distinguish between National Security Data and Commercial Data

There must be a clear definition of and distinction between national security data, which is generally agreed to be core to the security of the state (e.g. military and national defense information)[1] and commercial data, which companies use in the ordinary course of business or for legal and regulatory purposes (e.g. customer information which may include citizen data). The treatment of data such as passports, national IDs and driving licenses, which may be put into the category of national security or "strategic" data by some countries, has been debated. Understanding what data should constitute "strategic" and "national security," and implementing such a category is challenging, especially in certain sectors where the transfer of data is fundamental to its core business, such as financial services and healthcare. The aforementioned data should not be categorized as "strategic" or "national security" data.

While countries agree that some data are particularly important, they diverge on where it needs to be stored, with some leaning towards a complex process of onshoring. We therefore recommend that governments focus not on the location of the data, but on the availability of the data when requested (e.g. by law enforcement or for regulatory requirements) in determining an approach to the location of commercial data.

1.4.2 Develop Appropriate Classification Categories to allow for Contextualization

The ASEAN Data Classification Framework should provide non-binding guidance based on international standards, for individual ASEAN Member States and other organizations to adopt and tailor to their own systems of classifying data. Any proposed data classification model should outline appropriate categories with broad expectations and provide clear guidance on the types of security requirements accorded to each level based on its risk impact level (e.g. criticality and sensitivity of the data).

Bearing in mind the number of countries involved and sectors impacted, a prescriptive categorization system which outlines detailed types of protection to apply across ASEAN may pose challenges to adoption. Risk assessments should be contextual

[1] For example, the UK describes "Top Secret" information as "exceptionally sensitive HMG (or partner's) information assets that directly support (or threaten) the national security of the UK or allies AND require extremely high assurance of protection from all threats" (Government Security Classifications May 2018, UK Cabinet Office, Pg. 9). Similarly, the US defines "Top Secret" data as "information where unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to national security" (Executive Order 12356, Section 1.1(a)).

and subjective, and each classification system should ensure appropriate risk assessment and security protocols for each level.

Effective approaches to classification often result in organizations realizing that the majority of data they manage may not be highly sensitive. We recommend that only public sector national security data should be categorized into the highest classification category. The over-classification and/or over-inclusion of data incur additional costs when implementing controls due to additional resources required for securing, monitoring, measuring, remediating and reporting risks. This would greatly limit the availability of data, as well as capability or innovation opportunities. SMEs in particular would find compliance difficult.

1.4.3 Encourage Industry Self-Management of Commercial Data

Best practice data classifications only cover public sector (government) data sets. That is because private companies already maintain verifiable data management policies that deal with sensitive data. With respect to managing commercial data, companies should have in place verifiable data management policies, which classify data and assign data management practices, procedures and policies to ensure customer privacy and the security of data against fraud or cyber-attack within a country and for cross-border transfers. The distinction between PII and non-PII is often made by companies to protect the privacy of individuals.

Companies should already have specific measures in place to protect personal data, in line with the requirements of existing personal data protection and privacy regulations in most ASEAN jurisdictions. In addition, many companies already maintain comprehensive data management policies that distinguish between different types of data through a classification system and attribute different levels of protection to that information according to its sensitivity. A number of protective actions can be taken based on the classification applied to a specific piece of data. These may include encryption, restricting access rights, applying visual markings, executing a retention or deletion policy, or performing a data loss prevention action. Stricter information handling requirements are often required for the transmission, storage and disposal of data that may present a significant negative impact on a customer or company if disclosed.

Compliance with global or internationally-recognized standards and national or regional privacy policies are effective ways by which governments can determine whether companies have effective data management policies. If companies can demonstrate verifiable data management policies are in place to ensure data privacy, security, and accessibility, then data should be allowed to flow across borders.

Figure 2 (Part 1): Sample Reference Guide for Organizations to Develop and Implement Information Protection Policies

Data Classification	Data Examples	Possible Standards as Reference
Publicly Available Data	Data that is freely available within or outside the company or that is intended for public distribution. This may include media articles or company addresses.	No specific data management requirements
Internal Company Data; Private Data	Data which may have a negative impact on the company or its customers, staff or other third parties if disclosed. These may include internal company information such as financial reports or marketing strategies; as well as some PII such as certain business contact information. This may also include pseudonymized, anonymized or de-identified data under certain circumstances (e.g. data anonymized for analytics purposes).	Such data would have specific handling requirements for storage, processing and disposal.

Figure 2 (Part 2): Sample Reference Guide for Organizations to Develop and Implement Information Protection Policies

Data Classification	Data Examples	Possible Standards as Reference
Sensitive Company and Personal Data; Restricted Data; Confidential Commercial Data	Data which could have a significant negative impact on the company's legal or regulatory obligations, its financial status, or that of its customers, staff or third parties (e.g. identity theft, fraud, or economic loss) if disclosed. Specific examples may include: • Sensitive internal company information such as merger and acquisition information, strategy documents, intellectual property and other trade secrets; • PII such as biometric data or information on race or religion; • Personally identifiable financial information (PIFI) such as credit reports and banking customer records; • Protected health information (PHI) such as patient electronic medical and health records, including diagnosis, medication prescriptions, billing, admissions, and patient-generated health information. Generally, this category should not include pseudonymized, anonymized or de-identified data.	Sensitive customer data should be afforded the same levels of safeguards as sensitive internal company data. While such data should still be allowed to flow across borders, it should be subject to stricter handling requirements, such as encryption as well as additional disposal requirements. However, the specific data types that are in this category and their associated handling requirements should be determined on a per-company basis.

Dissemination and control markings may be used to add any extra granularity required for data handling of data. While they do not alter classification levels or any subsequent security controls and costs, markings provide further context and guidance as to who can access such data and how such data should be used (e.g. "For Official Use Only" or "Commercial in Confidence") within the established classification levels, throughout the data lifecycle. As a result, markings can provide organizations with a way to further protect and control data without building an entirely separate classification system.

1.4.4 Offer Clarity and Consistency

The most appropriate entity to assess the level of sensitivity of data is the organization which collects and uses that data. Each classification tier should be defined in a way that allows organizations to easily apply the right classification marking and handling, and for industries to self-regulate. Achieving as much classification consistency as possible amongst ASEAN Member States will be important to facilitate the stated goal of the Framework of cross border data transfers in an efficient and effective way.

As noted in 1.4.2, different classification systems require a change in security controls, would significantly increase costs, and would be difficult for companies – especially SMEs – to implement and for governments to monitor. It would therefore hinder the flow of data, thus reducing the net gains from a data-driven digital economy. Instead, it is important to encourage companies to adopt classification approaches, such as those mentioned in Figure 2, that provide appropriate safeguards for protecting data without stifling business operations and innovation.

Given the linkages ASEAN countries have with countries around the world – and the presence of companies from around the world in ASEAN – the framework should also achieve a high degree of consistency with other regions. The ability to transfer data to the U.S., EU and other countries in the Asia Pacific, and vice versa, should be factored into any ASEAN policy. Existing international standards, such as those developed by the International Standards Organization (ISO), should be used to guide organizations in assessing how their own data should be categorized and organized. Provisions under U.S. state privacy laws and the EU GDPR also need to be considered, so that companies in ASEAN Member States seeking to transfer data to and from these jurisdictions can utilize equivalence of mutual recognition regimes. This will further increase the interoperability of ASEAN-based companies with the rest of the world, and boost data-driven economic outcomes for ASEAN.

SECTORAL CONSIDERATIONS FOR DATA CLASSIFICATION

Different sectors have issues that need to be considered in formulating an ASEAN Data Classification Framework. As noted, some have considered including information on citizens, such as passport information, national ID or financial information, in a “national security” or “strategic” category. There are challenges to this approach in certain sectors and alternative approaches are needed for governments to address concerns they might have about protection of and access to that data.

The financial services sector is one of many sectors that may require additional considerations. Institutions such as banks need, for example, national identity documents in the ordinary, legitimate course of business, including verifying the identity of individuals in order to protect customer accounts from fraud and as part of national and international efforts related to Anti-Money Laundering (AML), Anti-Terrorist Financing and implementation of UN Sanctions. Similarly, institutions also need to rely on the international flow of financial information such as payments transaction data to provide effective fraud detection and prevention solutions.

If governments are concerned about access to data for regulatory, supervisory or legal inquiries, regulated financial firms can provide regulators with data within set time periods for legitimate regulatory, supervisory or legal inquiries in accordance with applicable laws, irrespective of the location of that data. Financial services firms can also ensure data is protected in accordance with local privacy requirements even if the data is offshore.

If financial services firms can provide adequate protection for data and can provide access to such data as described above, they should be able to send information across border, including national identity information or financial information relating to individuals or companies offshore. In addition, financial services firms should not be placed within a category of “national security” or “strategic” with a requirement to onshore data.

ASEAN STRATEGIC PRIORITY 2:

CROSS BORDER DATA FLOWS

2.1 FACILITATE THE FLOW OF DATA ACROSS BORDERS

The cross border flow of data underpins ASEAN's digital economy. As e-commerce continues to grow and digital technologies become ubiquitous, the ability of organizations to easily share data across borders is essential to advance a range of commercial interests as well as public policy objectives. Companies of all sizes and across all sectors rely on data flowing within and between countries to serve their customers, develop new products and services, increase cyber security and in many cases to enable regulatory compliance. As one of four initiatives outlined in the Framework on Digital Data Governance, an ASEAN cross border data flows mechanism that relies on tested existing transfer mechanisms can help ensure that appropriate safeguards are in place, so that data privacy and security are protected when data is transferred across borders, while also ensuring that home country regulators retain authorized access to that data. In addition to increasing trust among consumers and regulators, such a mechanism can also help provide certainty for businesses around data transfers.

An entirely new framework or mechanism for cross-border transfer that deviates too significantly from existing global best practices would raise the cost of compliance, affect interoperability and be detrimental to the growth of the digital economy in Southeast Asia. ASEAN and its Member States can draw from a range of existing mechanisms as outlined below, based on the following principles:

2.1.1 Maximize Data Flows

The ASEAN cross border data flows mechanism should seek to maximize data flows within the region. With this in mind, ASEAN Member States should seek to restrict data transfers only in very limited circumstances (e.g. where companies have not adhered to their legal or regulatory requirements).

2.1.2 Ensure that Requirements are Appropriate for the Associated Risks

Requirements on data flows should be commensurate with the associated risks. For example, if companies can demonstrate that data has been collected, stored and used in a secure and responsible manner, then data should be allowed to flow across borders.

Industry codes of conduct, developed through open, multi-stakeholder processes, can be an effective mechanism for allowing companies to show their compliance, including through certifications to international standards such as ISO/IEC 27001/27018. Recognizing standards and codes across borders, so that a given mechanism can be used in multiple markets, could provide consistency for regulators and customers in evaluating companies' compliance, without being overly-bureaucratic. It also provides an effective way of addressing privacy and security concerns associated with emerging technologies and rapidly evolving business models.

We also favor approaches aligned with the OECD's Accountability Principle and the ASEAN Framework on Personal Data Protection, which allow data to be transferred across borders if the data controller remains accountable for protecting the data regardless of its geographic location.

2.1.3 Harmonize Requirements

The requirements should be harmonized to ensure a consistent approach across the region, while also accounting for the different levels of maturity of ASEAN Member States. ASEAN should also leverage existing bilateral and multilateral frameworks, such as the APEC CBPR's multilateral cross-border data transfer framework, as it would enable companies to use established principles and mechanisms to protect the privacy and security of personal data as it moves across borders.

2.1.4 Provide Legal Frameworks for Appropriate Government Access to Offshore Data

It is recognized that there are instances where home country regulators may seek expedited access to data stored outside the country of its collection, including for law enforcement or regulatory objectives. ASEAN Member States should develop appropriate legal frameworks, both at the domestic and international level and including government-to-government agreements, that provide a basis for companies to promptly respond to cross border requests for data in ways that do not create conflicts of laws for companies operating in ASEAN.

2.1.5 Seek Interoperability

Achieving global interoperability, such as striving to adopt common global

standards, or the mutual recognition of standards or equivalent standards to key markets, will also support cross border data flows at both the intra-ASEAN level and at the international level. This is particularly important given ASEAN trade with the U.S., EU and other countries in the Asia Pacific region.

ASEAN Member States may also want to be mindful of some of the existing cross border transfer mechanisms, standards, and best practices:

Adequacy or Comparable Safeguards

Adequacy decisions set a legal basis for data transfer by requiring that data transferred to other jurisdictions be conferred an equivalent or appropriate level of protection for personal data via its domestic law and or its international commitments. Under GDPR, data can flow from the EU to a country deemed adequate (e.g. Japan has recently been granted adequacy status). However, the EU experience shows that achieving adequacy takes time and requires reworking of domestic privacy laws.

Other ASEAN Member States' data protection laws may also offer a model for proposed data transfer mechanisms based on ensuring that there are appropriate safeguards when facilitating the transfer of cross border data. As an example, Singapore's Personal Data Protection Act 2012 (PDPA) permits data transfers outside of the territory as long as the data is afforded a "comparable standard of protection".

Certification Regimes

US-ABC would caution against mandatory certification under any new ASEAN cross border transfer mechanism. In addition, any regime should be consistent with international standards, in order to avoid significant increases in complexity and the costs of compliance for all firms, especially SMEs.

Instead, ASEAN should encourage the use of internationally-recognized standards, such as relevant ISO standards, in order to raise the level of protection and improve interoperability among countries.

Undergoing independent third-party review and certification to existing privacy regimes, as in the APEC CBPR, could also facilitate data transfers. APEC CBPR is a voluntary, accountability-based system that facilitates data flows among eight participating APEC economies.[2] The system's program requirements are based on nine data privacy principles: preventing harm; notice; collection limitation; use choice; integrity; security safeguards; access; correction; and accountability.

APEC CBPR is consistent with global standards and is formally recognized as a valid data transfer mechanism in both Japan's amended privacy law and the recently concluded U.S.-Mexico-Canada Agreement (USMCA). By not superseding domestic legislation, CBPR also offers participating countries and companies a unified regime within a network of reciprocal, mutually-agreed privacy regulations that take account of local differences.

However, SMEs may find it difficult to use a certification regime like the APEC CBPR as it can be expensive and time consuming to achieve certification from the accountability agent. There are also questions around the value of being part of the regime as companies still need to comply with local requirements, which can differ significantly across countries. However, the US-ABC continues to encourage harmonization as countries introduce regulations consistent with CBPR so that they can be part of the regime.

Furthermore, the APEC CBPR does not currently work for companies in certain sectors, such as financial services. For example, the U.S. Federal Trade Commission (FTC)'s role as an enforcement body is not appropriate for financial institutions, which are not regulated by the FTC. Thus, an ASEAN cross border data flows mechanism must ensure the designation of an appropriate enforcement authority.

Facilitating Data Transfer Mechanisms

Existing data transfer mechanisms, such as Binding Corporate Rules (BCRs) and Standard Contract Clauses (SCCs), can also be considered as ASEAN seeks to facilitate global, regional, and bilateral data transfers. BCRs are internal rules that enable data transfers within the same corporate group. Under GDPR, they are legally binding and place liability on the EU-based entity. Since they are bespoke, BCRs allow for large data flows for different purposes, although reaching an agreement may take time. They are also limited in scope as data cannot be transferred to third parties. SCCs are model transfer terms drawn up by the European Commission that outline sets of contractual obligations and conditions to ensure that the same protections will be given to the transferred data. Since they are based on a standard template, this mechanism facilitates quick agreement. However, they are focused on specific data flows and so companies would need to agree and maintain many individual clauses.

[2] The APEC CBPR Participating Economies include: Australia, Canada, Chinese Taipei, Japan, the Republic of Korea, Mexico, Singapore and the United States of America. Many U.S. companies, particularly in the ICT sector, are also APEC CBPR certified.

ASEAN may also consider some other legal bases for data transfers which could facilitate regional or bilateral data transfer mechanisms; for example, "contractual necessity," which allows data transfers to take place where they are necessary for the performance of a contract between the data subject and data controller. Data transfers may also be allowed on grounds of "legitimate interests" by the data exporter, where there are legitimate grounds for such transfers of data overseas while also balancing the interests of the data subject as well.

We also encourage facilitating intra-group data transfers amongst entities operating as part of the same business group. Intra-group transfers of personal data such as employee or client contact databases between subsidiaries which are otherwise operating under the same parent entity are particularly important for the day-to-day operations of international commerce. The California Consumer Privacy Act (CCPA), for example, recognizes this issue and may be read as facilitating such intra-group transfers, because they currently should not be interpreted as a "sale".

Furthermore, ASEAN may want to consider enabling the free flow of non-personal data. The European Commission has issued non-binding guidance which prohibits EU Member States from maintaining or introducing non-personal data localization restrictions, unless it is justified on grounds of public security in compliance with the principle of proportionality. Although these rules only apply intra-EU and do not address data flows to or from third party countries, the guidance provides clarification on the interaction between the free flow of data and the GDPR. In particular, it offers clarity regarding datasets that are made up of both personal and non-personal data.

2.2 RECOGNIZE THE IMPORTANCE OF CROSS BORDER DATA FLOWS TO THE DIGITAL ECONOMY

Data is essential to the Internet and digital economy. As ASEAN economies strive to develop a well-functioning digital economy, it is critical to allow its key building block – data – to move freely. We encourage ASEAN Member States to draw from the work being done internationally, such as the WTO e-commerce initiative and in the USMCA, which preserves provisions for data flows, as they further enhance commitments made in the ASEAN Agreement on Electronic Commerce on accessing and moving data across borders.

The flow of data is fundamental to international trade, trade facilitation and the coordination of global value chains. The World Trade Organization (WTO) Moratorium on Electronic Transmissions, which prohibits customs duties on electronic transmissions, has facilitated the free movement of data flows for two decades and significantly enabled digital growth. If data is treated similarly to a physical import, it will definitively impede the flow of data as all entities – large and small companies, as well as individuals – will struggle to comply with import compliance requirements and additional fees in the form of duties. We encourage ASEAN Member States to respect the Moratorium.

In addition, data flows and digital data governance continue to impact businesses and services across all sectors, including in disaster response and recovery. Below are some sectoral considerations on the importance of data flows to different industries:

Financial Services

Cross border data flows are essential to the effective functioning of the domestic and international financial system, including to allow financial institutions to complete AML or Know-Your-Customer (KYC) checks to comply with country and United Nations sanctions, as well as to enhance cyber security. Data flows also assist with business continuity, for example, in the case of natural disasters. They are also crucial for the use of data for Artificial Intelligence (AI) and its application in fraud and threat intelligence. Fraud is not limited by national boundaries. Effective fraud mitigation is dependent on cross-border flows of data from all over the world. Only through the use of global or multi-country data sets can firms achieve the necessary sophisticated monitoring of transactions and rapid detection of the risk of fraud of each payment transaction. This not only protects individuals, banks and merchants from fraud, but in turn strengthens the integrity of a country's

financial system and helps ensure confidence among consumers in electronic payments and the digital economy.

International standards, such as the Payment Card Industry Data Security Standard (PCI DSS), ensure proper safeguards whilst enabling the free flow of data. Devaluing and desensitizing data through the employment of EMV chip technology, point-to-point encryption (e.g. PCI's P2PE standard), and tokenization also enhance payment security by rendering card data unusable by hackers.

Healthcare

The transfer of patient data is important for medical planning, across borders and in remote areas within a nation. Remote and cross border planning enables more efficient healthcare delivery systems by broadening the reach of healthcare providers. In addition, access to data can also improve the quality of medical care and promote a learning health system by offering greater insights into general patient behavior. Also, AI could have a significant impact on research and development efforts of pharmaceutical, medical technology and healthcare organizations in their ability to address potential inefficiencies in the patient journey and the overall delivery of healthcare.

Healthcare companies realize that in order to fully leverage the potential benefits of digitization in the healthcare sector, there needs to be sustainable and harmonized data governance policies. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITEC) are international standards which ensure that healthcare providers meet secure standards when storing, processing and transmitting PHI, while still enabling the transfer of data. For example, HIPAA and HITECH-covered entities are subject to safeguard PHI, such as through setting limitations around its use and disclosure, individual rights and administrative responsibilities. Moreover, international best practice experiences in this context could be considered by ASEAN in order to leapfrog into the appropriate collection, storage and use of PHI.

Manufacturing

Modern producers are embracing digitalization of plant and equipment within a smart manufacturing environment, and it is the future of all manufacturing. This includes operating smart machines within the context of the Internet of Things (IoT), in addition to legacy systems. It is increasingly common that companies have production facilities in disparate countries around the world, and manage their plant and machines using a digital twin and remote monitoring that allows them to manage operations globally on a real-time basis.

Fundamental to the effective use of IoT is the free flow of data, which will improve the productivity and efficiency of existing plants through an Infrastructure-as-a-Service (IaaS) model. The use of digital twinning infrastructure ensures reliability by providing proactive system maintenance and 24/7 remote monitoring for critical system parameters.

ASEAN STRATEGIC PRIORITY 3:

DIGITALIZATION AND EMERGING TECHNOLOGIES

3.1 LEVERAGE PUBLIC-PRIVATE PARTNERSHIPS FOR CAPACITY DEVELOPMENT

The American private sector remains steadfastly committed to partnering with ASEAN Member States in their capacity development efforts so that they can fully reap the benefits of the digital economy. Since 2014, the US-ASEAN Business Alliance for Competitive SMEs has administered training sessions for over 7,000 SMEs in ASEAN on a range of topics, such as how to leverage digital tools and emerging technologies (such as AI, 5G, quantum computing and the Internet of Things (IoT)) for growth, to empower local SMEs and support them in becoming regional business leaders and world-class suppliers in the global value chain. Leveraging such technologies also prepares ASEAN Member States to do their own innovations in these areas, most notably in the growing use cases and demand for IoT devices.

At the citizen-level, ASEAN should continue to promote digital literacy and enhance public awareness around individual data privacy and protection rights. U.S. companies have routinely and extensively partnered with universities in ASEAN to train and upskill the local workforce for digitalization and emerging technologies. The American private sector stands ready to continue partnering with ASEAN governments, academia, organizations and local businesses to equip ASEAN with the necessary resources to leverage emerging technologies and keep pace with the growth of the digital economy.

3.2 SUPPORT GLOBAL STANDARDS AND POLICIES KEY TO EMERGING TECHNOLOGIES

Data is carried by global technologies and is key to many emerging technologies, such as the deployment of 5G and the development of smart cities. For example, data is used by machine learning techniques to train AI. That data will increasingly be generated (and consumed) by the proliferation of IoT devices and use cases running over 5G and generations beyond. ASEAN Member States should continue to support, contribute to and adopt open, global technical standards and specifications to ensure that global companies continue to supply products, and to use as a basis for their own innovations and development in emerging technologies such as IoT. In addition to ISO standards, these may also include industry-specific standards (e.g. 3GPP). ASEAN Member States should also prioritize the allocation of resources (e.g. radio spectrum), to enable the timely deployment of these emerging technologies.

3.3 SUPPORT INTELLECTUAL PROPERTY RIGHTS TO DRIVE INNOVATION

As ASEAN Member States, leverage, and increasingly participate in the digital economy and emerging technologies, policies that support and encourage Intellectual Property Rights (IPR) are essential. The American system of innovation has widely been considered the product of a robust patent system, and strong IPR policies can help ASEAN members move from leveraging technology to becoming innovators in it.

ASEAN STRATEGIC PRIORITY 4:

LEGAL, REGULATORY AND POLICY

4.1 ALIGN DATA PROTECTION AND PRIVACY REGULATIONS WITH INTERNATIONAL BEST PRACTICES

Where countries have yet to implement basic personal data protection and privacy regulations, the US-ABC encourages the development of these policies and recommends that they be based on international best practices. The ASEAN Framework on Data Protection also offers a set of principles which may be referenced.

4.2 COORDINATE ACROSS RELEVANT REGULATORY BODIES

As innovative and emerging technologies continue to shape the landscape of digital trade, we also encourage Information and Communication Technology (ICT) ministries to proactively work with their counterparts in other ministries and agencies, such as those in finance and trade, as governments continue to formulate and implement new trade policies. Consistency in policies is crucial for nurturing an enabling environment for digital trade, which will in turn promote the growth of e-commerce and foster data-driven innovation in ASEAN.

4.3 ENSURE INTRA-ASEAN AND INTERNATIONAL TRANSFERS

Interoperability should be a key factor when assessing data governance in ASEAN. As well as transfers within ASEAN, data needs to be able to flow to other regions such as the U.S., EU and the Asia Pacific. Bridging mechanisms such as those outlined in the section on Cross Border Data Flows (e.g. adequacy, APEC CBPR, BCRs, etc.) should be considered as a way to do this.

4.4 ENCOURAGE INDUSTRY SELF-REGULATION

Whereas regulators and policymakers may set out baseline requirements, we recommend adopting a flexible approach which promotes industry self-regulation where possible. This will ensure there are proper safeguards in place without stifling innovation and takes account of firms working across borders. Such flexibility reinforces the principle on accountability and empowers companies to take charge in the upkeep of data privacy protection while keeping up with the pace of digitalization.

4.5 ENGAGE WITH PRIVATE SECTOR CONSISTENTLY AND COLLABORATIVELY

The American private sector always stands ready to assist ASEAN governments as they look to strengthen their data ecosystems and develop their regulatory environments. In the formulation of data governance policies, we recommend that ASEAN continue to consult with the private sector and other relevant stakeholders to leverage upon our technical expertise and experiences. By facilitating the sharing of information, perspectives and best practices, multi-stakeholder platforms, such as the ASEAN-US Digital Policy Consultative Forum, empower cooperation across borders and sectors in the development of ASEAN's data ecosystem.

US-ASEAN
BUSINESS COUNCIL, INC.

ABOUT THE US-ASEAN BUSINESS COUNCIL

For over 35 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's membership, more than 160 companies, generate over $6 trillion in revenue and employ more than 13 million people globally. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years.

The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.