JURNAL MAGISTER HUKUM UDAYANA
(UDAYANA MASTER LAW JOURNAL)
Vol. 12 No. 3 September 2023
E-ISSN: 2502-3101 P-ISSN: 2302-528x
http: //ojs.unud.ac.id/index.php/jmhu

The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesian's Personal Data Protection Law Followed it?

Merlita Yuli Safitri[1], Mahfud[2]

[1]Fakultas Hukum Universitas Syiah Kuala, E-mail: merlitasaff@gmail.com
[2]Fakultas Hukum Universitas Syiah Kuala, E-mail: mahfud_jufri@usk.ac.id

Article Info
Received: 18th April 2023
Accepted: 27th September 2023
Published: 29th September 2023

Keywords:
Personal Data Transfer, Cross-Border Data Flow, Compatibility of each PDPA's

Corresponding Author:
Mahfud, E-mail: mahfud_jufri@usk.ac.id

DOI:
10.24843/JMHU.2023.v12.i03.p06

Abstract

Nowadays, the use and transfer of personal data in various countries have increased. ASEAN has formed a regional instrument called ASEAN Framework on Personal Data Protection that is expected to become a standard legal system in cross-border data transfer. Indonesia has just ratified Law Number 27 of 2022 on personal data protection, which in this law also regulates the transfer mechanism of personal data outside the Indonesian territory. The more personal data flows outside the territory of Indonesia, the more important it should get adequate protection. This research aims to identify whether ASEAN has provided a sufficient legal system to protect the flow of international data transfers and to explore an adequate legal system in Indonesia that are compatible with the ASEAN framework on PDP towards cross-border data transfer. This is doctrinal legal research with a conceptual and statutory approach. The research shows that ASEAN has faced the issues of asymmetric legislation in the region by proposing any acts that could strengthen the cyber system in Southeast Asia, especially in the cross-border data flow. One of the mechanisms that have been proposed is ASEAN Model Contractual Clauses (MCC). By applying MCC, countries including Indonesia can carry out the personal data transfer across borders with the countries that do not yet have laws that are equal to the PDP Law. Indonesia can also harmonize the contents of the contract in line between domestic laws and regional instruments.

I. Introduction

Several cases that have been reported, especially those involving the dissemination of personal data and subsequent criminal activities, show that regulations protecting personal data are crucial. Personal data protection is connected to the privacy notion. In some cases of data leaks, there are two reasons personal data can be leaked; first, negligence of the system or control over personal data, and second, cybercrime attempts by hackers. Therefore, there is a need for laws that strictly regulate so that personal data

is protected as the right to privacy.[1] For instance, E-commerce may involve several activities such as electronic fund transfers, electronic data transfers, inventory management software, and data collection software. The existence of data collection and data transfer activities that are used as references need strict guarding on data protection.

The personal data protection concept entails that users are entitled to determine whether another user will join the group and then allow or exchange such privacy data with them, as well as the right to determine what conditions must be fulfilled to carry out these activities. In general, laws regarding personal data protection involve safeguarding measures to provide protection of personal data and permit their use by other parties as long as they comply with stipulated conditions.[2] It can be said that such protection is frequently considered a subset of confidentiality protection. For instance, the rules protect personal information. The concept of data protection has a wider privacy category. It is consistent with the notion that privacy is a form of confidentiality or the right to disclose or suppress information that data protection is a component of privacy. In addition, Personal data is defined as the internet's new oil and the digital world currency showing that information belonging to personals becomes an essential asset in digital finance.[3] Thus, it means that individual data may be considered as a new model of human remains which is prone to be amenable to multiple aims yielding multi kinds of value for diverse users, and as with personal remains, they might lose their potency and vitality, as well as their capacity to influence and be influenced.[4]

The management of personal data is essentially an individual issue, however.[5] The transmission of data subjects from one data controller to another is the transfer of personal data. Through bilateral, multilateral, regional, and international cooperation, cross-border data transmission activities are implemented. Under the United Nations, there are no international conventions governing cross-border data flows or other forms of data protection. It is impractical to anticipate such conventions to occur soon. In light of this phenomenon, there is a perceived need for an international legal framework, which has led to the emergence of a number of regional instruments that regulate the protection of data exchange flows, including the European Union's General Data

---

1 Kebocoran Data (Data Leakage), Kenali Penyebab Dan Dampaknya - Acer Commercial, n.d. Available from https://commercial.aacerid.com/supports/articles/kebocorandata-data-leakage-kenali-penyebab-dan-dampaknya/amp//.(accessed on October, 2022).

2 Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1). https://doi.org/10.35741/issn.0258-2724.56.1.23., p.204.

3 Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0.

4 Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data and Society*, *5*(2). https://doi.org/10.1177/2053951718786314, p.6.

5 Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., & McAuley, D. (2015). Personal Data: Thinking Inside the Box. *Aarhus Series on Human Centered Computing*, *1*, Article 1. https://doi.org/10.7146/aahcc.v1i1.21312.

Protection Regulation, the APEC Cross-Border Privacy Rules System, the ASEAN Framework on Personal Data Protection, and others.[6]

The Association of Southeast Asian Nations have published the ASEAN Framework on Personal Data Protection (later called the ASEAN Framework on PDP) in 2016. This instrument aims to strengthen data protection for citizens in ASEAN and facilitate collaboration between its member states to advance trade and information flow within the ASEAN region. Despite having a big goal, this instrument expressly states that this is just a document that reflects the intentions of the ASEAN countries and is not binding on them. The ASEAN Framework on PDP only regulates the transfer of personal data across national borders in a simple and flexible way. So it should be questioned how this regulatory umbrella is capable strengthen the PDP arrangements in the ASEAN region.[7] ASEAN nations must address a number of obstacles to realize a compatible PDP system in Southeast Asia. One of them is that not all ASEAN nations have personal data protection legislation. Following Malaysia in 2010, Singapore in 2012, amended in 2020, the Philippines in 2012, Laos in 2017, and Thailand in 2019, Indonesia is the sixth ASEAN nation to have a special law regulating the protection of personal data. Other ASEAN nations continue to use sector-specific laws and regulations to govern the processing of personal data. Cambodia, for instance, employs laws in the fields of telecommunications, e-commerce, and consumer protection to establish an ecosystem for the protection of personal data processing. Other ASEAN nations, such as Vietnam, have dispersed laws governing PDPs in the domains of civil law, cyber information security, electronic transactions, and population administration.[8] The scope of applicability of personal data protection legislation in ASEAN countries is also different.

The data security of the citizenry of each country is affected by this definite difference in PDP-related legislation between nations. How can a country receive data transmitted from another country while ensuring the data's security against cybercrime? If something occurs to the data in the future, the state can guarantee data recovery, and sanctions will be imposed if personal data is not protected adequately. Despite these distinctions, ASEAN still recognizes the need for a compatible PDP system to facilitate cross-border data transfers in Southeast Asia.[9] Even though the ASEAN Framework on PDP is not intended to create national and international legal obligations, ASEAN is still trying to make the instrument feasible.

Indonesia's PDP Law also incorporates cross-border data transfer articles; however, this article must be further regulated in the Subsidiary legislation of the law to harmonize it with regional instruments from ASEAN. With a personal data protection system that is compatible with regional instruments, Indonesia is opening up great opportunities for the growth of the national digital economy. The subsidiary legislation of PDP law must also be further regulated about the particular formation of personal data protection

[6] *Background-Data Protection*. (n.d.). Retrieved April 26, 2023, available from https://www.coe.int/en/web/data-protection/convention108/background, (accessed on September, 2022).

[7] Asean Framework for Personal data Protection, 2022, available from https://www.dataguidance.com/legalresearch/asean-framework-personal-data-protection, (accessed on October, 2022).

[8] Ibid.

[9] Ibid.

institutions. Based on the background that has been presented, there are two legal issues that arise, namely:

1. Has the ASEAN provided sufficient legal protection for data transfer among the countries in the ASEAN region?
2. How does Indonesia develop an Adequate Legal System compatible with the ASEAN framework on Personal Data Protection towards Cross-Border Data Transfer?

There are previous studies have looked into the issue of the ASEAN Cross Border Personal Data Transfer regulation. Krisman has discussed the next cyber security cooperation which is planning to connect to the whole of the region.[10] Ismail and Masud have discussed the e-commerce potentials of Alibaba's Role and the solution for settling these through cooperation within regional and sub-regional.[11] In addition, Kearney has looked into the increased threat of cyber-attacks within the ASEAN region recently and how to overcome or deal with the problem.[12] This research is going to find the gap that the above previous studies have not fulfilled yet. This research will be looking at the ASEAN legal protection for data transfer among the countries in the ASEAN region and Indonesia's way of developing an Adequate Legal System compatible with the ASEAN framework on Personal Data Protection towards Cross-Border Data Transfer.

2. Research Method

This study is doctrinal legal research that interprets logically and applies qualitative analysis. The primary data for this study came from secondary data obtained from a literature review. With a legal and conceptual approach, this research will describe a review of the law that binds the regulation of cross-border data flow among the countries also in Indonesia. Due to the fact that legal analysis relies primarily on normative juridical sources derived from literature rather than field research, there are no known data in legal research. Legal materials research is applied as a data acquisition method to find prescriptions for a legal event through legal interpretation. The author will systematically arrange to study and draw conclusions according to the problem to be researched using the technique of document study, legal materials, or data that the author obtains.[13]

3. Result and Discussion

3.1 Legal Protection of ASEAN Framework to Provide Personal Data Transfers Among the Countries in The ASEAN Region

ASEAN is the result of the regionalization of countries in Southeast Asia ASEAN became an association founded on August 8, 1967, in Bangkok initiated by Indonesia, the Philippines, Malaysia, Singapore, and Thailand. ASEAN members later developed into eleven states in Southeast Asia, namely, Indonesia, Malaysia, the Philippines, Singapore,

[10] Khanisa. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies*, *1*(1), 41–53, p.41.

[11] Ismail, N. A., & Masud, M. M. (2020). *Prospects and Challenges in Improving E-Commerce Connectivity in Malaysia*.

[12] Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*.

[13] Lexy J. Moleong. (2017). *Metodologi Penelitian Kualitatif*. Rosda Books.

Brunei Darussalam, Thailand, Laos, Myanmar, Vietnam, Timor Leste, and Cambodia which were the last to join. Associated with AEC, this integration is also a place to increase economic activity between countries and their regulations, one of which is in the matter of personal data security. Such integration is happening to a certain extent which includes the personal data issue and the protection of it.[14] Therefore, ASEAN member countries are committed to increasing their cooperation, especially on non-traditional issues.[15]

Personal data security is an important agenda for ASEAN member countries due to indications that ASEAN is the main target for cybercrime activities. This happens for several reasons. Firstly, ASEAN members like Indonesia, Malaysia, and Vietnam have developed as international host spots for the main banned web activities.[16] Secondly, the policy, governance, and capability of cybersecurity in the ASEAN Region is weak.[17] Thirdly, the region also lacks homegrown capacities and expertise because of unintegrated industry and a lack of skilled human resources.[18] Finally, the stakeholders of corporations in the region perceive that cybersecurity is not important for business.[19] The importance of a data localization framework in the ASEAN region is urgently needed as without this it will slow the integration of its regional economy.[20] In regard to this issue, the Government of the Republic of Indonesia has issued Government Regulation Number 82 of 2012 on the Operation of System and Electronic Transaction. Article 15 of this Regulation clearly states that the usage of personal data must be securely guaranteed by the government. This means that the transfer of personal data is also under the authority of the state including its cross-border transfer in the ASEAN.

The eleven member countries of ASEAN have significant differences in countries' interests, especially countries that still prioritize their physical domain. ASEAN has many issues with significant differences in each country's regulations. The following are some of the issues that must be faced by ASEAN:[21]

1. ASEAN member countries have different perceptions and interests in dealing with security threats. Not all ASEAN countries have legislation regarding personal data protection. Indonesia is the sixth country in the ASEAN region that has a special law regulating personal data protection, after Malaysia, Singapore,

---

[14] Surtiwa, S. S., Gultom, C. J., Law, F., Indonesia, U., & Barat, J. (2021). *Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer-to-Peer Lending ASEAN for Data Protection : 558*(Aprish 2019), 720–726, p.722.

[15] Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*.

[16] Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries, Information Institute Conferences. *Information Institute Conferences*, *March*, p.1.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Wong, B. (2020). Data Localization and ASEAN Economic Community. *Asian Journal of International Law*, *10*(1), 158–180, p.159. https://doi.org/10.1017/S2044251319000250

[21] Khanisa. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies*, *1*(1), 41–53, p.41.

the Philippines, Laos, and Thailand consecutively passed it in 2010, 2012, 2012, 2017, and 2019.

Other ASEAN countries still use sectoral laws as regulations in regulating such privacy individual data management. Cambodia, for example, uses laws in the fields of telecommunications, e-commerce, and consumer protection to create an ecosystem of protection in processing personal data. In Vietnam, laws governing civil law, cyber information security, electronic commerce, and population management all have sporadic rules governing such personal data protection. [22]

The applicability ambit of this confidential data protection legislation in ASEAN countries is also different. Malaysia's PDP regulations govern personal data management in connection with the transaction of e-commerce.[23] Singapore's PDP legislation places emphasis on personal data management for private purposes. [24]Thailand's PDP regulations are not aimed at the public sector, such as the parliament, senate, and judiciary. Indonesia, on the other hand, applies the principles of personal data protection for the public and private sectors. This is based on the premise that the right to personal data protection is part of a constitutional right.[25] These differences lead to an asymmetric system in the cross-border data flow. It seems questionable whether countries with no equivalent legislation on PDPA's are able to secure data from countries with national laws on personal data protection.

2. Not all ASEAN member states have the capacity to increase their countries' cyber capabilities, both in terms of literacy and technological aptitude, as this field requires a high level of scientific and technological knowledge. Thus, rather than investing money and energy in cyber security, several ASEAN member countries prefer to strengthen themselves in conventional security aspects, such as buying weapons. [26]
3. ASEAN member countries differ significantly in terms of the contribution of IT technology to the economy. Singapore, for example, is the center of information and technology in Southeast Asia and almost all sectors in Singapore are integrated with IT. As a result, in the event of a cyber attack, many critical infrastructures in Singapore will be affected. This is in contrast to other member states, such as Indonesia, where the level of IT use intervention is not very high.[27]

---

[22] Ibid

[23] Ismail, N. A., & Masud, M. M. (2020). *Prospects and Challenges in Improving E-Commerce Connectivity in Malaysia*.

[24] *Philippines and Singapore to co-lead the ASEAN Data Protection and Privacy Forum - OpenGov Asia*. (n.d.). Retrieved April 26, 2023, available from https://opengovasia.com/philippines-and-singapore-to-co-lead-the-asean-data-protection-and-privacy-forum.

[25] *Looking back on the biggest data breaches to impact ASEAN - Channel Asia*. (n.d.). Retrieved April 26, 2023, from https://www.channelasia.tech/article/645512/looking-back-biggest-data-breaches-impact-asean.

[26] Lee, J., & Perone, M, The Influx of Cybercrime Across Southeast Asia and the Cyber Security and Data Protection Measures That Are Being Placed to Bolster Security Within the Region. 2019.

[27] Ibid

With this variety, it is difficult to pick out the main cybersecurity concerns in ASEAN. However, there remain two areas of common interest for ASEAN countries, namely capacity building and the development of voluntary norms to prevent cyber warfare. It is possible that differences in national laws and regulations will limit the free flow of cross-border transfers of personal data. Important economic sectors such as the banking and insurance industries may be particularly affected by this. For the reasons stated by members of the OECD states, it is urgent to establish Guidelines helping to harmonize domestic privacy laws and to defend human rights while still to keep maintaining data flows globally. These guiding principles reflect the common sense of essential principles that could be regulated into existing domestic laws or represent basic rules of laws in states that have not promulgated them yet.[28] However, the ASEAN framework on PDP is deemed not yet sufficient in providing a system of legal protection. Until now, the ASEAN framework instrument on PDP is in the form of a framework meaning that it is more voluntary by its form, not an "agreement or convention." The framework is more unbinding in nature which does not have a target of implementing data protection law in all ASEAN countries.[29] Therefore, the ASEAN ON PDP is more likely as a roadmap, not an agreement.

ASEAN personal data protection is one of the samples of data security types from other organizations at the regional level, for instance, the General Data Protection Regime of the European Union (later called GDPR) and APEC's Cross-Border Privacy Rules (later called CBPR). Comparing the ASEAN Way concept, ASEAN would adjust its rules to the recent type hence it is following the CBPR. On the other hand, the GDPR model regulates all regulations regarding regional data protection under one umbrella which is very contrary to ASEAN's beliefs. There are four agendas needed to achieve digital personal data security, by following: [30]

1) increasing cybersecurity in regional policies
2) preparing full commitment
3) strengthening the ecosystem
4) building a wave of cybersecurity capabilities.

Nevertheless, ASEAN still continues to see the importance of building a compatible PDP system in facilitating cross-border transfers in the Southeast Asian region. Even though the ASEAN Framework on PDP is not intended to create national and international legal obligations, ASEAN is still trying to make the instrument feasible. At the 19th Telecommunication and Information Technology Ministerial Meeting in 2019 in Laos, two Cross Border Data Flows (CBDF) mechanisms were proposed, namely, the ASEAN Model Contractual Clauses (MCC) and ASEAN Certification for Cross Border Data Flows.[31] In 2020, ASEAN established voluntary guidelines for the implementation of MCC. This instrument contains standard contract clauses that can be used by personal data controllers or processors who will export or import personal data. The MCC clause can be modified according to the needs and regulations of each ASEAN country. These

[28] Ibid

[29] The ASEAN ICT Masterplan, ASEAN Secretariat, 2020.

[30] Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*

[31] *Membangun Mekanisme Transfer Data Pribadi Lintas Batas ASEAN*. (n.d.). Retrieved April 26, 2023, from https://nasional.kompas.com/read/2022/11/18/06000051/membangun-mekanisme-transfer-data-pribadi-lintas-batas-asean.

standard clauses can serve as practical guidelines for Micro, Small, and Medium Enterprises (MSMEs) in ASEAN countries

In another form of supporting ASEAN's cyber system, ASEAN member countries develop certain strategies to improve their security. For example, Singapore and Malaysia are developing cybersecurity experts. The Philippines has drawn up a National Cybersecurity Plan 2022. Collaboration has also been offered to Japan from Thailand to form a cybersecurity training program for ASEAN.[32] Capacity building training and efforts require a long time so if you want to catch up with the world average, there are still many preparations and practices that need to be carried out by ASEAN member countries, especially for countries that don't even have regulations in the field of cyber security.

3.2 Indonesian's Development of in Order to Make it Compatible with ASEAN Framework on Personal Data Protection Towards Cross-Border Data Transfer

In Indonesia, the regime of the development of data protection, particularly after the 1945 Constitution amendment, the privacy right that includes personal data protection is acknowledged as one of the citizens' constitutional rights.[33] The provision concerning guarantees for such protection has been worded in Article 28G paragraph (1) of the Indonesia constitution which provides that"Everyone is entitled to get the protection of personal, family, dignity, property protection, safety, free from fear to do or not to do a thing that is a fundamental right."

There is the fact that along with the growth of Indonesia's e-commerce industry, there have been a growing number of concerns regarding the loss of personal data. One of President Joko Widodo's goals in launching the 1000 Start-Up movement is to develop the digital economy.[34] What is anticipated to encourage the development of four (4) Indonesian unicorn startups, including Go-Jek, Tokopedia, Traveloka, and Bukalapak? It has triggered an enormous compilation of personal consumer data, personal data, and consumers' behavior of shopping data activities. They had no choice but to provide their personal data. Unfortunately, in the absence of a law on personal data protection (before the PDP Law 2022 passed), there was no standardization of data protection principles, resulting in a minimal recognition of the data subject's rights.[35] It can be said that the PDP Law of Indonesia is expected to prevent such personal data from being leaked.

Before the promulgation of PDP Law 2022, there was Law Number 11 of 2008 on Information and Electronic Transactions. Apart from this, the Ministry of Communication and Information has issued its Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems. Article 22 of this Regulation states that the transfer of personal data abroad has to report to and get approval from authorities

---

[32] An ASEAN way of cybersecurity - Policy Forum. (n.d.). Retrieved April 26, 2023, from https://www.policyforum.net/an-asean-way-of-cybersecurity.

[33] Ministry of Communication and Informatics, Existing Regulations Regarding Personal Data Protection in Indonesia.

[34] Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1). https://doi.org/10.35741/issn.0258-2724.56.1.23., p.20

[35] Ibid.

regarding the transformed data although it is not clear whether the approval is obtained before or after the transfer.[36] In addition, Article 17 of the Regulation has regulated that the data center and recovery center of its electronic office providing public data must be located in Indonesia.[37] Through this regulation, Indonesia is preparing itself to face the ASEAN cross-border personal data transfer.

Articles 56 and 57 of Law Number 27 of 2022 on Personal Data Protection regulate at least several options for transferring personal data outside the territory of the Republic of Indonesia. Transferring data is possible for both national and international transfer, with certain circumstances. Domestic data transfer is controlling data and processing data to ensure the protection of personal data under statutes. Indonesian Law on PDP has incorporated at least three requirements. Firstly, before internationally transferring personal data, the controller of data must ensure that the states where the controller of personal data and the processor of personal data receive those data transfers have a personal data protection level that is equal to or higher than Indonesia's PDP Law 2022. Secondly, if the destination country that receives the data does not have rules that are equal to or higher than the PDP Law, the personal data controller must ensure that there is adequate and binding personal data protection. It can also be interpreted through contracts or binding instruments hence data recipients are subject to regulations in Indonesia. Finally, if these two conditions are not met, the personal data controller is obliged to obtain the consent of the personal data subject.

Nevertheless, these three conditions apply alternatively, not cumulatively. Therefore, it is only applicable to one of the conditions. How the security position remains in principle while there is flexibility in the transmission of personal data outside the Republic of Indonesia's territory is perplexing. Law Number 27 of 2022 grants personal data controllers and processors two years (Grace Period) to modify their internal rules and personal data processing practices to the new system. A need for subsidiary legislation for laws to address some of the perceived deficiencies that necessitate an adequate legal framework to safeguard the privacy rights of Indonesian citizens' data. This is a new initiative by the Indonesian government to implement a legal framework that is even better suited to the rapid changes in data protection and cyber systems.[38] However, the Modal Contractual Clause proposed by the ASEAN Framework on Personal Data Protection can be an option for the act of transferring data across- borders and become a legal action that makes a compatible legal system between domestic or national law with international or regional instruments.

The licensing for the cross-border transfer of personal data must be rigorously regulated in Indonesia. Article 56 of the law lists several alternative options, in contrast to the cumulative nature of the PDPA in Europe and Singapore, so it must be emphasized that even if it is an alternative, data transmission must still be protected and privacy rights must be guaranteed by applying for permits for legislation that is compatible with national law in Indonesia. If a region lacks legislation equivalent to the Personal Data

[36] Wong, B. (2020). Data Localization and ASEAN Economic Community. *Asian Journal of International Law*, *10*(1), 158–180, p.167. https://doi.org/10.1017/S2044251319000250.

[37] Ibid.

[38] Ministry of Communication and Informatics. (2021). *Temu Kementerian Digital se-ASEAN, Indonesia Tekankan PDP di ADGSOM*. Accessed on January 2023.

Protection Law, sectoral laws can at least guarantee the security or recovery of data. If something were to happen to the personal data of Indonesian citizens, the country engaging in bilateral or multilateral cooperation with Indonesia could be held liable, or there are preventative measures in place to ensure that foreign countries are capable of ensuring data security.[39]

Indonesia is not only building a cross-border personal data transfer mechanism with ASEAN member countries, but also with the European Union, Asia Pacific, and other jurisdictions. With a personal data protection system that is compatible with regional instruments, Indonesia is opening up great opportunities for the growth of the national digital economy. Building a national personal data protection system that is compatible with regional instruments is a long process. [40]

4. Conclusion

In conclusion, the ASEAN PDP is a framework accord established by the ASEAN Member Countries to strengthen personal data protection in ASEAN, facilitate cooperation between countries, and contribute to promoting and developing regional and global trade and information flows. The ASEAN PDP was created to emphasize the necessity of developing a comprehensive policy framework for the preservation of personal data. However, there is still the absence of laws that are compatible with the others. The ASEAN Framework on PDP's concept of 'Framework' is also not binding under international law. As a result, the ASEAN Framework on PDP is regarded as insufficient for the legal framework of cross-border data transfer in ASEAN. As with other regions, ASEAN continues to develop and strengthen the legal framework governing the transfer of personal data. ASEAN proposes numerous actions to enhance Southeast Asia's cyber system. Two Cross Border Data Flows (CBDF) mechanisms, the ASEAN Model Contractual Clauses (MCC) and the ASEAN Certification for Cross Border Data Flows are proposed. Indonesia as the 6th country in ASEAN has legislation on PDP, which already ratified the Act of Personal Data Protection. The practice of transborder of personal data has been regulated by Articles 56-57 of Indonesia's PDP Law 2022, at least there are three points as requirements for personal data transfer outside Indonesia's jurisdictions. These three conditions do not apply cumulatively, but alternatively. Therefore, it can only be used with one of the conditions. This is confusing how the security position remains in principle, while there is flexibility in the transfer of personal data outside the territory of the Republic of Indonesia. Indonesia has two years or grace period to regulate it further in the form of subsidiary legislation. The paradigm to build a mechanism that is still in line between national law and international instruments is needed for cross-border data transfer.

References

An ASEAN way of cybersecurity - Policy Forum. (n.d.). Retrieved April 26, 2023, from https://www.policyforum.net/an-asean-way-of-cybersecurity.

[39] OECD (Organisation for Economic Co-operation and Development). (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies.

[40] Ministry of Communication and Informatics. (2021). *Temu Kementerian Digital se-ASEAN, Indonesia Tekankan PDP di ADGSOM*.

ASEAN Framework for Personal data Protection, 2022, available from https://www.dataguidance.com/legalresearch/asean-framework-personal-data-protection, (accessed on October, 2022).

Background-Data Protection. (n.d.). Retrieved April 26, 2023, available from https://www.coe.int/en/web/data-protection/convention108/background, (accessed on September, 2022).

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., & McAuley, D. (2015). Personal Data: Thinking Inside the Box. *Aarhus Series on Human Centered Computing*, *1*, Article 1. https://doi.org/10.7146/aahcc.v1i1.21312.

Ismail, N. A., & Masud, M. M. (2020). *Prospects and Challenges in Improving E-Commerce Connectivity in Malaysia*.

Kearney, A. T. (2018). Cybersecurity in ASEAN: An urgent call to action. *Seoul: AT Kearney Inc*.

Khanisa. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies*, *1*(1), 41–53.

Kebocoran Data (Data Leakage), Kenali Penyebab Dan Dampaknya - Acer Commercial, n.d. Available from https://commercial.aacerid.com/supports/articles/kebocorandata-data-leakage-kenali-penyebab-dan-dampaknya/amp//.(accessed on October, 2022).

Looking back on the biggest data breaches to impact ASEAN - Channel Asia. (n.d.). Retrieved April 26, 2023, from https://www.channelasia.tech/article/645512/looking-back-biggest-data-breaches-impact-asean.

Lexy J. Moleong. (2017). *Metodologi Penelitian Kualitatif*. Rosda Books.

Lee, J., & Perone, M, The Influx of Cybercrime Across Southeast Asia and the Cyber Security and Data Protection Measures That Are Being Placed to Bolster Security Within the Region. 2019.

Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data and Society*, *5*(2). https://doi.org/10.1177/2053951718786314, p.6.

Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1). https://doi.org/10.35741/issn.0258-2724.56.1.23.

Membangun Mekanisme Transfer Data Pribadi Lintas Batas ASEAN. (n.d.). Retrieved April 26, 2023, from https://nasional.kompas.com/read/2022/11/18/06000051/membangun-mekanisme-transfer-data-pribadi-lintas-batas-asean.

Ministry of Communication and Informatics, Existing Regulations Regarding Personal Data Protection in Indonesia.

Ministry of Communication and Informatics. (2021). *Temu Kementerian Digital se-ASEAN, Indonesia Tekankan PDP di ADGSOM*. Accessed on January 2023.

OECD (Organisation for Economic Co-operation and Development). (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies.

Philippines and Singapore to co-lead the ASEAN Data Protection and Privacy Forum - OpenGov Asia. (n.d.). Retrieved April 26, 2023, available from https://opengovasia.com/philippines-and-singapore-to-co-lead-the-asean-data-protection-and-privacy-forum.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0.

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries, Information Institute Conferences. *Information Institute Conferences*, *March*.

Surtiwa, S. S., Gultom, C. J., Law, F., Indonesia, U., & Barat, J. (2021). *Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer to Peer Lending ASEAN for Data Protection : 558*(Aprish 2019), 720–726.

The ASEAN ICT Masterplan, ASEAN Secretariat, 2020.

Wong, B. (2020). Data Localization and ASEAN Economic Community. *Asian Journal of International Law*, *10*(1), 158–180. https://doi.org/10.1017/S2044251319000250

Laws and Regulations

The Law Number 11 of 2008 on Information and Electronic Transaction

The Law Number 27 of 2022 on Personal Data Protection

The Government Regulation Number 82 of 2012 on the Operation of System and Electronic Transaction

The Ministry of Communication and Information Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems