

## **PERSONAL DATA PROTECTION IN ASEAN: INDONESIA'S ROLE IN DEVELOPING ASEAN'S PERSONAL DATA PROTECTION LEGAL FRAMEWORK**

**Syafri Hariansah**

[syafrihariansah@stihpertibapkp.ac.id](mailto:syafrihariansah@stihpertibapkp.ac.id)

Sekolah Tinggi Ilmu Hukum Pertiba

**Atma Suganda**

[atma\\_suganda@jayabaya.ac.id](mailto:atma_suganda@jayabaya.ac.id)

**Ramlani Lina Sinaulan**

[ramlani\\_ls@jayabaya.ac.id](mailto:ramlani_ls@jayabaya.ac.id)

Universitas Jayabaya, Indonesia

**Marsha Angelina**

[Marsha1201@kyungsung.ac.id](mailto:Marsha1201@kyungsung.ac.id)

Kyungsung University, South Korea

### **ABSTRACT**

The protection of personal data has become increasingly important in the digital era, including in the ASEAN region. However, some ASEAN countries still face challenges in developing adequate legal frameworks to protect personal data. This normative study aims to analyze the challenges and opportunities in developing a legal framework for personal data protection in ASEAN, including Indonesia's role in driving the unification of personal data protection laws in the region. The research method used is normative or doctrinal research, which involves analyzing existing legal sources related to personal data protection in ASEAN. The results of the study show that some challenges faced by ASEAN countries include a lack of human resources and information technology infrastructure, high costs in developing legal frameworks, and foreign interventions that can influence the development of personal data protection laws. However, opportunities exist in the form of increasing public awareness about personal data protection and collaboration between ASEAN countries to develop legal frameworks that are suitable for local and international conditions. This study provides valuable insights for policymakers in developing legal frameworks for personal data protection in ASEAN, with a particular emphasis on Indonesia's role in driving the unification of laws across the region

**Keywords:** Personal data protection, ASEAN, Legal Framework,

### **Background**

"The leakage of personal data is a serious problem faced by many countries worldwide, including in the ASEAN region. Therefore, the protection of personal data has become an important issue in the ASEAN region, especially with the increasing use of internet

and digital technology in the area.<sup>1</sup> This increase poses new challenges in protecting individuals' personal data and maintaining their privacy in the virtual world. Based on empirical evidence, there have been several cases of personal data leaks in the ASEAN region in the last three years. Statistics show that in July 2019, personal data of millions of users of the Lazada Thailand e-commerce platform leaked due to a security breach in the server.<sup>2</sup> The leaked data included full name, email address, phone number, and user's home address. Then, in August 2020, it was found that personal data of millions of users of the Philippine government website leaked. The leaked data included name, email address, phone number, date of birth, and user's home address.<sup>3</sup>

Furthermore, in the same year, a case of personal data leakage occurred in Vietnam, specifically in October 2020, where personal data of millions of users of the Tiki e-commerce platform leaked due to a cyber attack.<sup>4</sup> The leaked data included full name, email address, phone number, home address, and financial information. A few months later, specifically in 2021, there were consecutive incidents of personal data leaks in three countries. Firstly, in February 2021, it was discovered that personal data of millions of Malaysian citizens who registered for financial aid during the COVID-19 pandemic was leaked.<sup>5</sup> The leaked data includes full name, national identification number, address, phone number, and financial information.

Then, in March 2021, there was a case of employee data leakage in Singapore.<sup>6</sup> Based on legal facts, it was found that personal data of employees from more than 100 companies operating in Singapore leaked due to a security incident on the payroll platform of one of the payroll service providers in Singapore. The leaked data includes employee names, dates of birth, email addresses, and phone numbers. In the same month, a similar case occurred in Indonesia, specifically in March 2021, where personal data of millions of users of the Gojek transportation application leaked due to a security vulnerability on one of the company's servers. The leaked data includes user names, email addresses, phone numbers, and home addresses.

ASEAN, as an increasingly integrated economic region, has introduced various initiatives to enhance the protection of personal data. This started with the adoption of the "Declaration of Principles on Electronic Commerce" in 1999, which recognized the importance of personal data protection in electronic commerce. Furthermore, in

---

<sup>1</sup> Dewa Gede Sudika Mangku et al., "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University* 56, no. 1 (2021), <https://doi.org/10.35741/issn.0258-2724.56.1.23>.

<sup>2</sup> Bangkok Post, "Lazada denies being behind data leak, November 21, 2021 access through <https://www.bangkokpost.com/thailand/general/2023111/lazada-denies-being-behind-data-leak>.

<sup>3</sup> Inquirer.net "Over 1M records from NBI, PNP, other agencies leaked in massive data breach" access through <https://newsinfo.inquirer.net/1758456/over-1-million-records-from-nbi-pnp-other-agencies-leaked-in-huge-data-breach#ixzz8126OAzLG>.

<sup>4</sup> VN, "Vietnam has major data leak problem, citizens suffer" access through <https://e.vnexpress.net/news/news/vietnam-has-a-big-data-leak-problem-4501707.html> August 19, 2022.

<sup>5</sup> Malay Mail, "Major data breaches in Malaysia in the past 24 months", 31 Dec 2022, access through <https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722>.

<sup>6</sup> IT News "Singapore public sector saw 178 data breaches in 2021", August 1, 2022 access through <https://www.itnews.asia/news/singapore-public-sector-saw-178-data-breaches-in-2021-583428>.

2016, ASEAN adopted the "ASEAN Convention on Counter-Terrorism" which included provisions on personal data protection. In addition, in 2018, ASEAN also adopted the "ASEAN Framework on Personal Data Protection," which provides guidance for ASEAN countries in developing legal frameworks for personal data protection in the region.

However, there are still challenges in developing this legal framework. Some ASEAN countries still do not have strong enough laws for personal data protection, and the implementation of existing laws still needs improvement. Additionally, cybersecurity issues such as hacking and identity theft remain significant threats to personal data privacy in the region. On the other hand, the development of a strong legal framework for personal data protection in ASEAN also presents significant opportunities for the region. In the era of globalization and digitization, the ASEAN region can gain a competitive advantage by attracting investors and businesses that require strong personal data protection guarantees to expand their operations in the region. Therefore, research on personal data protection in the ASEAN region can help identify challenges and opportunities in developing an effective legal framework in the region, as well as provide insights for ASEAN countries in promoting personal data security and privacy in the digital age.

The first study titled "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries" International Journal of Advanced Trends in Computer Science and Engineering, by Mohamed Mizan, Nor Shazwina et al,<sup>7</sup> This research examines the cybersecurity challenges faced by ASEAN countries, covering important aspects such as threats, technology, policy, and regional cooperation. The aim is to increase awareness and provide recommendations to address these issues. Furthermore, the study "ASEAN Personal Data Protection (PDP): Achieving Digital Personal Data Security in Southeast Asia" (2020) written by Tampubolan et al and published in the Padjajaran Journal International Relations.<sup>8</sup> This research discusses the challenges and opportunities faced by ASEAN countries in protecting personal data in the digital era. It evaluates the regulations on personal data protection in ASEAN and provides recommendations to enhance personal data protection in the region. What distinguishes this current research from the previous studies is that it focuses more on the situation and challenges faced by ASEAN countries and other legal entities in managing personal data in ASEAN, as well as the role of Indonesia in promoting the development of an effective and comprehensive legal framework in the ASEAN region.

## Method

This study is a normative or doctrinal research. This method is based on collecting data from legal sources such as laws, regulations, court decisions, other legal documents, and relevant literature. The data is then analyzed and interpreted, and

---

<sup>7</sup> Mohamed Mizan, Nor Shazwina and Ma'arif, Muhamad Yusnorizam and Mohd Satar, Nurhizam Safie and Shahar, Siti Mariam, CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries (April 2019). *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No.1.4, 2019.

<sup>8</sup> Tampubolon, Trisa, and Rizki Ramadhan. "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara." *Padjajaran Journal of International Relations* 1.3 (2020): 270-286.

---

arguments and recommendations are developed based on the applicable laws in the ASEAN region. In this study, data was obtained through laws, regulations, conventions, and other legal frameworks related to the protection of personal data in ASEAN countries.

Additionally, the study examined other legal documents and relevant literature on the research topic such as scholarly articles, books, and other publications. After collecting the necessary data, the researcher will analyze and interpret the data, and develop arguments and recommendations based on the applicable laws in the ASEAN region.

## Discussion

Challenges ASEAN countries in developing a legal framework to protect personal data

Association of Southeast Asian Nations (ASEAN) was established on August 8, 1967. The organization was founded by five countries, namely Indonesia, Malaysia, the Philippines, Singapore, and Thailand, with the aim of increasing political and security stability in the Southeast Asian region, as well as enhancing economic cooperation among member countries. The establishment of ASEAN was triggered by a common concern about the communist influence in Southeast Asia at that time. At the same time, countries in the region also realized that they had many similarities in terms of history, culture, and language.

Initially, ASEAN focused more on cooperation in the political and security fields. This was reflected in the signing of the Bangkok Declaration in 1967, where member states agreed to work together in building a conflict-free region and upholding the principles of non-intervention, respecting sovereignty, and respecting the territorial integrity of each country.<sup>9</sup>

Furthermore, in 1976, ASEAN signed the Declaration on the Zone of Peace, Freedom, and Neutrality (ZOPFAN), which emphasized the commitment of member countries to promote peace and stability in the region.<sup>10</sup> Over time, ASEAN also strengthened its economic cooperation. In 1992, ASEAN established the ASEAN Free Trade Area (AFTA),<sup>11</sup> which aimed to eliminate trade barriers between member countries. This was the first step towards the formation of the ASEAN Free Trade Area (AFTA), which came into effect in 2010.

To date, ASEAN has developed into a regional organization comprising 10 countries, namely Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. ASEAN continues to strive to enhance cooperation among member countries in various fields, such as economics, socio-cultural, and environmental.

---

<sup>9</sup> Mohamad Faisol Keling et al., "The Development of ASEAN from Historical Approach," *Asian Social Science* 7, no. 7 (2011): 169–89, <https://doi.org/10.5539/ass.v7n7p169>.

<sup>10</sup> Laura Southgate, "ASEAN: Still the Zone of Peace, Freedom and Neutrality?," *Political Science* 73, no. 1 (2021): 31–47, <https://doi.org/10.1080/00323187.2021.1967762>.

<sup>11</sup> Koichi Ishikawa, "The ASEAN Economic Community and ASEAN Economic Integration," *Journal of Contemporary East Asia Studies* 10, no. 1 (2021): 24–41, <https://doi.org/10.1080/24761028.2021.1891702>.

The threat of cyber attacks and personal data leaks is a global threat that can affect any country, including countries in the ASEAN region.<sup>12</sup> These threats can include hacking attacks, viruses, malware, and phishing attacks, in which attackers attempt to gain access to sensitive systems or data by impersonating identities or deceiving users into providing their personal information.

Countries in the ASEAN region need to be vigilant against these potential threats because they have increasingly developed information technology infrastructure and growing internet users.<sup>13</sup> This can make them targets for attackers seeking ways to obtain sensitive information or damage systems. Therefore, ASEAN countries need to pay attention to the threat of cyber attacks and personal data leaks by increasing awareness of cybersecurity and strengthening their infrastructure security. They should also have strong security protocols and regularly conduct security audits to protect their sensitive data and prevent hacking attacks.<sup>14</sup>

Based on empirical evidence, there are several important challenges for ASEAN countries in building a joint legal framework as an effort to protect their citizens' personal data.<sup>15</sup> The first challenge is oriented towards legal and policy diversity,<sup>16</sup> which is one of the challenges faced by ASEAN countries in developing a legal framework to protect their citizens' personal data. ASEAN countries have differences in terms of legal systems and policies, as well as different cultures and values. This diversity can be an obstacle in achieving consensus and developing the same rules among ASEAN countries in order to protect personal data.

For example, there are differences among ASEAN countries in terms of the definition of personal data. Some countries have a broad definition, while others may have a narrower one. This can result in differences in the regulation and protection of personal data among ASEAN countries. In addition, some ASEAN countries may have immature laws that are not capable of dealing with complex personal data protection issues, while others may have mature and effective laws in protecting personal data. This can also cause differences in the regulation of personal data protection among ASEAN countries.

Legal and policy diversity can also hinder harmonization and coordination in developing an effective legal framework to protect personal data. Therefore, ASEAN

---

<sup>12</sup> Md Ershadul Karim et al., "Too Enthusiastic to Care for Safety: Present Status and Recent Developments of Nanosafety in ASEAN Countries," *Technological Forecasting and Social Change* 92 (2015): 168-81, <https://doi.org/10.1016/j.techfore.2014.07.003>.

<sup>13</sup> Heejin Kim, "Globalization and Regulatory Change: The Interplay of Laws and Technologies in E-Commerce in Southeast Asia," *Computer Law and Security Review* 35, no. 5 (2019): 105315, <https://doi.org/10.1016/j.clsr.2019.03.009>.

<sup>14</sup> Warren B. Chik, "The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform," *Computer Law and Security Review* 29, no. 5 (2013): 554-75, <https://doi.org/10.1016/j.clsr.2013.07.010>.

<sup>15</sup> Narcyz Roztocki, Piotr Soja, and Heinz Roland Weistroffer, "The Role of Information and Communication Technologies in Socioeconomic Development: Towards a Multi-Dimensional Framework\*," *Information Technology for Development* 25, no. 2 (2019): 171-83, <https://doi.org/10.1080/02681102.2019.1596654>.

<sup>16</sup> Nguyen Xuan Thuy, "' Diversity of Legal Culture in Southeast Asian Countries ( ASEAN ) '" 9, no. April (2020): 1-7.

countries need to adopt an inclusive approach and focus on developing a legal framework that is appropriate to their own context, but still adopts the same principles to protect personal data throughout ASEAN. In this regard, the role and support of international institutions such as the European Union and the OECD can help ASEAN countries to overcome these challenges by adopting international standards in personal data protection.

The second and equally serious challenge is related to the legal culture that is correlated with the awareness<sup>17</sup> of the importance of personal data protection in ASEAN countries, which is another challenge in the development of a legal framework to protect personal data. Although the importance of personal data protection is increasingly recognized in the current digital era, awareness of its importance in some ASEAN countries remains low.<sup>18</sup>

This lack of awareness can be caused by several factors, such as the lack of education on personal data protection and the lack of transparency from technology companies about how they collect, use, and manage users' personal data. The impact of the lack of awareness of the importance of personal data protection is the lack of public support to strengthen the existing legal framework and improve the implementation of personal data protection policies. This can result in weaknesses in the implementation and supervision of personal data protection policies, making personal data vulnerable to misuse or theft by irresponsible parties.

Therefore, efforts are needed to increase awareness of the importance of personal data protection in ASEAN countries through more extensive and effective education campaigns. Education on personal data protection can be taught in schools and universities, as well as through social media and information campaigns conducted by governments or civil society organizations. In addition, technology companies must also be responsible for providing transparency about how they collect, use, and manage users' personal data. Thus, the public can understand the risks associated with technology use and take action to protect their personal data.

Apart from the substantive and legal culture issues, challenges to privacy sovereignty in ASEAN can also be influenced by resource and financial limitations,<sup>19</sup> which is another challenge faced by ASEAN countries in developing a legal framework to protect personal data. The implementation of a legal framework to protect personal data requires sufficient resources and costs, such as trained human resources, adequate information technology infrastructure, and sufficient budget for monitoring and law enforcement.

---

<sup>17</sup> Syafri Hariansah, "Analisis Implementasi Nilai-Nilai Budaya Hukum Dalam Kehidupan Berbangsa Dan Bernegara : Studi Kritis Pendekatan Masyarakat , Budaya Dan Hukum" 16, no. 1 (2022): 121-30.

<sup>18</sup> Mubarak Rahamathulla, "Cyber Safety of Children in the Association of Southeast Asian Nations (ASEAN) Region: A Critical Review of Legal Frameworks and Policy Implications," *International Journal on Child Maltreatment: Research, Policy and Practice* 4, no. 4 (2021): 375-400, <https://doi.org/10.1007/s42448-021-00087-5>.

<sup>19</sup> Xiangyu Zhu and Yang Yang, "Big Data Analytics for Improving Financial Performance and Sustainability," *Journal of Systems Science and Information* 9, no. 2 (2021): 175-91, <https://doi.org/10.21078/JSSI-2021-175-17>.

In several ASEAN countries, human resources and information technology infrastructure are still limited,<sup>20</sup> making it difficult to develop adequate legal frameworks to protect personal data. Moreover, the costs required to develop legal frameworks and ensure effective monitoring and enforcement of laws can be a heavy burden for ASEAN governments facing budget constraints. These resource and financial limitations can hinder ASEAN countries from adopting and implementing international standards for the protection of personal data, such as the General Data Protection Regulation (GDPR) of the European Union.<sup>21</sup>

The implementation of these international standards requires significant resources and costs, which can pose challenges for ASEAN countries with limited resources and finances to adopt and implement them. Therefore, ASEAN countries need to seek creative solutions to address these resource and financial limitations in developing legal frameworks to protect personal data. One solution is to build partnerships with the private sector and international institutions to obtain resource and financial support. For example, some ASEAN countries have formed partnerships with large technology companies to develop data privacy policies and standards, as well as to strengthen the government's capacity to monitor and enforce data privacy laws. In addition, ASEAN countries can also strengthen cooperation with international institutions, such as the European Union or OECD, to obtain technical and financial assistance in developing adequate legal frameworks.

Moreover, ASEAN countries can leverage technology and innovation to optimize the use of existing resources and finances. For instance, by using blockchain technology, ASEAN countries can develop more efficient and transparent data security and privacy systems at a lower cost. In the long run, ASEAN countries also need to increase budget allocations to strengthen information technology infrastructure and enhance human resource capacity in the field of data privacy. This can be achieved by strengthening cooperation with the private sector, international institutions, and optimizing government budget allocations. Thus, ASEAN countries can develop adequate legal frameworks for protecting personal data in an effective and sustainable manner.

Furthermore, foreign influence in the development of legal frameworks in ASEAN can pose a serious challenge in protecting personal data. Some ASEAN countries have adopted international standards for personal data protection, such as the General Data Protection Regulation (GDPR) of the European Union. However, the adoption of these standards can lead to intervention by foreign countries or institutions with different interests.

Examples of foreign interventions that may occur include pressure to adopt data privacy standards that are not in line with local conditions or national interests. Moreover, foreign countries or institutions can also intervene through political and economic influence, such as through trade agreements or technical and financial

---

<sup>20</sup> Ying Chyi Chou et al., "Assessing the Human Resource in Science and Technology for Asian Countries: Application of Fuzzy AHP and Fuzzy TOPSIS," *Symmetry* 11, no. 2 (2019), <https://doi.org/10.3390/sym11020251>.

<sup>21</sup> Sidi Mohamed Sidi Ahmed and Sonny Zuhuda, "Data Protection Challenges in the Internet of Things Era: An Assessment of Protection Offered By Pdpa 2010," *International Journal of Law, Government and Communication* 4, no. 17 (2019): 01-12, <https://doi.org/10.35631/ijlgc.417001>.

assistance. One example of foreign intervention in the development of data privacy legal frameworks in ASEAN is through trade agreements. Some ASEAN countries have signed trade agreements with foreign countries or institutions that include provisions related to data privacy. However, these provisions may not be adequate or may even be contrary to national interests or local conditions, thus hindering ASEAN countries' efforts in developing legal frameworks that are suitable for local conditions.

Technical and financial assistance from foreign countries or institutions can also influence the development of data privacy legal frameworks in ASEAN. Such assistance may come with certain requirements or influence the agenda of ASEAN countries' policy development in personal data protection. In some cases, such assistance may be an unwanted form of intervention in ASEAN countries' development of data privacy legal frameworks. Therefore, ASEAN countries need to ensure that the development of data privacy legal frameworks is based on local conditions and national interests, and consider the impact of foreign intervention in the process. ASEAN countries also need to enhance their capacity in policy development and decision-making to ensure that decisions made are in line with local conditions and national interests.

#### Indonesia's Role in Driving Opportunities for Developing a Legal Framework for Personal Data Protection in ASEAN "

The protection of personal data has become increasingly important in the digital era, as more people interact with technology and provide personal information.<sup>22</sup> In ASEAN, the protection of personal data has been regulated in several national laws and international agreements. However, due to differences in legal systems within ASEAN, there is a need to develop a specific legal framework governing the protection of personal data throughout the ASEAN region. ASEAN member states have a great opportunity to build partnerships, especially in the legal field.

As a regional organization, ASEAN has established various frameworks and agreements in the legal field to enhance cooperation and integration among its member states. To develop a new legal framework specifically governing the protection of personal data in ASEAN, ASEAN member states must work together to develop the same minimum standards for personal data protection and implement them throughout the ASEAN region. Concrete steps can be taken through the development of international agreements or conventions at the ASEAN level, such as the proposed ASEAN Convention on Personal Data Protection in 2018.

In developing a new legal framework, ASEAN countries must also consider the cultural and values differences, as well as differences in national legal systems. Additionally, ASEAN countries need to pay attention to the constantly changing technology landscape and update the legal framework accordingly. It is important to note that

---

<sup>22</sup> Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means," *Information and Communications Technology Law* 28, no. 1 (2019): 65–98, <https://doi.org/10.1080/13600834.2019.1573501>.



data protection is not just a legal issue, but also involves other aspects such as technology, cyber security, and privacy.<sup>23</sup> Therefore, in developing a new legal framework, ASEAN countries must also work with the private sector, civil society organizations, and academics to ensure that the agreed legal framework covers all relevant aspects.

As a country with the largest economy in ASEAN and one of the largest internet users in the world, Indonesia has an important role in initiating efforts to strengthen data protection in ASEAN.<sup>24</sup> One such effort is to encourage the unification of data protection laws in ASEAN through the ASEAN Summit forum to be held this year. In this effort, Indonesia can play a role as a director or coordinator for other ASEAN countries in developing a uniform legal framework for data protection. Indonesia can also leverage its experience in developing laws such as the Information and Electronic Transactions Act No. 11 of 2008, the Personal Data Protection Act No. 27 of 2022, and other technical regulations that have included principles of data protection.

An initial step that Indonesia can take is to propose the drafting of an ASEAN Convention or Charter on Personal Data Protection that includes key principles such as the definition of personal data, principles of data protection, supervision and law enforcement, and inter-country cooperation. In addition, Indonesia can facilitate dialogue and discussion among ASEAN countries to address differences in data protection policies and legal frameworks, thus creating a more uniform understanding among those countries. In this regard, it is important to ensure that the unification of data protection laws in ASEAN is not only regulations that align with good data protection principles, but also considers the interests and needs of ASEAN countries in their respective political, social, and economic contexts.

Furthermore, Indonesia can promote the harmonization of ASEAN laws on personal data protection as an effort to achieve an agreement on consistent policies and minimum standards for personal data protection across the ASEAN region.<sup>25</sup> The effort to harmonize these laws aims to ensure that personal data handled by organizations or companies in ASEAN are protected in a uniform and equitable manner, thereby promoting digital economic growth and protecting human rights in the region.

One way to achieve ASEAN law harmonization is to adopt personal data protection laws in each member state. However, in recent years, efforts to achieve law harmonization have evolved into efforts to implement a uniform legal framework for personal data protection throughout the ASEAN region, rather than just adopting laws in each country. To achieve this unification, member states can use several strategies systematically:

---

<sup>23</sup> Jay Pil Choi, Doh Shin Jeon, and Byung Cheol Kim, "Privacy and Personal Data Collection with Information Externalities," *Journal of Public Economics* 173 (2019): 113–24, <https://doi.org/10.1016/j.jpubeco.2019.02.001>.

<sup>24</sup> Bama Andika Putra, "Indonesia'S Leadership Role in Asean: History and Future Prospects," *IJASOS-International E-Journal of Advances in Social Sciences* 1, no. 2 (2015): 188, <https://doi.org/10.18769/ijasos.82584>.

<sup>25</sup> Antonia Vlahou et al., "Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics?," *Hypertension* 77, no. 4 (2021): 1029–35, <https://doi.org/10.1161/HYPERTENSIONAHA.120.16340>.

Member states can adopt conventions or agreements at the ASEAN level that regulate personal data protection. These conventions or agreements will serve as a binding legal basis for ASEAN countries to ensure equal personal data protection throughout the region.

Member states can coordinate and work together to develop a strong and consistent national legal framework for personal data protection. The national legal framework should reflect the policies and minimum standards established at the ASEAN level.

Member states can develop strong and effective regulators responsible for enforcing personal data protection rules. Regulators must have sufficient power and resources to monitor the collection, processing, and use of personal data and to take action against violations.

Member states can conduct educational and socialization campaigns to increase public awareness of the importance of personal data protection, individual rights to their personal data, and ways to protect their own personal data. These educational and socialization campaigns can help strengthen public support for personal data protection and support efforts to unify personal data protection laws in ASEAN.

To achieve personal data protection law unification in ASEAN, member states must commit to working together and reaching a joint agreement on policies and minimum standards for personal data protection. With sustained efforts, ASEAN can build a new legal framework that can effectively provide personal data protection in ASEAN member states.<sup>26</sup> The ASEAN countries can take the following steps to develop a comprehensive framework for personal data protection:

Establish uniform policies and minimum standards for personal data protection across the ASEAN region. This can be achieved through dialogue and meetings between regulators and governments of ASEAN countries. Once these minimum standards are established, ASEAN countries can develop legal frameworks that align with these policies.

Develop an agreement or convention on personal data protection at the ASEAN level. This agreement or convention can serve as a binding legal basis for ASEAN countries to ensure equal protection of personal data. It can cover basic principles, such as the requirement for obtaining consent from data owners before collecting, processing, and using their personal data. The convention can also regulate authorization and permission for data collection, processing, and use, as well as the sanctions that will be imposed if violations occur.

Develop a strong and consistent national legal framework for personal data protection. This framework should align with the policies and minimum standards established at the ASEAN level. ASEAN countries can strengthen their national legal framework by enacting special laws that regulate personal data protection, as has been done by some ASEAN countries such as Indonesia and Thailand.

Strengthen the regulator responsible for enforcing personal data protection rules. ASEAN countries can strengthen the regulator by providing adequate resources to oversee the collection, processing, and use of personal data, and by taking action against violations that occur. Regulators can collaborate with each other in ASEAN countries to improve and strengthen the legal framework in the region.

---

<sup>26</sup> Vlahou et al.

Increase public awareness of the importance of personal data protection. ASEAN countries can conduct educational and awareness campaigns to increase public awareness of the importance of personal data protection, individual rights regarding their personal data, and ways to protect their personal data.

The success of ASEAN in developing a legal framework for personal data protection is quite promising with the efforts to harmonize laws and unify policies among member countries. In this regard, Indonesia's initiative to accelerate the unification of laws in ASEAN related to personal data protection is important. With good cooperation and coordination, it is hoped that a uniform and effective legal framework can be created to protect personal data in ASEAN, thus creating a safe and trustworthy digital environment for the growth of the digital economy in the region.

### Conclusion

Based on the previous description and analysis, it can be concluded that ASEAN countries face challenges and obstacles in developing an adequate legal framework to protect personal data. Firstly, some of these challenges include the lack of human resources and information technology infrastructure, high costs in developing legal frameworks, as well as foreign intervention that can influence the development of personal data protection laws. However, there are opportunities for ASEAN countries to develop a new legal framework. These opportunities primarily stem from the increasing public awareness about the protection of personal data and collaboration among ASEAN countries in developing legal frameworks that are appropriate for local and international conditions.

Secondly, Indonesia has an important role in promoting the birth of a new legal framework for personal data protection in ASEAN, especially in the effort to unify personal data protection laws throughout the region. As the host of the 43rd ASEAN Summit, Indonesia can use this momentum to strengthen its role and influence in developing an adequate legal framework to protect personal data in ASEAN. Therefore, it is crucial for policymakers to consider the results of this research and take appropriate actions to ensure sufficient protection of personal data in ASEAN.

### Bibliography

1. Chik, Warren B. "The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform." *Computer Law and Security Review* 29, no. 5 (2013): 554–75. <https://doi.org/10.1016/j.clsr.2013.07.010>.
2. Choi, Jay Pil, Doh Shin Jeon, and Byung Cheol Kim. "Privacy and Personal Data Collection with Information Externalities." *Journal of Public Economics* 173 (2019): 113–24. <https://doi.org/10.1016/j.jpubeco.2019.02.001>.
3. Chou, Ying Chyi, Hsin Yi Yen, Van Thac Dang, and Chia Chi Sun. "Assessing the Human Resource in Science and Technology for Asian Countries: Application of Fuzzy AHP and Fuzzy TOPSIS." *Symmetry* 11, no. 2 (2019). <https://doi.org/10.3390/sym11020251>.
4. Hariansah, Syafri. "Analisis Implementasi Nilai-Nilai Budaya Hukum Dalam Kehidupan Berbangsa Dan Bernegara : Studi Kritis Pendekatan Masyarakat , Budaya Dan Hukum" 16, no. 1 (2022): 121–30.

5. Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information and Communications Technology Law* 28, no. 1 (2019): 65–98. <https://doi.org/10.1080/13600834.2019.1573501>.
6. Ishikawa, Koichi. "The ASEAN Economic Community and ASEAN Economic Integration." *Journal of Contemporary East Asia Studies* 10, no. 1 (2021): 24–41. <https://doi.org/10.1080/24761028.2021.1891702>.
7. Karim, Md Ershadul, Abu Bakar Munir, Ahmed Wasif Reza, Firdaus Muhammad-Sukki, Siti Hajar Mohd Yasin, Siti Hawa Abu-Bakar, and Ruzairi Abdul Rahim. "Too Enthusiastic to Care for Safety: Present Status and Recent Developments of Nanosafety in ASEAN Countries." *Technological Forecasting and Social Change* 92 (2015): 168–81. <https://doi.org/10.1016/j.techfore.2014.07.003>.
8. Keling, Mohamad Faisol, Hishamudin Md Som, Mohamad Nasir Saludin, Md Shukri Shuib, and Mohd Na eim Ajis. "The Development of ASEAN from Historical Approach." *Asian Social Science* 7, no. 7 (2011): 169–89. <https://doi.org/10.5539/ass.v7n7p169>.
9. Kim, Heejin. "Globalization and Regulatory Change: The Interplay of Laws and Technologies in E-Commerce in Southeast Asia." *Computer Law and Security Review* 35, no. 5 (2019): 105315. <https://doi.org/10.1016/j.clsr.2019.03.009>.
10. Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliantini, I. Nengah Suastika, and I. Gusti Made Arya Suta Wirawan. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56, no. 1 (2021). <https://doi.org/10.35741/issn.0258-2724.56.1.23>
11. Mohamed Mizan, Nor Shazwina and Ma'arif, Muhamad Yusnorizam and Mohd Satar, Nurhizam Safie and Shahar, Siti Mariam, CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries (April 2019). *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No.1.4, 2019..
12. Putra, Bama Andika. "Indonesia'S Leadership Role in Asean: History and Future Prospects." *IJASOS- International E-Journal of Advances in Social Sciences* 1, no. 2 (2015): 188. <https://doi.org/10.18769/ijasos.82584>.
13. Rahamathulla, Mubarak. "Cyber Safety of Children in the Association of Southeast Asian Nations (ASEAN) Region: A Critical Review of Legal Frameworks and Policy Implications." *International Journal on Child Maltreatment: Research, Policy and Practice* 4, no. 4 (2021): 375–400. <https://doi.org/10.1007/s42448-021-00087-5>.
14. Roztockı, Narcyz, Piotr Soja, and Heinz Roland Weistroffer. "The Role of Information and Communication Technologies in Socioeconomic Development: Towards a Multi-Dimensional Framework\*." *Information Technology for Development* 25, no. 2 (2019): 171–83. <https://doi.org/10.1080/02681102.2019.1596654>.
15. Sidi Ahmed, Sidi Mohamed, and Sonny Zuhuda. "Data Protection Challenges in the Internet of Things Era: An Assessment of Protection Offered By Pdpa 2010." *International Journal of Law, Government and Communication* 4, no. 17 (2019): 01–12. <https://doi.org/10.35631/ijlgc.417001>.
16. Southgate, Laura. "ASEAN: Still the Zone of Peace, Freedom and Neutrality?" *Political Science* 73, no. 1 (2021): 31–47. <https://doi.org/10.1080/00323187.2021.1967762>.
17. Tampubolon, Trisa, and Rizki Ramadhan. "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara." *Padjadjaran Journal of International Relations* 1.3 (2020): 270-286.

18. Thuy, Nguyen Xuan. “ Diversity of Legal Culture in Southeast Asian Countries ( ASEAN ) ” 9, no. April (2020): 1–7.
19. Vlahou, Antonia, Dara Hallinan, Rolf Apweiler, Angel Argiles, Joachim Beige, Ariela Benigni, Rainer Bischoff, et al. “Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics?” *Hypertension* 77, no. 4 (2021): 1029–35. <https://doi.org/10.1161/HYPERTENSIONAHA.120.16340>.
20. Zhu, Xiangyu, and Yang Yang. “Big Data Analytics for Improving Financial Performance and Sustainability.” *Journal of Systems Science and Information* 9, no. 2 (2021): 175–91. <https://doi.org/10.21078/JSSI-2021-175-17>.

### Internet online

Bangkok Post, Lazada denies being behind data leak, November 21, 2021 access through <https://www.bangkokpost.com/thailand/general/2023111/lazada-denies-being-behind-data-leak>.

Inquirer.net “Over 1M records from NBI, PNP, other agencies leaked in massive data breach” access through <https://newsinfo.inquirer.net/1758456/over-1-million-records-from-nbi-pnp-other-agencies-leaked-in-huge-data-breach#ixzz8126OAzLG>  
Malay Mail, “Major data breaches in Malaysia in the past 24 months”, 31 Dec 2022, access through <https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722>

VN, “Vietnam has major data leak problem, citizens suffer” August 19, 2022, access through <https://e.vnexpress.net/news/news/vietnam-has-a-big-data-leak-problem-4501707.html>

IT News “Singapore public sector saw 178 data breaches in 2021”, August 1, 2022 access through <https://www.itnews.asia/news/singapore-public-sector-saw-178-data-breaches-in-2021-583428>