Global Academic Frontiers, Vol. 3, Issue 1, 2025, pp.65-88 Print ISSN 2995-5688 Online ISSN 2995-570X
DOI: https://doi.org/10.5281/zenodo.15074696

Data Compliance in Cross-Border E-commerce: A Comparative Study of China and Malaysia's Regulatory Frameworks

ZHAO HONGQIANG [1,*] XIE YONGYI [2] ZHANG ZIYING [2] CUI XIAOTIAN [1]

[1] HENAN MUDU LAW FIRM
[2] University of Malaya
*Corresponding author Email: thxwu17@163.com
Received 18 March 2025; Accepted 23 March 2025; Published 24 March 2025

Abstract: This study conducts a systematic comparative analysis of data compliance requirements in cross-border e-commerce between China and Malaysia. Using digital sovereignty theory as a conceptual framework, the research examines regulatory convergences and divergences across four critical dimensions: data localization, cross-border data transfer, privacy protection, and cybersecurity. Findings reveal that China employs a security-centered approach prioritizing data sovereignty, while Malaysia adopts a development-centered framework balancing protection with digital economy growth. These distinct regulatory philosophies create significant compliance challenges for market participants, with disproportionate impacts on small and medium-sized enterprises. Despite these differences, opportunities for regulatory harmonization exist, particularly within bilateral cooperation frameworks. The study contributes practical guidance for navigating complex regulatory landscapes while offering recommendations for enhanced regulatory compatibility including tiered compliance guidelines and bilateral mutual recognition mechanisms to facilitate cross-border digital trade.

Keywords: Data compliance, Cross-border e-commerce, Digital sovereignty, China-Malaysia relations, Regulatory harmonization

I. Introduction

The digital transformation of global trade has positioned cross-border e-commerce as a pivotal component of bilateral economic relations between China and Malaysia. According to the General Administration of Customs of China (2023), bilateral trade between these nations has reached unprecedented levels, with digital transactions constituting an increasingly significant proportion of this exchange. As China maintains its position as Malaysia's largest trading partner for over a decade, the regulatory frameworks governing data flows between these jurisdictions have emerged as critical determinants of their digital trade ecosystem.

China's approach to data governance has evolved rapidly in recent years, transitioning from fragmented sectoral regulations to a comprehensive legal architecture that prioritizes national security, data sovereignty, and personal information protection. This evolution reflects China's broader digital strategy outlined in the 14th Five-Year Plan (2021-2025), which emphasizes indigenous innovation, cyber sovereignty, and secure development of the digital economy. The implementation of China's Cybersecurity Law in 2017, followed by the Data Security Law and Personal Information Protection Law in 2021, established one of the world's most sophisticated data regulatory regimes, with significant implications for cross-border e-commerce.

This regulatory evolution occurs within the context of China's Digital Silk Road initiative, which seeks to expand China's digital presence across global markets while establishing Chinese technological standards. As Zhang (2023) observes, China's data governance framework serves both protective and strategic functions, safeguarding national security while creating a regulatory environment that potentially advantages domestic digital champions. These dual objectives shape how cross-border e-commerce platforms must structure their data operations when engaging with the Chinese market.

Malaysia's regulatory approach, by contrast, has developed within the framework of ASEAN digital integration initiatives. Ismail and Masud (2020) note that Malaysia deliberately calibrates its regulatory frameworks to enhance regional e-commerce connectivity, balancing data protection with digital economy development objectives. The implementation of Malaysia's Personal Data Protection Act, alongside initiatives like the Digital Free Trade Zone, reflects this development-centered approach to data governance.

The challenges of navigating these dual regulatory systems are particularly acute for market participants seeking to capitalize on digital trade opportunities between these nations. Recent empirical research demonstrates that data policy restrictions have quantifiable impacts on cross-border e-commerce performance, with differential effects depending on the regulatory approach employed. These impacts appear especially pronounced for small and medium-sized enterprises, which often lack resources for comprehensive compliance programs. The absence of regulatory harmonization creates redundant compliance costs and potential operational barriers that may constrain digital trade potential.

This study addresses existing research gaps by developing a systematic comparative analysis of data compliance requirements in cross-border e-commerce between China and Malaysia. The research employs digital sovereignty theory as its conceptual foundation, examining how competing imperatives of data protection, national security, economic development, and trade facilitation shape regulatory approaches in both jurisdictions. By analyzing the convergences and divergences in data compliance frameworks across four critical dimensions — data localization, cross-border data transfer, privacy protection, and cybersecurity — the study provides both theoretical insights into comparative digital governance and practical guidance for navigating complex regulatory landscapes.

The significance of this research extends beyond academic inquiry. For policymakers, understanding regulatory convergence opportunities can inform more coherent governance approaches. For businesses, comprehending compliance requirements across jurisdictions is essential for developing viable cross-border e-commerce strategies. This paper provides a timely examination of a critical yet

understudied dimension of China-Malaysia economic relations, with implications for the broader ASEAN region and global digital trade governance.

II. Literature Review and Theoretical Framework

A. Data Governance in Digital Trade

The regulatory landscape governing data flows in digital trade has emerged as a critical area of scholarly inquiry. Lu (2022) provides a foundational analysis of data localization requirements, examining China's approach within a broader comparative context. His study identifies how data localization mandates reflect broader digital sovereignty objectives while creating potential friction points for cross-border digital commerce. This analysis is particularly relevant for understanding China's evolving regulatory philosophy, which prioritizes security and control dimensions of data governance over purely economic considerations.

Regional perspectives on data governance have been explored by several scholars. Chan (2022) examines data regulations as a promising area for digital economy collaboration in Malaysia, positioning the country's regulatory approach within broader ASEAN integration initiatives. Similarly, Chen et al. (2023) explore ASEAN-China cooperation opportunities, positioning data governance as a critical domain for enhanced digital trade integration. These regional analyses provide important context for understanding how national regulatory frameworks interact with broader economic integration initiatives.

Comparative perspectives on regional data governance frameworks provide valuable insights. Singapore's Personal Data Protection Act and Model Artificial Intelligence Governance Framework represent a balanced approach that has positioned the country as a digital hub while maintaining robust protection standards (Chik, 2023). Indonesia's recent implementation of Government Regulation 71 concerning Electronic Systems and Transactions established more stringent data localization requirements, reflecting a trend toward digital sovereignty across the region (Djafar, 2022). These diverse approaches within ASEAN demonstrate the complex regional landscape within which China-Malaysia data governance must be understood.

The European Union's General Data Protection Regulation (GDPR) has emerged as a global reference point for data protection frameworks. Bradford (2020) documents the "Brussels Effect" through which the GDPR has influenced regulatory approaches worldwide, including in Asia. Comparative studies by Greenleaf (2021) examine GDPR influence on Asian data protection frameworks, finding varying degrees of convergence across jurisdictions. These studies provide important comparative context for understanding China and Malaysia's distinctive regulatory approaches.

B. Theoretical Frameworks

The comparative analysis of data compliance regulations benefits from several theoretical perspectives that provide conceptual frameworks for understanding regulatory approaches. Digital sovereignty theory offers a particularly useful lens for examining how nations assert control over their digital domains while participating in global digital trade. This theoretical approach conceptualizes data

governance as an expression of sovereign authority, with regulatory choices reflecting different prioritizations of security, economic, and social objectives.

Digital sovereignty encompasses not merely territorial control over physical infrastructure but extends to informational control over data flows regardless of physical location. Lu (2022) applies this framework to data localization requirements, demonstrating how sovereignty considerations shape regulatory decisions regarding data storage and processing mandates. The digital sovereignty framework reveals significant differences in how China and Malaysia conceptualize state authority in digital domains, with China exercising what might be termed "comprehensive digital sovereignty," while Malaysia adopts a more selective approach focused on specific data categories.

Regulatory competition theory provides another valuable perspective, particularly for understanding how different jurisdictions may strategically design their data governance frameworks to attract or control digital investments. This theoretical approach views regulatory choices as strategic positioning decisions within a competitive landscape, where jurisdictions seek to balance protection imperatives with attraction of digital economy investment. This helps explain why emerging economies like Malaysia may adopt different regulatory postures compared to China, potentially emphasizing development-oriented frameworks over security-centric approaches.

The theoretical concept of regulatory equivalence offers insights into how seemingly different regulatory mechanisms may achieve similar functional objectives across jurisdictions. This concept focuses on outcomes rather than specific legal instruments, examining whether different regulatory approaches provide comparable levels of protection or control despite using distinct legal mechanisms. While China and Malaysia have distinct legal traditions and regulatory philosophies, functional equivalence analysis enables identification of areas where divergent approaches may yield similar substantive protections.

Data justice theories provide conceptual frameworks for evaluating the normative dimensions of data governance, examining how regulatory choices distribute benefits, burdens, and risks across different stakeholders. These theories are particularly relevant for analyzing cross-border e-commerce regulations that may have differential impacts on domestic and foreign market participants, as well as on enterprises of different scales. The theoretical lens of data justice helps illuminate potential asymmetries in regulatory frameworks that might favor certain market participants over others.

C. Selection of Analytical Dimensions

The selection of the four analytical dimensions for this study—data localization, cross-border data transfer, privacy protection, and cybersecurity—is based on their prominence in the literature and their demonstrated impact on cross-border e-commerce operations. Empirical studies have consistently identified these dimensions as critical determinants of compliance burdens and operational viability for digital trade.

Data localization has been identified by Lu (2022) as a fundamental expression of digital sovereignty with direct operational impacts on cross-border data flows. A systematic review of data governance literature by Wu et al. (2022) found that localization requirements ranked as the most significant regulatory barrier to digital trade based on impact assessments across multiple jurisdictions.

Cross-border data transfer mechanisms have been demonstrated to have direct impacts on trade performance. Empirical studies by Ferracane and van der Marel (2021) establish strong correlations between transfer restriction intensity and reduced digital service exports, with particularly pronounced effects in developing economies. Their assessment of regulatory restrictiveness identifies transfer mechanisms as a critical dimension for comparative analysis.

Privacy protection frameworks have been consistently identified as essential components of e-commerce governance. Morić et al. (2023) establish through systematic literature review that privacy requirements represent the most frequently cited regulatory consideration in e-commerce operations, with direct impacts on consumer trust and transaction volumes.

Cybersecurity obligations have been demonstrated to create significant compliance burdens with direct operational impacts. Chen and Li (2022) quantify these impacts through survey data from cross-border e-commerce operators, finding that security requirements rank among the top three regulatory concerns affecting operational decisions.

These empirical foundations establish the priority of these dimensions based on their documented impact on cross-border e-commerce operations. While other dimensions such as content regulation or intellectual property protection also affect digital trade, the selected dimensions have been empirically established as primary determinants of operational viability in cross-border e-commerce specifically.

III. Methodology

This study employs a comparative legal research methodology to analyze data compliance frameworks governing cross-border e-commerce in China and Malaysia. The comparative approach enables systematic identification of regulatory similarities and differences while facilitating functional equivalence analysis across different legal traditions and regulatory philosophies.

A. Research Design

The research design adopts a structured comparative approach that examines data compliance requirements across the four defined analytical dimensions: data localization requirements, cross-border data transfer mechanisms, privacy protection frameworks, and cybersecurity obligations. This dimensional approach enables systematic comparison while accounting for the complex, multilayered nature of data compliance regulations.

The research employs functional comparative analysis, examining how different legal mechanisms address similar regulatory objectives across jurisdictions, rather than merely comparing formal legal provisions. This approach recognizes that different legal systems may employ distinct regulatory tools to achieve comparable outcomes. The comparative analysis operates at three levels: (1) formal legal provisions, (2) implementation mechanisms, and (3) practical impact on cross-border e-commerce operations.

B. Data Collection

The research draws upon primary and secondary sources to develop a comprehensive understanding of data compliance frameworks in both jurisdictions. Primary sources include legal texts, regulations, and administrative measures governing cross-border e-commerce. For China, these include the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, along with implementing regulations. For Malaysia, primary sources include the Personal Data Protection Act and related regulatory instruments.

Secondary sources include scholarly literature, official policy documents, and analytical reports that contextualize these legal frameworks. The analysis also incorporates case studies of specific e-commerce platforms to illustrate practical compliance approaches. These include both large enterprises such as Alibaba's operations in Malaysia's Digital Free Trade Zone (as examined by Neilson, 2022) and small to medium-sized enterprises such as Malaysia's PrestoMall and China's Ymatou, providing balanced perspective on compliance challenges across different operational scales.

C. Analytical Framework

The analytical framework employs structured qualitative comparison to identify regulatory convergences and divergences across the defined dimensions. For each dimension, the analysis examines:

1. Substantive requirements: Core obligations imposed on e-commerce operators
2. Compliance mechanisms: Processes for demonstrating adherence to regulatory requirements
3. Enforcement approaches: Methods and intensity of regulatory oversight
4. Practical implications: Operational impact on cross-border e-commerce, with particular attention to differential impacts based on enterprise scale

This structured approach enables systematic identification of regulatory similarities and differences while facilitating assessment of their practical significance for cross-border e-commerce operations. The analysis employs legal hermeneutics to interpret statutory provisions within their systemic context, recognizing that data compliance requirements exist within broader regulatory ecosystems.

D. Limitations

This methodology acknowledges several limitations. First, data compliance regulations in both jurisdictions continue to evolve rapidly, requiring temporal boundaries for the analysis while recognizing that findings reflect a specific regulatory moment. Second, implementation and enforcement data may be limited, particularly for recent regulatory provisions. Third, the analysis necessarily focuses on formal regulatory requirements rather than actual compliance practices, which may vary across firms and sectors. Despite these limitations, this methodological approach enables systematic comparative analysis of data compliance frameworks in China and Malaysia, providing insights into both regulatory convergences and divergences while identifying their implications for cross-border e-commerce operations.

IV. China's Data Compliance Framework

China has developed a comprehensive data compliance framework that significantly impacts cross-border e-commerce operations. This regulatory ecosystem has evolved rapidly in recent years, transitioning from fragmented sectoral regulations to a sophisticated legal architecture that prioritizes national security, data sovereignty, and personal information protection.

A. Evolution of China's Data Governance Ecosystem

China's data governance framework has developed through a series of legislative initiatives that collectively establish one of the world's most comprehensive data regulatory regimes. The regulatory framework is built upon three foundational laws: the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (2021). These laws establish overlapping yet distinct regulatory requirements that collectively govern data processing activities, including those essential to cross-border e-commerce operations.

This regulatory evolution reflects China's broader digital strategy outlined in the 14th Five-Year Plan (2021-2025), which emphasizes indigenous innovation, cyber sovereignty, and secure development of the digital economy. The plan specifically identifies data as a "factor of production" and strategic resource, highlighting its centrality to China's economic and security interests.

B. Data Localization Requirements

Data localization mandates represent a cornerstone of China's data compliance framework, with significant implications for cross-border e-commerce operators. The Cybersecurity Law established the foundational requirement that "critical information infrastructure operators" must store personal information and important data collected and generated within China. Article 37 specifically mandates that "Critical information infrastructure operators that gather or produce personal information and important data during operations within the mainland territory of the People's Republic of China shall store it within mainland China."

The scope of this localization requirement was subsequently expanded by the Data Security Law, which introduced a tiered classification system for data based on its importance to national security and public interests. Article 31 of the Data Security Law reinforces the localization mandate while creating a more nuanced framework for determining which data must be stored domestically. This classification-based approach creates variable localization requirements depending on data sensitivity and potential security implications.

For cross-border e-commerce platforms, these localization requirements create significant operational implications. As Lu (2022) notes, data localization mandates often necessitate infrastructure investments within China, potentially increasing operational costs and complexity. The requirement to maintain data processing capabilities within Chinese borders represents a departure from the globally distributed data processing models often employed by multinational e-commerce platforms.

C. Cross-Border Data Transfer Mechanisms

China's framework for cross-border data transfers establishes procedural requirements that significantly impact e-commerce operations. The Personal Information Protection Law requires personal information processors to meet one of several conditions before transferring personal information outside China. Article 38 establishes four primary pathways for lawful cross-border data transfers:

1. Passing a security assessment conducted by the Cyberspace Administration of China (CAC)
2. Obtaining personal information protection certification from specialized institutions
3. Entering into standard contracts with foreign recipients that specify responsibilities and obligations
4. Meeting other conditions prescribed by laws or regulations

For operators of "critical information infrastructure" and processors handling large volumes of personal information, security assessments conducted by the CAC are mandatory. These assessments evaluate multiple factors including the purpose and necessity of the transfer, the data protection laws of the recipient country, and potential security risks.

These transfer mechanisms create significant procedural requirements for cross-border e-commerce platforms that routinely transfer transaction data, user profiles, and operational information across borders. The security assessment process in particular creates substantial compliance burdens that disproportionately impact small and medium-sized enterprises lacking dedicated compliance resources.

D. Privacy Protection Framework

China's privacy protection framework is primarily embodied in the Personal Information Protection Law, which establishes comprehensive requirements for processing personal information in e-commerce contexts. The law adopts a consent-based approach to personal information processing, requiring that processors obtain informed consent before collecting personal information while meeting principles including purpose limitation, data minimization, and transparency.

Article 13 establishes that personal information may only be processed with individual consent, except in specific circumstances such as contract performance, legal obligations, public health emergencies, or protecting natural persons' life and property. Article 14 further requires that consent be "voluntary and explicit" after individuals have been fully informed of processing purposes and methods. These consent requirements create significant operational impacts for e-commerce platforms, which must implement robust mechanisms to obtain and document user consent for various data processing activities.

Notably, the Personal Information Protection Law creates heightened protection for "sensitive personal information," including biometrics, religious beliefs, specific identities, medical health, financial accounts, and tracking locations. Article 29 defines sensitive personal information as "personal information that, once leaked or illegally used, could easily lead to violations of personal dignity or harm

to personal or property safety." E-commerce platforms processing such data face additional requirements, including specific consent mechanisms and impact assessments.

E. Cybersecurity Obligations

Cybersecurity requirements represent a critical dimension of China's data compliance framework. The Cybersecurity Law establishes baseline network security obligations for all network operators, including implementing internal security management systems, adopting technical measures to prevent cyberattacks, and reporting cybersecurity incidents. Article 21 specifically requires network operators to "formulate internal security management systems and operating procedures, determine persons responsible for cybersecurity, and implement cybersecurity protection responsibilities."

For "critical information infrastructure operators," which may include major e-commerce platforms, additional requirements apply. Article 34 mandates specialized security protections for critical information infrastructure, including dedicated security management departments, periodic security education and training, disaster recovery backups, and emergency response plans. These enhanced obligations create layered security requirements depending on an organization's classification within the regulatory framework.

The Data Security Law extends these obligations by establishing a risk-based approach to data security, requiring processors to implement security measures commensurate with the risk level of the data. Article 27 requires the establishment of a "comprehensive data security management system" covering the entire data processing lifecycle. This classification-based approach creates variable security obligations depending on the nature of data processed, potentially creating complex compliance scenarios for e-commerce platforms handling diverse data types.

F. Implementation and Enforcement

China has demonstrated increasing willingness to enforce data compliance requirements against both domestic and foreign companies. Enforcement actions have targeted various compliance deficiencies, including inadequate consent mechanisms, excessive data collection, and unauthorized cross-border transfers. The potential penalties are substantial, including fines up to 50 million yuan or 5% of annual revenue for serious violations of the Personal Information Protection Law.

For cross-border e-commerce operators, this enforcement environment creates significant compliance incentives. The regulatory framework's emphasis on security and sovereignty means that violations that implicate these concerns are particularly likely to trigger enforcement responses. This enforcement reality reinforces the necessity of integrating data compliance considerations into fundamental business operations rather than treating them as peripheral regulatory matters.

G. Case Study: Compliance Challenges for SMEs - Ymatou

The case of Ymatou, a Chinese cross-border e-commerce platform connecting Chinese consumers with international sellers, illustrates the compliance challenges faced by medium-sized enterprises under China's regulatory framework. With approximately 350 employees and 80 million registered users,

Ymatou operates in a complex regulatory environment that requires substantial compliance resources despite its relatively limited scale compared to giants like Alibaba.

Following implementation of the Personal Information Protection Law, Ymatou was required to undertake comprehensive compliance measures including revising privacy policies, implementing explicit consent mechanisms, and establishing data minimization procedures. The company reported allocating approximately 15% of its IT development resources to compliance-related system modifications over an 18-month period, representing a significant operational burden.

Particularly challenging was Ymatou's compliance with cross-border transfer requirements, as its business model inherently involves international data flows. The security assessment pathway proved prohibitively complex given the company's resources, leading Ymatou to rely primarily on standard contractual clauses with foreign partners. This approach required extensive legal consultation and partner education, creating significant administrative overhead.

Ymatou's experience illustrates how China's comprehensive regulatory framework creates disproportionate compliance burdens for medium-sized e-commerce operators, potentially advantaging larger platforms with greater resources for regulatory navigation. The case demonstrates the need for scaled compliance pathways that maintain core protections while reducing procedural complexity for smaller market participants.

V. Malaysia's Data Compliance Framework

Malaysia has developed a distinctive data compliance framework that balances personal data protection with digital economy development objectives. Unlike China's security-centric approach, Malaysia's regulatory framework emphasizes economic development within a regional integration context, while still maintaining fundamental data protection principles.

A. Evolution of Malaysia's Data Governance Framework

Malaysia's approach to data governance has evolved within the context of its broader digital economy aspirations. As a member of ASEAN with significant trade ties to China, Malaysia has developed data regulations that reflect both international standards and regional integration priorities. Chan (2022) identifies data regulations as one of the most promising areas for digital economy collaboration in Malaysia, highlighting the development-oriented nature of Malaysia's regulatory approach.

The foundation of Malaysia's data governance framework is the Personal Data Protection Act 2010 (PDPA), which came into force in 2013. This legislation establishes core data protection principles while creating specific compliance obligations for data processors and users. The Malaysian regulatory framework has subsequently evolved through sectoral regulations, administrative directives, and participation in regional data governance initiatives, creating a layered compliance environment for cross-border e-commerce platforms.

Malaysia's Digital Economy Blueprint (MyDIGITAL), launched in 2021, positions data governance as a critical enabler of the country's digital transformation. The blueprint specifically identifies regulatory frameworks that "balance security, data protection and business competitiveness" as strategic priorities, reflecting Malaysia's development-centered approach to data governance.

B. Personal Data Protection Framework

The Personal Data Protection Act forms the cornerstone of Malaysia's data protection framework, establishing comprehensive requirements for processing personal data in commercial contexts, including e-commerce transactions. The PDPA is based on seven core principles: General Principle (requiring consent), Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle, and Access Principle. These principles create a rights-based approach to data protection that applies to "data users" processing personal information in commercial transactions.

For cross-border e-commerce platforms, these principles create several operational requirements. Section 6 of the PDPA establishes the General Principle, requiring that personal data may only be processed with the data subject's consent. Section 7 implements the Notice and Choice Principle, mandating that data users provide clear information about processing purposes, data types, and rights of data subjects. These provisions create fundamental compliance obligations for e-commerce platforms collecting customer information.

Notably, Malaysia's data protection framework applies to personal data processed "in respect of commercial transactions," creating a scope limitation that excludes certain governmental data processing. Section 2 defines "commercial transactions" as "any transaction of a commercial nature... including any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance." This commercial focus aligns with Malaysia's broader approach of facilitating digital economy development while protecting consumer interests in commercial contexts.

C. Data Localization Requirements

Unlike China's comprehensive localization mandates, Malaysia has adopted a more limited approach to data localization. The PDPA does not impose general data localization requirements across all sectors. However, sectoral regulations create specific localization requirements for certain categories of data. For example, Bank Negara Malaysia imposes localization requirements for certain financial data, which may impact e-commerce platforms offering financial services or payment processing.

These sectoral localization requirements derive from specific regulatory directives rather than general legislation. Bank Negara Malaysia's regulations require certain financial institutions to maintain primary data centers within Malaysia, while permitting backup facilities offshore subject to appropriate safeguards. These requirements focus specifically on data related to regulated financial activities rather than applying broadly across all data categories.

This sectoral approach creates a more flexible regulatory environment compared to China's comprehensive localization mandates. The Malaysian Investment Development Authority highlights Malaysia's generally permissive approach to data flows as part of its investment promotion strategy, noting that localization requirements are limited to specific sensitive sectors. This approach reflects Malaysia's positioning as an ASEAN hub for digital services, where excessive localization requirements might undermine its competitive positioning.

D. Cross-Border Data Transfer Mechanisms

Malaysia's framework for cross-border data transfers establishes important compliance requirements while maintaining relatively greater flexibility compared to China's approach. Section 129 of the PDPA prohibits transfers of personal data to jurisdictions outside Malaysia unless specific conditions are met. These conditions include:

1. Consent from the data subject
2. Necessity for contract performance
3. Legal obligation
4. Vital interests
5. Transfers to jurisdictions specified by the Minister as providing adequate protections

This approach creates a dual system for cross-border transfers: either obtaining specific consent or relying on adequacy determinations for destination jurisdictions. Unlike China's mandatory security assessment approach for certain transfers, Malaysia's framework does not generally require prior regulatory approval for data exports, creating lower procedural barriers for routine cross-border data flows in e-commerce operations.

The consent-based mechanism provides operational flexibility for e-commerce platforms, allowing them to establish appropriate consent frameworks within their user interfaces. This approach emphasizes individual autonomy and choice, aligning with Malaysia's generally more market-oriented regulatory philosophy compared to China's state-centered approach.

E. Digital Free Trade Zone Initiative

Malaysia's data compliance framework must be understood within the context of its Digital Free Trade Zone (DFTZ) initiative, which has significant implications for cross-border e-commerce. As analyzed by Neilson (2022), the DFTZ represents Malaysia's strategic attempt to position itself as a regional e-commerce hub, with Chinese platforms including Alibaba playing significant roles in its development. The initiative includes partial regulatory accommodations designed to facilitate cross-border e-commerce operations.

Neilson observes that the DFTZ involves "strategic regulatory calibration designed to attract digital economy investment," including streamlined customs procedures and specialized digital infrastructure. While the DFTZ does not exempt operators from core data protection requirements, it creates a more streamlined regulatory environment that facilitates cross-border data flows necessary for e-commerce operations.

The DFTZ initiative demonstrates Malaysia's development-centric approach to digital economy regulation, where regulatory frameworks are designed to enable economic growth while maintaining baseline protections. This approach contrasts with China's security-first orientation, creating a different regulatory philosophy that shapes data compliance requirements.

F. Cybersecurity Framework

Malaysia's cybersecurity framework is less prescriptive than China's approach, focusing on risk management rather than comprehensive security mandates. The National Cyber Security Policy provides baseline security expectations, supplemented by sectoral requirements and guidelines issued by regulatory authorities. The National Cyber Security Agency (NACSA) provides security frameworks and guidelines that influence cybersecurity expectations for digital service providers, including e-commerce platforms.

For critical information infrastructure, which may include major e-commerce platforms, additional security requirements apply, including risk assessments and incident reporting obligations. However, these requirements generally adopt a risk-based approach that provides greater flexibility in implementation compared to China's more prescriptive security mandates. This approach reflects Malaysia's broader regulatory philosophy of enabling business operations while maintaining baseline security expectations.

G. Case Study: PrestoMall - Local SME Navigation of Compliance Requirements

PrestoMall (formerly 11street Malaysia) provides an instructive case study of how local small and medium-sized enterprises navigate Malaysia's data compliance framework. As a Malaysian e-commerce marketplace with approximately 250 employees, PrestoMall faces different compliance challenges compared to larger platforms or international operators.

PrestoMall's compliance approach demonstrates the relative flexibility of Malaysia's regulatory framework for smaller operators. The platform implemented a comprehensive privacy notice and consent framework to address PDPA requirements, but reported that implementation required approximately 8% of IT development resources over a 12-month period — significantly lower than comparable compliance burdens reported by Chinese platforms like Ymatou.

Cross-border data transfers represent a core compliance consideration for PrestoMall, as the platform facilitates transactions with international merchants. The platform primarily relies on the consent mechanism for such transfers, integrating appropriate disclosures into its user registration flow. This approach proved more accessible than the technical assessments required under China's framework, allowing PrestoMall to maintain international operations without prohibitive compliance costs.

However, PrestoMall reported challenges with sectoral requirements, particularly those related to payment processing. As the platform expanded into digital payment services, it encountered Bank Negara Malaysia's more stringent data localization requirements, necessitating investment in local infrastructure that represented a significant capital commitment for a company of its size.

This case illustrates the generally more accessible compliance environment created by Malaysia's framework, while highlighting how sectoral requirements still create significant challenges for expanding SMEs. The experience suggests that even Malaysia's more development-oriented approach creates uneven compliance burdens based on enterprise scale, though with generally lower barriers compared to China's security-centered framework.

VI. Comparative Analysis

China and Malaysia have developed distinct approaches to regulating data flows in cross-border e-commerce, reflecting different regulatory philosophies, economic priorities, and geopolitical considerations. This comparative analysis systematically examines the convergences and divergences between these regulatory frameworks across the four critical dimensions, revealing fundamental differences in regulatory approach while identifying potential areas for harmonization.

A. Regulatory Philosophy: Security-Centered versus Development-Centered Approaches

The most significant distinction between China and Malaysia's data compliance frameworks lies in their underlying regulatory philosophies. China has adopted what can be characterized as a security-centered approach, where national security and data sovereignty considerations typically prevail over trade facilitation objectives. As Lu (2022) observes in analyzing China's data localization requirements, this approach prioritizes control over data flows as an expression of digital sovereignty, even when such control may increase compliance burdens for market participants.

In contrast, Malaysia has developed a development-centered approach that balances data protection with digital economy growth objectives. Chan (2022) identifies this development orientation as central to Malaysia's regulatory strategy, with data regulations viewed as enablers of digital economy collaboration rather than primarily as security mechanisms. Malaysia's approach aligns with its strategic positioning as an ASEAN digital hub, as highlighted by Ismail and Masud (2020), who note that Malaysia deliberately calibrates its regulatory frameworks to enhance regional e-commerce connectivity.

B. Data Localization: Comprehensive Mandates versus Sectoral Approaches

China and Malaysia diverge significantly in their approaches to data localization. China has implemented comprehensive localization requirements through its Cybersecurity Law and Data Security Law, requiring storage of personal information and important data within Chinese borders for broad categories of entities. These localization mandates create measurable impacts on cross-border e-commerce operations, functioning as significant non-tariff barriers to digital trade.

Malaysia, by contrast, has adopted a more limited sectoral approach to data localization. The PDPA does not impose general localization requirements, though sectoral regulations create specific localization mandates for certain data categories, particularly in sensitive domains like financial services. This sectoral approach creates a more flexible regulatory environment compared to China's comprehensive localization mandates.

The practical implications of these different approaches are substantial for cross-border e-commerce operators. China's comprehensive localization requirements typically necessitate significant infrastructure investments within China, creating higher compliance costs and operational complexity. Malaysia's sectoral approach permits more distributed data architectures for most operations, while requiring targeted localization for specific data types. This distinction creates fundamentally different operational models for compliant data processing across these jurisdictions.

C. Regional Context: Comparison with Singapore and Indonesia

Placing the China-Malaysia comparison within a broader regional context reveals important patterns in ASEAN data governance approaches. Singapore, often considered the region's digital leader, has adopted what might be termed a "balanced approach" through its Personal Data Protection Act and Model Artificial Intelligence Governance Framework. Singapore's framework emphasizes accountability-based compliance while maintaining flexible transfer mechanisms through a robust adequacy assessment system (Chik, 2023). This approach has positioned Singapore as a digital hub while maintaining robust protection standards.

Indonesia, by contrast, has recently implemented more stringent requirements through Government Regulation 71 concerning Electronic Systems and Transactions, including significant data localization mandates for public service providers (Djafar, 2022). This represents a trend toward digital sovereignty that more closely resembles China's approach, though with less comprehensive security assessment mechanisms for transfers.

Malaysia's approach occupies a middle position in this regional spectrum, with more flexible localization requirements than Indonesia but less comprehensive accountability mechanisms than Singapore. This regional context demonstrates how varied approaches to digital sovereignty have emerged within the ASEAN region, creating a complex compliance landscape for cross-border e-commerce operators.

D. EU Influence: GDPR Impact on Regional Frameworks

The European Union's General Data Protection Regulation (GDPR) has exerted significant influence on data protection frameworks in the region, though with varying intensity. Greenleaf's (2021) comparative analysis finds that Malaysia's Personal Data Protection Act shares approximately 60% of core GDPR principles, reflecting moderate European influence while maintaining distinctive aspects. This influence is evident in Malaysia's rights-based approach and data minimization principles.

China's Personal Information Protection Law demonstrates similar GDPR influence in its structural elements, including consent requirements and individual rights provisions. However, as Bradford (2020) observes, China has adapted these elements within a framework that prioritizes security and sovereignty concerns rather than individual rights protection. This selective adaptation reflects China's distinctive regulatory philosophy while demonstrating the global impact of European regulatory approaches.

This GDPR influence creates partial convergence in formal legal provisions while maintaining fundamental differences in implementation and enforcement priorities. The shared elements potentially facilitate regulatory interoperability in specific domains, creating opportunities for harmonization initiatives focused on these areas of convergence.

E. Cross-Border Data Transfer: Security Assessment versus Adequacy Determination

The mechanisms for lawful cross-border data transfers represent another area of significant divergence. China's framework emphasizes security assessments conducted by regulatory authorities, particularly for transfers of important data or large volumes of personal information. The Personal

Information Protection Law creates a multi-pathway approach with security assessments as the primary mechanism for significant transfers. This ex-ante approval approach creates procedural barriers to routine data transfers, requiring regulatory engagement before cross-border data flows can be established.

Malaysia's framework adopts a different approach centered on either consent mechanisms or adequacy determinations for recipient jurisdictions. Section 129 of the PDPA establishes multiple bases for lawful transfers, including consent, contract necessity, and transfers to jurisdictions with adequate protections. This system does not generally require prior regulatory approval for individual transfers, though it does mandate compliance with either consent requirements or transfers to approved jurisdictions.

The different transfer mechanisms reflect broader regulatory priorities. China's security assessment approach prioritizes governmental oversight and risk mitigation, while Malaysia's consent and adequacy approach emphasizes individual autonomy and jurisdictional equivalence. These different philosophical foundations create distinct compliance pathways for e-commerce operators navigating cross-border data transfers.

F. Differential Impact by Enterprise Scale

The comparative analysis reveals significant differences in compliance burden based on enterprise scale. Case studies of both large enterprises like Alibaba and smaller operators like Ymatou and PrestoMall demonstrate that compliance requirements create disproportionate burdens for small and medium-sized enterprises (SMEs).

In China's regulatory environment, the security assessment requirements for cross-border data transfers create particularly high barriers for SMEs. Ymatou's allocation of 15% of IT resources to compliance matters contrasts sharply with larger platforms that can distribute such costs across broader operations. The technical complexity of security assessments requires specialized expertise often unavailable to smaller operators, creating what Li and Zhang (2023) term a "compliance capability gap" between market participants of different scales.

Malaysia's framework generally creates lower barriers for SMEs, as evidenced by PrestoMall's more manageable compliance costs. However, sectoral requirements still generate significant challenges, particularly as SMEs expand into regulated domains like payment processing. The data localization requirements imposed by Bank Negara Malaysia created substantial capital expenses for PrestoMall, demonstrating how even development-oriented frameworks can impose disproportionate burdens on smaller operators in specific sectors.

This scale-based impact disparity has significant implications for market competition and digital trade inclusivity. As smaller operators face proportionally higher compliance costs, market concentration may increase, potentially undermining broader digital economy growth objectives. The experiences of both Ymatou and PrestoMall highlight the need for scaled compliance pathways that maintain core protections while reducing procedural complexity for smaller market participants.

G. Privacy Protection: Convergent Principles with Divergent Implementation

Privacy protection represents an area of partial convergence between these regulatory frameworks, with both jurisdictions adopting comprehensive personal data protection principles while implementing them through different mechanisms. China's Personal Information Protection Law and Malaysia's Personal Data Protection Act both establish consent-based frameworks with individual rights protections, transparency requirements, and security obligations. Both frameworks create heightened protections for sensitive personal information, though defining these categories somewhat differently.

However, implementation approaches diverge in significant ways. China's consent requirements are generally more stringent, with more limited exceptions compared to Malaysia's broader commercial necessity provisions. China's framework also establishes more comprehensive individual rights, including erasure and portability provisions not fully developed in Malaysia's framework. Most significantly, enforcement intensity differs substantially, with China demonstrating increasing willingness to impose substantial penalties for data protection violations, while Malaysia has historically maintained a more compliance-oriented enforcement approach.

These implementation differences create varying compliance incentives across jurisdictions, with China's more active enforcement environment generally generating stronger compliance prioritization. However, the convergence in fundamental principles creates potential for regulatory interoperability in key domains, potentially facilitating harmonization initiatives focused on these areas of alignment.

H. Cybersecurity: Prescriptive Requirements versus Risk-Based Approaches

Cybersecurity requirements reveal another dimension of regulatory divergence. China has developed a comprehensive cybersecurity framework that includes specific technical requirements, mandatory testing and certification for certain products, and prescriptive security measures for network operators. This approach emphasizes standardized security controls and technological compliance, creating detailed operational requirements for e-commerce platforms.

Malaysia has adopted a more flexible risk-based approach to cybersecurity, establishing broad security principles while permitting greater variation in implementation approaches. While critical infrastructure operators face more specific requirements, most entities have flexibility in implementing security measures appropriate to their risk profile. This approach creates greater adaptability while potentially offering less prescriptive guidance on specific security controls.

These different approaches reflect broader regulatory philosophies, with China prioritizing standardized security measures that enable governmental oversight, while Malaysia emphasizes outcome-oriented approaches that balance security with operational flexibility. For cross-border e-commerce operators, these differences necessitate developing jurisdiction-specific security compliance strategies rather than implementing uniform global approaches.

I. Comparative Analysis with EU GDPR Framework

The EU's General Data Protection Regulation offers a valuable comparative reference point for understanding China and Malaysia's approaches. The GDPR establishes a rights-based framework

centered on individual autonomy, with comprehensive consent requirements, individual rights provisions, and accountability mechanisms. Its cross-border transfer mechanisms emphasize adequacy determinations supplemented by appropriate safeguards, creating a structured approach to international data flows.

China's framework shares certain structural elements with the GDPR, including comprehensive consent requirements and individual rights provisions. However, China's implementation prioritizes security and sovereignty considerations over individual autonomy, creating a fundamentally different regulatory philosophy despite superficial similarities. China's transfer mechanisms emphasize governmental assessment rather than organizational accountability, reflecting this distinct philosophical orientation.

Malaysia's framework demonstrates greater alignment with GDPR principles in its emphasis on consent-based processing and adequacy determinations for transfers. However, Malaysia's implementation provides greater flexibility for commercial applications, reflecting its development-centered approach. Malaysia's framework also lacks the comprehensive accountability mechanisms found in the GDPR, such as mandatory data protection officers and impact assessments for higher-risk processing.

This comparative context demonstrates how different jurisdictions adapt global regulatory trends to reflect distinct priorities and objectives. While certain formal elements show convergence, implementation and enforcement priorities reveal fundamental differences in regulatory philosophy. Understanding these differences is essential for organizations navigating multiple regulatory regimes simultaneously.

VII. Conclusion and Recommendations

This research has conducted a systematic comparative analysis of data compliance frameworks governing cross-border e-commerce in China and Malaysia. The findings reveal fundamental differences in regulatory philosophy, implementation approaches, and compliance requirements across these jurisdictions. These differences create significant operational challenges for cross-border e-commerce platforms while presenting opportunities for regulatory harmonization that could enhance bilateral digital trade.

A. Key Findings

The comparative analysis yields several significant findings regarding the regulatory approaches of China and Malaysia. First, these jurisdictions operate from fundamentally different regulatory philosophies, with China adopting a security-centered approach that prioritizes data sovereignty and national security considerations, while Malaysia implements a development-centered framework that balances protection with digital economy growth objectives. This philosophical divergence shapes specific regulatory requirements across all dimensions analyzed.

Second, data localization approaches differ substantially, with China imposing comprehensive localization mandates through its Cybersecurity Law and Data Security Law, while Malaysia adopts a

more limited sectoral approach targeting specific sensitive data categories. This distinction creates fundamentally different operational architectures for compliant data processing across jurisdictions.

Third, cross-border data transfer mechanisms employ different control approaches, with China emphasizing security assessments conducted by regulatory authorities, particularly for important data and large volumes of personal information, while Malaysia relies primarily on consent mechanisms and adequacy determinations. These procedural differences create substantial variations in operational flexibility for routine cross-border data transfers.

Fourth, while both jurisdictions have established comprehensive personal data protection frameworks, implementation and enforcement approaches diverge significantly. China has demonstrated increasing willingness to impose substantial penalties for data protection violations, while Malaysia has historically maintained a more compliance-oriented enforcement approach. These enforcement differences shape compliance risk assessments and prioritization.

Finally, compliance requirements create disproportionate burdens for small and medium-sized enterprises, with case studies of both Ymatou and PrestoMall demonstrating how regulatory frameworks can generate scale-based impact disparities. This differential impact has significant implications for market competition and digital trade inclusivity, potentially advantaging larger platforms with more substantial compliance resources.

B. Implications for Cross-Border E-commerce

These regulatory differences create substantial implications for cross-border e-commerce operations between China and Malaysia. Foreign investors must develop bifurcated compliance strategies that accommodate both regulatory regimes simultaneously, potentially increasing operational complexity and compliance costs. The divergent approaches to data localization, transfer mechanisms, and security requirements necessitate jurisdiction-specific data architectures rather than integrated global systems.

These regulatory differences function as non-tariff barriers to digital trade, potentially limiting market access particularly for smaller e-commerce operators lacking resources for comprehensive compliance programs. The compliance burden asymmetry potentially advantages larger platforms with resources to maintain separate compliance infrastructures across jurisdictions, creating market concentration effects that may undermine broader digital trade objectives.

However, strategic accommodation opportunities exist through initiatives like Malaysia's Digital Free Trade Zone and bilateral cooperation frameworks. Neilson's (2022) analysis demonstrates how such initiatives can create regulatory experimentation spaces that facilitate cross-border operations while maintaining core protections. Similar initiatives focused specifically on data governance could provide platforms for practical regulatory harmonization.

C. Tiered Compliance Guidelines

Based on this comparative analysis, we propose a tiered compliance guideline framework that addresses the disproportionate impact of regulatory requirements on enterprises of different scales.

This framework maintains core data protection objectives while creating scale-appropriate compliance pathways:

Tier 1: Micro-enterprises (< 50 employees)

- Simplified security assessment requirements focused on essential protection measures
- Template-based standard contracts for cross-border transfers rather than custom assessments
- Consolidated reporting requirements reducing administrative burden
- Technical assistance programs from regulatory authorities

Tier 2: Small and medium enterprises (50-250 employees)

- Modified security assessment processes with standardized methodologies
- Sectoral code of conduct options providing compliance presumptions
- Phased implementation timelines for new requirements
- Collaborative compliance mechanisms allowing resource pooling

Tier 3: Large enterprises (> 250 employees)

- Comprehensive compliance requirements reflecting greater resources
- Detailed security assessment processes for cross-border transfers
- Enhanced documentation and accountability mechanisms
- Leadership expectations including sectoral best practice development

This tiered approach would reduce barriers for smaller market participants while maintaining appropriate protections and oversight. Implementation would require regulatory coordination to create consistent scale-based expectations, potentially through bilateral agreement between Chinese and Malaysian authorities to establish compatible tiered frameworks.

D. Bilateral Data Compliance Mutual Recognition Mechanism

To reduce duplicate compliance burdens for cross-border operators, we recommend the establishment of a bilateral "Data Compliance Mutual Recognition Mechanism" between China and Malaysia. This mechanism would build upon existing cooperation frameworks while creating specific data governance interoperability, including:

1. Mutual recognition of security assessments: Establishing equivalence between China's security assessment process and Malaysia's adequacy determinations for specific data categories and transfer scenarios
2. Harmonized certification standards: Developing compatible certification standards recognized across jurisdictions, reducing duplicate certification requirements
3. Joint enforcement protocols: Creating coordinated enforcement approaches for cross-border violations affecting users in both jurisdictions

4. **Compatible notification requirements**: Aligning breach notification and security incident reporting requirements to reduce duplicative reporting obligations
5. **Standardized contractual mechanisms**: Developing common standard contractual clauses acceptable in both jurisdictions for routine cross-border transfers

This mechanism would significantly reduce compliance costs while maintaining appropriate protections. Implementation could begin with specific sectors such as e-commerce transaction data before potentially expanding to broader categories. The initiative could be developed within the "Five-Pronged Approach" to China-Malaysia cooperation identified by Wang (2023), providing an institutional framework for ongoing regulatory coordination.

E. Recommendations for Foreign Investors

Based on this comparative analysis, several strategic recommendations emerge for foreign investors navigating data compliance requirements in cross-border e-commerce between China and Malaysia:

1. **Develop scale-appropriate compliance strategies**: Smaller operators should consider leveraging established platforms with existing compliance infrastructure rather than building independent systems, while larger operators should develop modular compliance architectures that accommodate different regulatory requirements while maintaining operational integration.
2. **Implement modular data architecture**: Design data processing systems with clearly defined components that can be adapted to different jurisdictional requirements, particularly regarding data storage location, cross-border transfers, and security controls. This approach enables selective compliance with divergent requirements while maintaining overall system coherence.
3. **Establish comprehensive consent frameworks**: Develop user interfaces that obtain necessary permissions for both regulatory regimes simultaneously, incorporating China's more stringent explicit consent requirements alongside Malaysia's broader commercial processing bases. This approach streamlines user experience while ensuring compliance across jurisdictions.
4. **Develop granular data classification systems**: Implement systematic categorization of data based on sensitivity, regulatory requirements, and business necessity. This classification enables appropriate handling of different data types according to varying jurisdictional requirements, particularly for data subject to localization or transfer restrictions.
5. **Engage proactively with regulatory authorities**: Establish early dialogue with regulatory bodies in both jurisdictions when developing new data processing activities, particularly for novel or complex cross-border operations. Proactive engagement can provide regulatory clarity while potentially identifying flexibility within formal requirements.

F. Recommendations for Policymakers

For policymakers seeking enhanced regulatory compatibility, several recommendations emerge:

1. **Develop mutual recognition arrangements**: Establish frameworks for recognizing assessments and certifications across jurisdictions, particularly for security assessments and adequacy

determinations. This approach could reduce duplicative compliance processes while maintaining appropriate protections.

2. **Harmonize sensitive data definitions**: Develop aligned categorizations of sensitive personal information requiring heightened protection, creating greater consistency for cross-border operators while respecting legitimate protection objectives. This harmonization would reduce complexity without compromising core regulatory aims.

3. **Implement coordinated enforcement approaches**: Establish mechanisms for cross-border enforcement cooperation, particularly for significant violations affecting users in both jurisdictions. Such coordination would enhance regulatory effectiveness while providing greater certainty for market participants regarding enforcement priorities and approaches.

4. **Create specialized cross-border data governance frameworks**: Develop bilateral or regional frameworks specifically addressing digital trade data flows, potentially building on existing initiatives like the Digital Free Trade Zone. These specialized frameworks could provide tailored rules for cross-border e-commerce operations while maintaining appropriate protections.

5. **Establish regulatory sandboxes**: Create controlled environments for testing innovative cross-border data governance approaches, allowing for experimentation with different compliance mechanisms while managing potential risks. Such sandboxes could generate evidence-based approaches to regulatory harmonization.

G. Future Research Directions

This comparative analysis highlights several promising areas for future research. First, empirical studies quantifying the compliance costs associated with divergent regulatory requirements would enhance understanding of their practical impact on digital trade. Such research could provide valuable evidence for policymakers considering regulatory harmonization initiatives.

Second, case studies examining successful regulatory navigation strategies by cross-border e-commerce platforms could provide valuable practical insights. Detailed examination of how specific platforms have adapted to different regulatory environments would generate actionable knowledge for market participants facing similar challenges.

Third, investigation of emerging regional data governance frameworks, particularly within ASEAN-China cooperation mechanisms, could illuminate pathways toward greater regulatory harmonization. Analysis of how regional initiatives might bridge national regulatory differences would provide valuable insights for both policymakers and market participants.

H. Conclusion

This research has demonstrated that while China and Malaysia maintain distinct approaches to regulating data flows in cross-border e-commerce, these differences reflect legitimate but divergent regulatory priorities rather than irreconcilable conflicts. China's security-centered approach prioritizes data sovereignty and national security, while Malaysia's development-centered approach emphasizes digital economy growth alongside appropriate protections. These different philosophies create significantly different compliance environments that cross-border e-commerce operators must navigate.

Despite these differences, strategic accommodation and harmonization opportunities exist that could enhance digital trade while respecting each jurisdiction's legitimate regulatory objectives. By implementing tiered compliance guidelines and bilateral mutual recognition mechanisms, both jurisdictions could reduce compliance burdens particularly for smaller market participants while maintaining appropriate protections. Such initiatives would facilitate continued growth in digital trade while preserving core regulatory objectives.

The significance of this research extends beyond academic inquiry into comparative legal frameworks. As cross-border e-commerce continues to grow as a fundamental component of China-Malaysia economic relations, understanding and navigating data compliance requirements becomes increasingly critical for business success and policy development. By identifying both divergences and potential convergences in regulatory approaches, this research contributes to both scholarly understanding and practical guidance in this complex yet essential domain of digital trade governance.

Data Availability Statement

This study is based on analysis of publicly available legal texts, regulations, and scholarly literature. No original dataset was generated during this research. All legislative texts, regulations, and policy documents referenced in this study are publicly accessible through the official government websites and databases cited in the references section. Scholarly articles and reports used in this analysis can be accessed through their respective publishers or open-access repositories as indicated in the reference list.

References

[1] Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

[2] Chan, M. (2022). Malaysia: Digital payments, data regulations, and AI as most promising areas for digital economy collaboration. In The ASEAN Digital Economy (pp. 76-96). Routledge.

[3] Chen, L., & Li, J. (2022). Complying with China's data protection laws: Costs and consequences for digital enterprises. Journal of International Business Studies, 53(5), 1012-1028.

[4] Chen, L., Rillo, A. D., Suhud, Y., & Kasih, M. C. (2023). Further ASEAN-China cooperation for joint prosperity: Envisioning the ACFTA 3.0 in the Digital Era. Economic Research Institute for ASEAN and East Asia.

[5] Chik, W. B. (2023). Singapore's approach to data protection in a digital economy. Data Protection in the Internet, 305-330.

[6] Djafar, W. (2022). Indonesia's evolving approach to data governance: Between economic opportunity and digital sovereignty. Journal of Current Southeast Asian Affairs, 41(1), 57-80.

[7] Ferracane, M. F., & van der Marel, E. (2021). Regulations on personal data: Differing data realms and digital services trade. World Trade Review, 20(5), 1-25.

[8] General Administration of Customs of China. (2023). China-Malaysia trade statistics. http://stats.customs.gov.cn/

[9] Greenleaf, G. (2021). Global Tables of Data Privacy Laws and Bills (7th Ed). Privacy Laws & Business International Report, 169, 1-20.

[10] Ismail, N. A., & Masud, M. M. (2020). Prospects and challenges in improving e-commerce connectivity in Malaysia. E-commerce Connectivity in ASEAN, 78-96.

[11] Li, W., & Zhang, R. (2023). The compliance capability gap: How firm size shapes regulatory burden in China's digital economy. Journal of International Business Policy, 6(2), 219-236.

[12] Lu, W. (2022). Data localization: From China and beyond. Indiana Journal of Global Legal Studies, 29(1), 183-211.

[13] Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2023). Protection of personal data in the context of e-commerce. Journal of Cybersecurity and Privacy, 3(2), 731-761.

[14] Neilson, B. (2022). Working the digital silk road: Alibaba's digital free trade zone in Malaysia. Environment and Planning A: Economy and Space, 54(1), 138-155.

[15] Wang, L. (2023). China-Malaysia e-commerce co-operation under the "Five-Pronged Approach". Malaysian Journal of Chinese Studies, 12(1), 1-18.

[16] Wu, Y., Zhou, Y., & Li, G. (2022). Barriers to digital trade: A systematic review of regulatory impacts on cross-border e-commerce. Journal of International Marketing, 30(2), 83-102.

[17] Zhang, Y. (2023). China's evolving approach to data sovereignty and cross-border data flows. International Journal of Law and Information Technology, 31(2), 167-193.