TOWARDS A DATA-DRIVEN FUTURE - FOSTERING THE FLOW OF PERSONAL DATA BETWEEN ASEAN COUNTRIES AND THE EUROPEAN UNION

NGUYEN THAI CUONG
Institute of Comparative Law, Ho Chi Minh City University of Law, Vietnam
Email: ntcuong@hcmulaw.edu.vn
LE HUYNH MAI TAM, NGUYEN HOANG MINH CHAU
Ho Chi Minh City University of Law, Vietnam
Email: lehuynhmaitam@gmail.com; chau.nguyen@ngo-partners.com

Abstract

In the period of opening a new chapter of Association of Southeast Asian Nations (ASEAN) and the European Union (EU) relations, the issue of digital transition and economic cooperation is mentioned as a special concern. Transferring the cross-border flow of personal data is the key to growing the digital economy. However, differences in personal data protection regulations between the ASEAN and the EU pose challenges to the cooperation and economic development of the two blocs. This article undertakes a comparative legal analysis of existing personal data protection regulations in the EU and selected ASEAN countries: Singapore, Indonesia, and Vietnam, highlighting their respective approaches to cross-border data transfers. The article identifies aspects of normative uncertainty and legal fragmentation that may hinder data mobility and digital cooperation between the two blocs. Based on this comparative overview, the article outlines preliminary considerations for improving regulatory alignment in a manner that facilitates secure and lawful data flows while respecting regional legal diversity.

Keywords: *ASEAN-EU, cross-border data transfers, data governance, harmonization of regulations, personal data flow*

Received: 28 April 2025 Revised: 17 May 2025 Accepted: 17 June 2025

"Personal data" is a term that has garnered much global discussion as it is the "fuel" for economic development in the digital age. Nearly all economic activities that involve the application of the internet depend on the collection, transfer, and processing of customer data, personal information, consumer information, and business information.[1] Cross-border personal data flows impact the entire process of conducting international business transactions, especially in digital environments.[2] It allows businesses to participate in global supply chains and access foreign markets. Thus, the cross-border personal data flows not only aim to enhance connectivity but also serve as a crucial key in the digital economy era, allowing countries to unlock development opportunities and achieve new milestones.

1 Dung, T. V. & Cong, L. T. Q. (2025). Trách nhiệm của chủ thể quản lý nền tảng kỹ thuật số (Platforms) – Kinh nghiệm của EU. Trong Đ. V. Đại & B. Hégédus (Chủ biên), *Kỷ yếu hội thảo: Bảo vệ dữ liệu cá nhân trong môi trường số* (tr. 204–235). Nhà xuất bản Đại học Quốc gia TP. Hồ Chí Minh [trans: Tran, V. D., & Le, T. Q. C. (2025). Responsibilities of digital platform operators – EU experiences. In V. D. Do & B. Hégédus (Eds.), *Proceedings of the Conference: Personal Data Protection in the Digital Environment* (pp. 204–235). Vietnam National University Publishing House]

2 Phuong, N. L. & Dong, N. Q. (2022). Bảo vệ dữ liệu cá nhân xuyên biên giới: Thực tiễn và kiến nghị hoàn thiện pháp luật Việt Nam. *Tạp chí Quản lý và Kinh tế quốc tế* [trans: Protecting personal data across borders: Practices and recommendations to improve Vietnamese law. *Journal of International Economics and Management*], (149), p. 77-91.

The Association of Southeast Asian Nations (ASEAN)'s cross-border personal data transfer is growing rapidly. The digital economy is the primary driver of growth in the region.[3] As business activities shift online and data grows exponentially, reliance on data centres to power the digital economy increases.[4] ASEAN stands at a critical juncture in the development and integration of its digital economy, which is estimated to contribute approximately 1 trillion US dollars in Gross Merchandise Value (GMV) by 2030,[5] making regulations on data transfers crucial for its development. At the same time, ASEAN-EU relations have strengthened as strategic partners, reaffirmed in the Joint Leaders' Statement on 14 December 2022, emphasizing a peaceful, stable, and prosperous region, respect for international law, and promotion of human rights, including personal data protetion. With ASEAN is the European Union (EU)'s third-largest trading partner and the EU is ASEAN's second-largest investor[6] cross-border data flows are expected to grow. However, both regions are confronted with certain challenges in managing cross-border personal data flows. Therefore, researching and refining legal frameworks on this issue between the two regions will help promote the development of cross-border personal data flows, advancing towards a data-driven future and achieving sustainable development goals set by both sides.

1. Regulations on personal data transfer in the European Union

The General Data Protection Regulation (GDPR) is widely regarded as a pioneering and comprehensive data protection law, serving as a model for similar regulations globally.[7] Replacing the 1995 Data Protection Directive (95/46/EC), it aims to safeguard EU citizens' privacy while allowing the free flow of personal data within the EU.[8] For data transfers outside the EU, GDPR requires that the level of protection remains equivalent to that within the EU. To lawfully transfer personal data abroad, data controllers and processors must meet one of the mechanisms provided: adequacy decisions, appropriate safeguards, or derogations.

3 Google, Temasek & Bain&Company (2023). E-Conomy SEA 2023. *Google*. https://economysea.withgoogle.com/intl/ALL_vn/report/

4 Singapore's Infocomm Media Development Authority (IMDA) & InformaTech (2022, June 1). *Charting ASEAN's Digital Future: Emerging Policy Challenges* [Reports and Conference Highlights]. Singapore Institute of International Affairs, p. 4. https://siiaonline.org/charting-aseans-digital-future-emerging-policy-challenges/

5 Association of Southeast Asian Nations (ASEAN) and European Commission (2024). *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. ASEAN Secretariat, p. 3. https://asean.org/wp-content/uploads/2024/02/Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf

6 Association of Southeast Asian Nations (ASEAN) and European Commission (2024), *supra* note 5, p. 5.

7 Geradin, D., Karanikioti, T. & Katsifis, D. (2021). GDPR Myopia: How a well-intended regulation ended up favoring large online platforms-the case of ad tech. *European Competition Journal*, *17*(1), p. 47-92. https://doi.org/10.1080/17441056.2020.1848059; Taylor, M. (2012, April). *Genetic data and the law: A critical perspective on privacy protection*, Cambridge University Press. https://doi.org/10.1017/CBO9780511910128; Ryngaert, C. & Taylor, M. (2020, January 06). The GDPR as Global Data Protection Regulation?. *American Journal of International Law, 114*, 5–9. https://doi.org/10.1017/aju.2019.80

8 On 14 November 2018, the European Parliament and the Council of the EU approved a legislative reform banning data localization restrictions. The Regulation (EU) 2018/1807, published in the Official Journal of the European Union on November 28, 2018 and therefore applicable in all EU Member States as of May 2019.

First, regarding adequacy decisions, when transferring personal data, the first step is to consider whether that country has been granted an adequacy decision under Article 45 GDPR. An adequacy decision is a determination by the European Commission that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection for personal data.[9] In essence, the European Commission adopts an adequacy decision based on two main elements: (i) the content of the rules applied and (ii) the means used to ensure that the application of those rules in the third country or international organization guarantees a level of protection essentially equivalent to that guaranteed in the Union.[10] Once a third country or international organization has this kind of decision, personal data may be transferred to that location without any further approval.[11] If the Commission decides to withdraw an adequacy decision that has been granted, it shall notify the third country or international organization and give the reasons for its decision.[12] As of the end of June 2024, no country in ASEAN has been recognized as having provided adequate decisions under GDPR.[13]

Second, in the absence of adequacy decisions, appropriate safeguards can be applied.[14] These safeguards require approval from the supervisory authority, either in advance or on a case-by-case basis. Having adequacy decisions depends on the regulations of a third country, as it must be found to have a level of data protection essentially equivalent to that guaranteed in the EU.[15] In practice, businesses often rely on appropriate safeguards - especially standard contractual clauses (SCCs) and binding corporate rules (BCRs) - as the primary tools for cross-border data transfers.[16]

SCCs are model data protection clauses that have been pre-approved by the European Commission.[17] According to the International Association of Privacy Professionals – Ernst & Young Annual Privacy Governance Report 2019, SCCs are one of the most commonly used methods for transferring personal data to third countries outside the EU.[18] The use of SCCs requires a

9 Article 45. (1) of the GDPR.
10 Article 45. (2) of the GDPR; Wilderoth, S. (2019), *EU data transfer requirements for an adequacy decision and the Vietnamese legal realities* [Graduate Thesis]. Lund University, p. 32-64. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9000444&fileOId=9003963
11 Ibid., *supra* note 10.
12 Intersoft Consulting (2016, April 27). Recital 103: Appropriate Level of Data Protection Based on an Adequacy Decision. In *Recital*. https://gdpr-info.eu/recitals/no-103/
13 For a list of countries that have been granted Adequacy decisions can be found at: Euro Commission. (2025). *Adequacy decisions*. Euro Commission. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
14 Article 46. (1) of the GDPR.
15 Case 362/14 *Maximillian Schrems v Data Protection Commissioner*, Digital Rights Ireland Ltd. [2015] EU:C:2015:650 (Schrems case), para 74 & 96.
16 Article 46. (2). (b), (c) of the GDPR.
17 Article 46.2(c), (d) of the GDPR.
18 Euro Commission. (2021). *New Standard Contractual Clauses - Questions and answers overview - frequently asked questions on the new SCCs*. Euro Commission. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-

legally binding agreement between the data exporter and importer, setting out contractual obligations to ensure that EU data subjects' rights are protected during and after the transfer outside the EU. SCCs include general clauses applicable in all situations and four modules tailored to different transfer scenarios.[19] Notably, if parties modify the general clauses of the SCCs, the altered terms cannot serve as a basis for data transfers to third countries,[20] unless approved by a national data protection authority as a "special provision".[21] SCCs were initially based on the 1995 Data Protection Directive (95/46/EC), but this framework was challenged in the 2020 Schrems II case.[22] In this case, Maximilian Schrems argued that Facebook's data transfers to the United States (US) could be accessed by US intelligence, violating EU privacy laws. The Court of Justice of the EU agreed, invalidating the EU-US Privacy Shield framework based on SCCs. Then the EU adopted updated SCCs in 2021, aligning them with the GDPR and requiring additional safeguards to protect personal data. Businesses can still use existing SCCs but must now assess each transfer individually to ensure it meets EU's level protection. This requires conducting a risk assessment and implementing additional safeguards where necessary, including access restrictions or suspension of the transfer.[23]

BCRs are internal policies within a multinational corporation[24] that govern the cross-border transfer of data by its subsidiaries.[25] Each corporation designs its own BCRs to ensure all branches comply with GDPR.[26] These BCRs must be approved by an EU supervisory authority in a member state where the company is established.[27] The rigorous approval process ensures the BCRs meet GDPR's high protection standards. Once approved by an EU supervisory authority, the BCRs are legally binding, and the corporation can use the rules to transfer personal data outside the EU without the need for any further authorizations.[28]

Third, under GDPR, when adequacy decisions or appropriate safeguards are not feasible, Article 49 allows derogations. Such derogations include:

answers-overview_en

19 Directorate-General for Justice and Consumers (2021, June4). *Publications on the Standard Contractual Clauses (SCCs)*. Euro Commission. https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

20 Directorate-General for Justice and Consumers (2021, June4), *supra* note 20.

21 Article 46. (3). (a) of the GDPR.

22 Riswandi, B. A. & Gultom, A. M. (2023). Protecting our mosts valuable personal data: A comparison of transborder data flow laws in the European Union, United Kingdom, and Indonesia. *Prophetic Law Review*, *5*(2), 179-206. https://doi.org/10.20885/PLR.vol5.iss2.art3

23 "New Standard Contractual Clauses - Questions and Answers overview - Frequently asked questions on the new SCCs", *supra* note 20.

24 This may be a corporate group, or a group of undertakings or enterprises engaged in a joint economic activity, such as franchises or joint ventures.

25 Article 47 of the GDPR.

26 Article 47(2) and 47(3) G of the DPR.

27 Information Commissioner's Office (2018). *Guide to the General Data Protection Regulation (GDPR)*, p. 246. https://archive.comsuregroup.com/wp-content/uploads/2018/01/Guide-to-the-General-Data-Protection-Regulation-GDPR-_-ICO.pdf

28 Article 47(1) of the GDPR.

(i) explicit consent of the data subject, fully informed of risks; (ii) contract performance involving the data subject; (iii) important public interests; (iv) legal claims or proceedings; (v) protection of vital interests of the data subject or another person where the data subject is incapable of giving consent (e.g., medical emergencies); and (vi) data transfers from public registers designed for public information access might be allowed.[29] These derogations require justification and should be considered only after efforts to establish adequate safeguards or utilize an adequacy decision have been exhausted.[30] Transfers under derogations may occur more than once but must be occasional, limited in scope, and include appropriate safeguards to protect data.[31] Organizations are required to notify the relevant supervisory authority whenever they use these derogations and must provide additional information to individuals affected by such transfers.[32]

The EU's legal framework adopts a "prior safe harbor" approach, facilitating cross-border data transfers while ensuring high protection standards. In addition, GDPR has an extraterritorial effect in the context that there is no harmonization of personal data protection laws on an international level.[33] Therefore, GDPR imposes data protection standards on all businesses that process the data of EU citizens in order to provide optimal security and to enhance trust and transparency in the context of the complex flow of personal data around the world.

2. The legal framework of the Association of Southeast Asian Nations countries on cross-border personal data transfers

2.1. Regulations on cross-border personal data transfers in selected Association of Southeast Asian Nations countries

Although ASEAN has made considerable efforts to establish a harmonized legal environment for personal data protection, the current regional legal framework remains fragmented and lacks binding force. This fragmented situation underscores the challenge ASEAN faces in reconciling national sovereignty with the regional imperative of harmonizing data governance frameworks. In this context, the article adopts a comparative country-level approach to examine the evolution of legal frameworks governing cross-border personal data transfers in three ASEAN countries: Singapore, Indonesia, and Vietnam. These jurisdictions are selected based on their markedly

29 Article 49(1) of the GDPR stipulates 7 specific cases of Derogations from clause a to clause g, however, due to the similar nature of clauses b and c of this Article - which all serve the performance of the contract, the authors only mention 6 main cases in this article.

30 European Data Protection Board (2018). *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*. European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

31 Article 49(1) of the GDPR.

32 Article 49(1), (6) of the GDPR.

33 Voss, W. G. (2019). Cross-border data flows, GDPR, and data governance. *Washington International Law Journal, 29*(3), 485, p. 503. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7/

different levels of legal maturity and regulatory readiness. Singapore, the region's strongest digital economy,[34] is a pioneer in personal data protection.[35] Its Personal Data Protection Act (PDPA), enacted in 2012 and amended in 2020, reflects its adaptability to innovation and the digital landscape. As ASEAN's largest digital economy and a major online market,[36] Indonesia offers a key example of how emerging legal systems address cross-border data flows. The Indonesian Personal Data Protection Law (Indonesian PDPL) reflects efforts to regulate personal data amid rapid digital and e-commerce growth. Vietnam, one of East Asia's most dynamic emerging economies,[37] is undergoing a significant legal shift from decree-based to statute-based data protection. For Vietnam, the 2024 Data Law and 2025 Personal Data Protection Law reflect a stronger and more formal commitment to privacy and personal data protection, offering a progressive perspective on regional data governance trends.

2.1.1. Cross-border data transfers under Singapore's Personal Data Protection Act

The regulation of cross-border personal data transfers in Singapore[38] is based on an accountability approach.[39] Accordingly, data controllers must take appropriate steps to ensure that personal data transferred outside Singapore receives protection equivalent to the PDPA's standards. This equivalent protection is demonstrated in one of two forms: legally enforceable obligations or specified certifications. This aspect of the PDPA resembles the EU's GDPR. However, while GDPR requires the equivalent level of protection to be assessed by the European Commission, which grants adequacy decisions to the recipient country or organization, the PDPA mandates that data controllers independently undertake appropriate steps for evaluation without requiring written approval from a competent authority. This provision in Singapore mirrors GDPR's appropriate safeguards, but differs in that the PDPA does not require initial approval from a supervisory authority. The PDPA allows data controllers to independently evaluate and transfer data without needing specific approval from an authority. However, data controllers remain accountable in the event of a breach. Additionally, Singapore aligns with GDPR by providing five exceptions wherein data controllers are not required to undertake the above-mentioned appropriate steps before transferring personal data.

34 EDB Singapore (2024). *A stable and trusted hub to access Asia's growth markets*. A Singapore Government Agency Website. https://www.edb.gov.sg/en/why-singapore/an-economic-powerhouse.html

35 Liu, J., Sengstschmid, U., & Ge, Y. (2023, August 22), "Facilitating Data Flows Across ASEAN: Challenges and Policy Directions", *ACI Research Paper, 19*, p. 1. http://dx.doi.org/10.2139/ssrn.4547683

36 Nurhayati-Wolff, H. (2021, December 12). *Number of internet users in Indonesia from 2017 to 2022 with forecasts until 2028*. Statista. https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia

37 World Bank Group (2024, April). *The World Bank In Viet Nam*. World Bank Group. https://www.worldbank.org/en/country/vietnam/overview

38 Personal Data Protection Act 2012 – 2020 Revised Edition. https://sso.agc.gov.sg/Act/PDPA2012

39 Phuong & Dong (2022), *supra* note 2, p. 83.

By granting significant autonomy to data controllers, the PDPA facilitates smoother data transfers without the need for authority approval for each specific transaction. Furthermore, the exceptions are a crucial element in promoting cross-border data flows, demonstrating flexibility to accommodate necessary and urgent situations, thus benefiting businesses engaged in international trade.

2.1.2. Cross-border data transfers under Indonesia's Personal Data Protection Law

Indonesia passed the Indonesian PDPL 2022[40] to provide general rules for the processing of personal data in both the online and offline environments.[41] Similar to GDPR, Indonesian PDPL has an extraterritorial effect, applying to any individual, entity, or organization processing the personal data of Indonesian citizens, regardless of location.[42] Under Indonesian PDPL, cross-border data transfers are permitted where one of three conditions is met: (i) the recipient country provides a level of protection equal to or higher than Indonesian PDPL,[43] (ii) where such protection is lacking, legally binding safeguards must be implemented through contracts or equivalent instruments, (iii) if neither condition is met, the controller must obtain the data subject's consent, allowing transfers without further consideration of the recipient country's protection level.[44]

In addition to Indonesian PDPL's general provisions, Indonesia maintains sector-specific regulations. Indonesian PDPL draws heavily from GDPR, reflecting comparable principles. The requirement for equivalent protection parallels GDPR's adequacy adecisions, while the mandate for binding safeguards mirrors its appropriate safeguards. Indonesia's reliance on data subject consent resembles GDPR's Derogations, but with broader application, as it imposes fewer transparency obligations.

2.1.3. Cross-border data transfers under Vietnamese law

The enactment of the 2024 Data Law and the 2025 Vietnamese PDPL, has fundamentally transformed Vietnam's data protection landscape, replacing the previous decree-based framework under Decree No. 13/2023/ND-CP[45] to jointly regulate cross-border personal data transfers, under which enterprises must comply with both laws.

The 2024 Data Law regulates all digital data, categorizing "core data"[46] and "important data".[47] Article 23 allows free cross-border data transfer, provided that it complies with Vietnamese law and international treaties. However, transferring core/important data abroad requires strict conditions

40 Undang-undang (UU) Nomor 27 Tahun 2022 - Pelindungan Data Pribadi [trans: The Personal Data Protection Law]. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

41 Unlike previous regulations that focused solely on personal data processed through electronic systems.

42 Article 2 of the Indonesian PDPL.

43 Article 56(2) of the Indonesian PDPL.

44 Article 56(4) of the Indonesian PDPL.

45 Nghị định số 13/2023/NĐ-CP của Chính phủ: Bảo vệ dữ liệu cá nhân [trans: Decree no.13/2023/NĐ-CP]. https://vanban.chinhphu.vn/?pageid=27160&docid=207759

46 Article 3(5) of the 2024 Data Law.

47 Article 3(6) of the 2024 Data Law.

with a "prior-review" mechanism, which means data owners and controllers must conduct a Transfer Impact Assessment (TIA) themselves in accordance with Form No. 02 in the Decree No. 165/2025/ND-CP. This should only be done once for an organization's operational duration, with updates as required.[48] The TIA report should include: (i) legality, necessity, scope, and method of data transfer and recipient's processing; (ii) risks to national security, economy, foreign relations, social stability, public interest, or individual/organizational rights, including data falsification, destruction, leakage, loss, or unlawful use; (iii) recipient's responsibilities, obligations, and technical measures; and (iv) other relevant issues.[49]

Meanwhile, the Vietnamese 2025 PDPL focuses on personal data, categorized as "basic data" [50] and "sensitive data", [51] emphasizing the consent of the individual. It adopts a flexible "post-audit" mechanism, allowing cross-border personal data transfers if enterprises:[52] (i) prepare a Data Processing Impact Assessment (DPIA) covering data type, receiving country, protections, and risks; (ii) submit the DPIA within 60 days of the first transfer; and (iii) align with the data subject's consented purpose.[53] The law removes complex prior-reviews, reducing burdens but mandating self-compliance. Certain cases, like public service data transfers, cloud-stored employee data, or individual self-transfers, are exempt from DPIA requirements.[54] Notably, although the Vietnamese PDPL inherits from Decree 13/2023/NĐ-CP and continues to abolish the requirement for storing personal data in Vietnam for cross-border transfers, Articles 26 and 27 of Decree 53/2022/NĐ-CP – guiding Article 26 of Cybersecurity Law No. 24/2018/QH14 – remain in effect. Accordingly, domestic and foreign enterprises providing telecommunications, Internet, or value-added cyberspace services in Vietnam that collect, exploit, analyze, or process the following data must store it in Vietnam for at least 24 months: (i) personal information of service users in Vietnam; (ii) data generated by such users; and (iii) data on their relationships. Additionally, foreign enterprises in specified fields under Article 26(3)(a) must establish a branch or representative office in Vietnam for data storage purposes. Regarding inspection and penalties, the 2024 Data Law relies mainly on risk reports and indirect inspections, with penalties awaiting detailed decrees. In contrast, the 2025 PDPL sets out clearer mechanisms: periodic (once per year) and surprise inspections (in

48 Article 12(1), (8) of the Decree 165/2025/ND-CP; Nghị định số 165/2025/NĐ-CP của Chính phủ quy định chi tiết một số điều và biện pháp thi hành luật dữ liệu [trans: Decree 165/2025/ND-CP of the Government detailing a number of articles and measures for the implementation of the Law on Data]. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-165-2025-ND-CP-huong-dan-Luat-Du-lieu-663547.aspx

49 Article 12(2), (8) Decree 165/2025/ND-CP.

50 Article 2(3) of the Vietnamese PDPL.

51 Article 2(4) of the Vietnamese PDPL.

52 Article 20 of the Vietnamese PDPL.

53 Article 17 of the Vietnamese PDPL.

54 Article 20(6) of the Vietnamese PDPL.

case of violations or breaches).[55] The Vietnamese PDPL also provides clear sanctions: administrative fines up to 5% of annual revenue or 3 billion VND (or 10 times the revenue gained), remedial measures, and criminal liability for serious breaches such as large-scale data leaks.[56]

These legislative developments mark a pivotal shift from a fragmented decree-based system to a dual statutory framework, emphasizing self-responsibility, consent, and national security while easing bureaucratic hurdles. Vietnam has also adopted a more permissive approach, allowing exemptions for cross-border data transfers and aligning more closely with frameworks like the GDPR, Singapore PDPA, and Indonesian PDPL. Key reforms include: (i) clearer data classification to guide transfer restrictions; (ii) a shift to prior-review TIA for core/important data and post-audit DPIA submissions (within 60 days) for personal data, eliminating complex pre-approvals; (iii) reliance on domestic conditions, exemptions, and inspections rather than "adequacy decisions" in GDPR or Singapore's PDPA; and (iv) removal of routine post-transfer notices (like to Ministry of Public Security as requested in Decree No. 13/2023/ND-CP). However, this dual-law regime creates complexity as businesses must balance national security mandates under the 2024 Data Law with privacy obligations under the 2025 PDPL, while Decree No. 53/2022/ND-CP's 24-month data localization requirement for certain types of data[57] continues to add compliance burdens.

2.2. The Association of Southeast Asian Nations' regional regulations to promote cross-border personal data transfers

Inconsistency is a salient feature of cross-border personal data transfer regulations in the ASEAN, where each member state applies its own legal framework. Moreover, the uneven development of legal systems among countries further highlights this disparity. Singapore is widely recognized as the regional leader in personal data protection, while Indonesia and Vietnam have recently enacted laws reflecting digital transformation. Meanwhile, countries like Cambodia and Laos lack comprehensive legal frameworks, leaving cross-border data transfers largely unregulated. Consequently, ASEAN is considered by many scholars to be a region particularly susceptible to external policy influences due to its relatively less developed legal framework[58] and the absence of any binding regional standards.[59] In response to this fragmentation, ASEAN has

55 Article 20(4) of the Vietnamese PDPL.
56 Article 8 of the Vietnamese PDPL.
57 Liu, H.-W. (2018). Data localization and digital trade barriers: ASEAN in megaregionalism. In P. L. Hsieh & B. Mercurio (Eds.) (2019). ASEAN law in the new regional economic order: Global trends and shifting paradigms. Cambridge University Press. https://ssrn.com/abstract=3367929.
58 Although Decree 13/2023/ND-CP, once officially issued, removed the requirement for personal data to be stored in Vietnam in cases of cross-border transfers. However, Articles 26 and 27 of the Decree 53/2022/ND-CP, which provide guidance on Article 26 of the Law on Cybersecurity no. 24/2018/QH1, are still in effect. Therefore, in certain cases mentioned above, Vietnam still imposes data localization requirements.
59 Burri, M. (2022). Approaches to digital trade and data flow regulation across jurisdictions: implications for the future ASEAN-EU agreement. *Legal Issues of Economic Integration*, *49*(2), 149–168.

introduced several regional instruments to promote regulatory harmonization:

The 2016 ASEAN Framework on Personal Data Protection (PDP), inspired by the 1980 Organisation for Economic Co-operation and Development principles and the 2004 Asia-Pacific Economic Cooperation principles, set out general requirements for cross-border data transfers: the consent of the individual for the overseas transfer or taking reasonable steps to ensure the recipient offers comparable protection. The PDP merely sets out general principles without providing any enforcement mechanism. In 2021, the ASEAN Data Management Framework (DMF) and the ASEAN Model Contractual Clauses (MCCs) are approved.[60] The MCCs were designed as a voluntary standard to provide guidance on baseline considerations for transferring personal data; encourage businesses to review ASEAN Member States (AMS) laws to ensure compliance with specific AMS requirements.[61] This implies that adopting the MCCs does not automatically guarantee compliance with the AMS personal data transfer regulations. The MCCs provide a contractual framework for data protection but have not been uniformly adopted across all AMS. These instruments are primarily soft law, which limits their enforceability and practical impact. While providing a useful foundation for cross-border personal data transfers, they face several key limitations:

First, the instruments lack legally binding force and set relatively low protection standards, which, combined with limited adoption, render their impact largely theoretical. As voluntary guidelines, they impose no mandatory obligations on businesses, relying on discretionary compliance, which weakens their practical effectiveness. Compared to stricter regimes like the EU's GDPR – featuring binding obligations and accountability measures – ASEAN's frameworks remain largely incompatible with international standards, limiting their utility in cross-border data transfers involving jurisdictions with stronger protections. For example, only Singapore actively promotes the MCCs and has issued implementation guidelines. In contrast, Indonesia and Vietnam, despite enacting personal data protection laws after these ASEAN instruments were introduced, do not reference them in their legislation.

Second, conceptual inconsistencies create legal uncertainty. Although the MCCs derive from the PDP, they impose an additional requirement: data exporters must comply with applicable AMS laws. This diverges from the PDP's general principle of ensuring protection "consistent with these Principles",[62] leading to confusion over whether businesses must follow ASEAN principles, national laws, or both.

60 ASEAN Secretariat (2025). *ASEAN digital masterplan 2025*. Association of Southeast Asian Nations. https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf

61 ASEAN (202, January). *ASEAN model contractual clauses for cross border data flows*. Final Copy Endorsed by the 2nd ASEAN Digital Senior Officials' Meeting (ADGSOM), p. 5. https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

62 Article 6(f) of the PDP.

3. Challenges in the diverse legal frameworks of the Association of Southeast Asian Nations - European Union

Both ASEAN and the EU recognize the importance of protecting personal data and aim to promote cross-border data flows for digital economic development. There are significant organizational structures and power differences between the representative bodies of ASEAN and the EU. Specifically, the EU has central agencies with legislative and enforcement powers binding on all Member States, resulting in a more unified legal system with stronger enforcement capabilities.[63] ASEAN focuses on cooperation and coordination among its Member States, lacking a unified legislative or enforcement body. Member States retain autonomy in enacting laws and national policies.[64] This leads to substantial differences, particularly in the degree of legal harmonization within the region.

The EU achieves a high degree of regulatory coherence, as GDPR is directly applicable across all Member States. In contrast, ASEAN exhibits lower legal harmonization due to each Member State having its own data protection laws, resulting in regulatory differences (as analyzed above). The significant legal disparities among ASEAN countries complicate and increase costs for businesses engaged in data transfers. In ASEAN, micro, small, and medium enterprises (MSMEs) constitute a significant proportion of businesses and are considered the backbone of the region, contributing significantly to economic growth of AMS.[65] MSMEs face significant difficulties in complying with personal data protection regulations, primarily due to limited financial resources and a lack of legal expertise. The regulatory divergence between ASEAN and the EU in cross-border data transfer further intensifies these challenges by increasing compliance costs, creating legal uncertainty, and placing a heavier operational burden on MSMEs, thereby restricting their capacity for innovation. Identifying and complying with diverse regulations can be complex, potentially causing businesses to unintentionally breach laws without awareness.

4. Between flexibility and rigidity: The Association of Southeast Asian Nations and the European Union model contract clauses

MCCs and SCCs are designed as adaptable templates to suit the practical operational contexts of individual enterprises. Recognizing the potential of MCCs and SCCs to facilitate bidirectional data flows, ASEAN and the EU jointly issued the "Joint Guide to ASEAN Model Contractual Clauses and EU

63 European Union (n.d.). *How EU policy is decided*. European Union. https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en

64 ASEAN Secretariat (n.d.). *What We Do*. Association of Southeast Asian Nations. https://asean.org/what-we-do/

65 ASEAN Secretariat (n.d.). *Overview - ASEAN Main Portal*. Association of Southeast Asian Nations. https://asean.org/our-communities/economic-community/resilient-and-inclusive-asean/development-of-micro-small-and-medium-enterprises-in-asean-msme/overview/

Standard Contractual Clauses" in 2023.[66] This document not only helps cross-bloc businesses understand the similarities and differences between the two legal tools but also supports simultaneous compliance with both personal data protection systems. It signifies a concrete step towards reinforcing ASEAN's efforts and reflects the shared commitment of both blocs to enhancing data governance through the adoption of international best practices.[67] However, both MCCs and SCCs originate from vastly different legal systems, reflecting contrasting views on privacy rights, legal structures, and enforcement capabilities. The following analysis compares two key aspects of these tools.

First, regarding the legal basis, binding nature and customizability, SCCs are built upon the robust legal framework of GDPR, holding binding effects across EU Member States. Their use for cross-border data transfers is explicitly recognized in GDPR, inherently carrying legal binding force for businesses. Additionally, SCCs are clearly and uniformly designed, facilitating and optimizing their application across the EU without the need to consider individual national regulations. In contrast, MCCs are based on ASEAN's personal data protection framework, which lacks binding legal effect across the entire ASEAN region. Currently, Singapore is the only ASEAN country that explicitly recognizes MCCs as a tool for transferring personal data out of its jurisdiction. In terms of customizability, SCCs feature four data transfer modules, enabling flexible use. MCCs are limited to two modules: one for Controller-to-Processor transfers and another for Controller-to-Controller transfers.[68] In many instances, the clauses fail to adequately clarify the distinct roles of controllers and processors, thereby limiting their applicability in complex data supply chains.

Second, regarding practicality, compliance costs, and protection of data subject rights, SCCs are "ready-to-use" standardized templates. Businesses only need to fill in specific information and can implement them immediately without complex customization or in-depth legal consultation. In contrast, when transferring personal data of AMS citizens across borders using MCCs, businesses must consider several issues. To be more specific, MCCs require more intricate adjustments to meet national regulations. Businesses must include all necessary clauses in MCCs contracts, excluding those marked as "Choose the relevant clause", and adjust them to comply with national and

66 Portnoy, A. & Nauwelaerts, W. (2023). *Joint regulatory guidance aims to help companies transfer personal data across ASEAN and eu member states*. Alston & Bird. https://www.alstonprivacy.com/joint-regulatory-guidance-aims-to-help-companies-transfer-personal-data-across-asean-and-eu-member-states/

67 Citing H.E. Dr. Kao Kim Hourn (Secretary-General of ASEAN). In Association of Southeast Asian Nations (ASEAN) and European Commission. (2024, January 31). *Joint Guide to ASEAN model contractual clauses and EU standard contractual clauses*. ASEAN, p. 3. https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf

68 Greenleaf, G. (2021). ASEAN model contractual clauses: Low and ambiguous data privacy standards. *Privacy Laws & Business International Report*, *174* (22-24). University of New South Wales Law Research Series, No. 21-83. https://dx.doi.org/10.2139/ssrn.4027670

local regulations.[69] The absence of a unified legal system like GDPR requires businesses to assess the legality of MCCs in each country, a costly and error-prone process, especially for MSMEs with limited resources. Meanwhile, SCCs clearly embody a rights-based approach, with binding obligations on notification, complaints, access, rectification, and compensation for data subjects.[70] MCCs exhibit flexibility and business-oriented tendencies, allowing parties to agree on excluding or not applying certain clauses. The lack of clear and mandatory rights for data subjects makes MCCs challenging to meet the EU's high protection standards in bidirectional data transfers. Therefore, while MCCs may be used for ASEAN-to-EU data flows, SCCs remain required for EU-to-ASEAN or bidirectional transfers to ensure the EU's high protection standards.

While both MCCs and SCCs provide valuable interim solutions for enabling cross-border data flows between ASEAN and the EU, material differences in their legal foundations, operational frameworks, and data subject rights protections render them insufficiently interoperable at present. However, Didier Reynders, the EU Commissioner for Justice, affirmed: "This is certainly not the end of our joint efforts: we will continue to work with stakeholders to bridge the two sets of clauses by gathering best practices in implementation and use".[71] The 2023 ASEAN-EU Joint Guide is an important initial step toward fostering mutual understanding but also candidly acknowledges the incomplete compatibility between MCCs and SCCs. This indicates that without convergence in legal standards and data protection levels, cross-use of the two tools will face significant obstacles.

5. Harmonizing personal data transfers between the Association of Southeast Asian Nations and the European Union

This article has provided an overview of existing legal instruments and regional initiatives, highlighting the strengths, limitations, and outstanding issues in the current legal framework for cross-border personal data transfers. It further outlines preliminary recommendations aimed at fostering regulatory harmonization that ensures secure and lawful data flows while accommodating the region's legal heterogeneity as following:

First, a common legal framework with binding force for all AMS is essential. One of the key obstacles to cross-border personal data transfer between two blocs is the lack of regulatory uniformity within ASEAN. Even soft law instruments like the PDP, DMF, and MCCs exhibit inconsistencies, complicating secure cross-border transfers and generating legal uncertainty.

69 Aw, C., Cicco, D. D., Martin, B., Helleputte, C-A., Warren, S., Zhu, L. & Fan, K. (2023, June). *A practical comparison of the EU, China and ASEAN standard contractual clauses*. International Association of Privacy Professionals. https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/

70 Aw, C. et al. (2023, June), *supra* note 72.

71 Association of Southeast Asian Nations (ASEAN) and European Commission (2024), supra note 5, p. 4..

Establishing a binding regional framework would harmonize regulations, fostering a consistent and transparent legal environment. This framework should provide data protection levels equivalent to GDPR to increase compatibility between the two regions' regulations. Only with a unified and effective legal framework can ASEAN promote the free and secure flow of personal data and fully exploit the potential of the digital economy within the region and globally.

Second, ASEAN should create a common reference system for legal data transfers. It would enable businesses that meet standards to legally transfer data across borders. If creating a new set of common principles proves challenging, ASEAN could adopt existing frameworks such as Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors certifications. These are referenced in ASEAN's MCCs as exemplary standards. Singapore, for instance, is the first in the region to officially recognize APEC's frameworks as meeting the conditions for cross-border data transfers under its PDPA.[72] Additionally, having CBPR certification facilitates organizations' acceptance of BCRs by the EU.[73] Therefore, a unified and reference system in ASEAN would reduce compliance burden for businesses and promote cross-border data flows.

Third, ASEAN governments need to enhance the dissemination and usage of MCCs among businesses. Official mechanisms to encourage and guide the use of MCCs, tailored to each AMS's regulations, would provide strong motivation and positive support for businesses, particularly MSMEs, to confidently adopt MCCs. The article proposes practical steps for AMS governments to ensure the roadmap from (i) raising awareness and promoting the choice of MCCs, (ii) providing specific incentives for using MCCs, to (iii) offering guidance on MCC usage. Based on the national context and businesses' awareness of MCCs, AMS can organize workshops and create public publications to disseminate and promote MCCs usage within the region.

In summary, despite ongoing efforts and initial progress, the legal framework governing personal data transfers within ASEAN and between ASEAN and the EU remains fragmented and ambiguous in several respects. Enhancing legal harmonization and regulatory coordination should be regarded as a continuous process that requires practical steps, as well as strong engagement and commitment from all relevant stakeholders. The analysis presented in this article is intended to contribute to policy discussions on the future of personal data protection and digital cooperation in the ASEAN-EU context. ●

72 Infocomm Media Development Authority (2025, August 12). *About APEC Cross Border Privacy Rules (CBPR)*. Government of Singapore. https://www.imda.gov.sg/how-we-can-help/cross-border-privacy-rules-certification#:~:text=The%20CBPR%20certification%20is%20based,Safeguards%20and%20Access%20and%20Correction

73 Kuktelionis, C. (n.d.). *5 Benefits of APEC CBPR Certification You Should Know About*. TrustArc Incorporated. https://trustarc.com/resource/5-benefits-of-apec-cbpr-certification/

References

[1] Burri, M. (2022). Approaches to digital trade and data flow regulation across jurisdictions: implications for the future ASEAN-EU agreement. *Legal Issues of Economic Integration*, *49*(2), 149–168

[2] Dung, T. V. & Cong, L. T. Q. (2025). Trách nhiệm của chủ thể quản lý nền tảng kỹ thuật số (Platforms) – Kinh nghiệm của EU. Trong Đ. V. Đại & B. Hégédus (Chủ biên), *Kỷ yếu hội thảo: Bảo vệ dữ liệu cá nhân trong môi trường số* (tr. 204–235). Nhà xuất bản Đại học Quốc gia TP. Hồ Chí Minh [trans: Tran, V. D., & Le, T. Q. C. (2025). Responsibilities of digital platform operators – EU experiences. In V. D. Do & B. Hégédus (Eds.), *Proceedings of the Conference: Personal Data Protection in the Digital Environment* (pp. 204–235). Vietnam National University Publishing House]

[3] Geradin, D., Karanikioti, T. & Katsifis, D. (2021). GDPR Myopia: How a well-intended regulation ended up favoring large online platforms-the case of ad tech. *European Competition Journal*, *17*(1), 47-92. https://doi.org/10.1080/17441056.2020.1848059

[4] Liu, H-W. (2018). Data localization and digital trade barriers: ASEAN in megaregionalism. In P. L. Hsieh & B. Mercurio (Eds.) (2019). *ASEAN law in the new regional economic order: Global trends and shifting paradigms*. Cambridge University Press.

[5] Liu, J., Sengstschmid, U., & Ge, Y. (2023, August 22), "Facilitating Data Flows Across ASEAN: Challenges and Policy Directions", *ACI Research Paper*, *19*.

[6] Phuong, N. L. & Dong, N. Q. (2022). Bảo vệ dữ liệu cá nhân xuyên biên giới: Thực tiễn và kiến nghị hoàn thiện pháp luật Việt Nam. *Tạp chí Quản lý và Kinh tế quốc tế* [trans: Protecting personal data across borders: Practices and recommendations to improve Vietnamese law. *Journal of International Economics and Management*], *149*

[7] Riswandi, B. A. & Gultom, A. M. (2023). Protecting our mosts valuable personal data: A comparison of transborder data flow laws in the European Union, United Kingdom, and Indonesia. *Prophetic Law Review*, *5*(2), 179-206. https://doi.org/10.20885/PLR.vol5.iss2.art3

[8] Ryngaert, C. & Taylor, M. (2020, January 06). The GDPR as Global Data Protection Regulation?. *American Journal of International Law, 114*, 5–9. https://doi.org/10.1017/aju.2019.80

[9] Singapore's Infocomm Media Development Authority (IMDA) & InformaTech (2022, June 1). *Charting ASEAN's Digital Future: Emerging Policy Challenges* [Reports and Conference Highlights]. Singapore Institute of International Affairs

[10] Taylor, M. (2012, April). *Genetic data and the law: A critical perspective on privacy protection*, Cambridge University Press. https://doi.org/10.1017/CBO9780511910128

[11] Voss, W. G. (2019). Cross-border data flows, GDPR, and data governance. *Washington International Law Journal, 29*(3), 485-531

[12] Wilderoth, S. (2019). *EU data transfer requirements for an adequacy decision and the Vietnamese legal realities* [Graduate Thesis]. Lund University

Author Contribution

All authors contributed to the study conception and design. All authors read and approved the final manuscript.

Declarations

Conflict of Interest: The authors declare no competing interests.

Disclaimer: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.