

Comparison Of Personal Data Protection Laws Indonesia and Thailand

Wardah Yuspin^{1*}, Miranti Kusretno Tampawestri², Ridho Bawana Jati³

^{1,2,3} Faculty of Law, Universitas Muhammadiyah Surakarta, Indonesian

*Correspondence: wy204@ums.ac.id

HISTORY ARTICLE

Received: 01.04.2025

Accepted: 05.06.2025

Published: 29.06.2025

ARTICLE LICENSE

Copyright © 2025 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution ShareAlike 4.0 International (CC BY-SA 4.0)

ABSTRACT

The era of globalization puts information technology in an important position because it can create a part of the world without any restrictions, distance, space, and time and can increase work productivity and time efficiency. The importance of personal data protection has become stronger by increasing number of cell phone and internet users. The emergence the leakage of personal data realizes the protection of personal data is very important because it involves the concept of one's privacy. This research uses juridical-normative approach method by examining and analyzing legal aspects and comparing laws and using descriptive research type. This research aims to examine at Indonesian and Thai laws protecting personal data in providing sanctions for personal data violators and personal data supervisors. Indonesia has not officially had a personal data protection supervisory body in the PDP Law has not regulated a special supervisory body for personal data protection. In Thailand's PDPA, the supervisory body is clearly regulated. Sanctions for violators of personal data protection in the PDP Law and PDPA both have criminal and administrative.

Keywords: Personal Data, Protection, Comparison.

1. Introduction

The era of globalization puts information technology in an important position because it can create a part of the world without any restrictions, distance, space, and time and can increase work productivity and time efficiency. Information technology changes people's lives and causes rapid socio-cultural, economic, and legal changes (Wulansari, 2020).

The importance of protecting personal data has become a major issue with the increase in the number of mobile phone and internet users. The number of cases have emerged, especially those related to the leakage of one's personal data and leading to fraud or pornographic crimes, reinforcing the discourse on the importance of creating legal rules to protect personal data. The definition of personal data protection is related to the concept of privacy that need to be protect. The concept of privacy itself is the idea of maintaining personal integrity and dignity from others misconduct (Djafar & Komarudin, 2014).

Personal data protection is all efforts to protect Personal Data in the series of Personal Data processing by guaranteeing the constitutional rights of Personal Data subjects (Indonesia, 2022). The application of personal data protection has more than 132 countries that have specific regulations governing the privacy and personal data of their citizens. In some ASEAN countries, there are also many that have special rules regarding personal data protection such as Malaysia, Singapore, Philippines and Thailand (Kurnia, 2022).

Indonesia is a country that adheres to the Civil Law legal system and Thailand also adheres to the Civil Law legal system where this legal system is the law obtaining binding force, because it is realized in regulations in the form of laws and arranged systematically (Nurhadianto, 2015). Thailand also has special regulations regarding Data Protection, in The Thailand Personal Data Protection Act B.E. 2562 enacted in 2019, in which was passed earlier than Law number 27 of 2022 concerning Protection of Indonesian Personal Data which was passed in September 2022 but the Thai PDP Law was delayed and only came into force as of June 2022. Indonesia gets a lot of cyber-attacks which from year to year always increases and several cases that occur in Thailand are the basis for making special regulations as a form of providing protection of personal data to its citizens (Yusuf, 2022).

Data leakage is something that is often found in the development in information technology systems today, where data is something that is very confidential but easy to steal. The state has to provide protection to its citizens by making special regulations concerning the protection of personal data in which also contain sanctions imposed on violators and the State makes a supervisory body to protect data whose job is to supervise and enforce data protection regulations (Doly, 2021).

Previous research on personal data protection is by F. Yudhi Priyo Amboro and Viona Puspita on "Legal protection of personal data (comparative study of Indonesia Law in Indonesia: A Comparative Study of English and Malaysian Law", Nadiyah Tsamara's research "Comparison of Privacy Protection Rules on Personal Data Between Indonesia and Several Countries", Siti Yuniarti's research "Legal Protection of Personal Data in Indonesia".

This research when compared to previous studies has a difference where this research is new which discusses the comparison of Data Protection Laws between Indonesia and Thailand which discusses the Personal Data Protection Supervisory Agency and what sanctions are imposed on violators. This research has a reason to conduct a comparison of personal data protection regulations,

namely because Indonesia and Thailand are countries located in Southeast Asia and both countries have had a bill on personal data protection for a long time and finally enacted regulations on data protection in 2022.

Based in the above background, the problem discussed in this research is How are the sanctions For violators of personal data protection and the implementation of a special body for supervising personal data protection in the PDP Law between the State of Indonesia and the State of Thailand?

2. Research Methods

This research employs a normative method, commonly used in legal studies, by examining legal texts such as statutes and regulations to understand the meaning and application of rules within the prevailing legal system (Negara, 2023). Furthermore, the approach deemed most appropriate for examining and comparing the legal norms applicable in Indonesia and Thailand is a comparative legal approach. Through this approach, researchers can observe similarities and differences in the legal systems of the two countries, while simultaneously assessing the impact of these differences (Pitriani, 2024). Furthermore, this research also aims to develop legal theory, explore basic principles, and assess the relevance of legal rules to societal dynamics, through a literature review and interpretation of applicable regulations (Chuasanga & Victoria, 2019).

3. Results and Discussion

3.1 Results

Legal sanctions are an important instrument in ensuring the effectiveness of personal data protection. The law aims to regulate societal behavior and protect citizens' rights, both through written and unwritten rules. In Indonesia, constitutional guarantees for the protection of self, family, honor, and property are stipulated in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution. This provision serves as an important basis for the application of sanctions for violations of the right to personal data, as is also regulated in the Thai legal system.

Law is a rule whose purpose is to regulate the behavior of society which is usually purred into written and unwritten regulations. In all countries, providing protections to citizens is an obligation. Indonesia is a country that strongly protects the rights of its citizens as stated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which reads:

"Every person shall have the right to the protection of his or her person, family, honor, dignity and property under his or her control, and shall have the right to security and protection from threats of fear to do or not to do something which is a human right" (MK, 1945) and Article 28H paragraph (4) which reads:

"Everyone has the right to private property and such property shall not be expropriated by aby person." (MK, 1945) The existence of the Constitution proves that the Indonesian state fully protects its citizens.

Law No. 12/2005 on the Ratification of the International Covenant on Civil and Political Rights regulates the limitations of the authority of law enforcement officers to conduct secret surveillance of citizens, among others as stated in Article 17, which states that:

(1) No one shall have his private, family, home or correspondence arbitrarily or unlawfully interfered with, or

- his honor and good name unlawfully invaded
(2) Everyone is entitled to legal protection against such interference or attacks.

From this description, it can be seen that the state of law and human rights have. A relationship that is not only formal but also material, which means that the material relationship is that the attitude of actions by State administrators must be based on the rule of law (Nasution & Zen., 2006).

The protection of personal data is realized by the government with the creation of the Personal Data Protection Law in 2019 and the purpose of this law is ensuring citizens' rights regarding personal data protection and rising public awareness also respect for the prominence of personal data protection. From 2019 the Indonesian PDP Bill has also not been passed due to differences of opinion between the DPR and the government regarding the position of the personal data protection supervisory authority (Indonesia, 2021).

In September 2022 Law Number 27 of 2022 concerning Personal Data Protection was finally passed and signed by President Joko Widodo and came into force on October 17, 2022 with the aim of protecting people's personal data so as to minimize misuse from irresponsible individuals. This PDP Law is given a transition period regarding data controllers, data processors and parties related to processing personal data until October 17, 2024 so that they can adjust to this Law. After the transition period is over, all parties are required to comply with the rules and any non-compliance will be subject to sanctions (Prastyanti, Rahayu, Yafi, Wardiono, & Budiono, 2022).

This personal data protection law is not only owned by Indonesia but there are many other countries that have regulations regarding personal data protection, namely the UK with GDPR, China, Japan, Hong Kong, Taiwan, then in ASEAN there are Singapore, Malaysia, Thailand, and the Philippines.

The Thai government deemed it necessary to enact a special Act on personal data protection. The Thailand Personal Data Protection Act B.E 2562 (PDPA) was enacted to protect individuals from authorized or unlawful collection, use or disclosure of their personal data. The enactment of the PDPA will initially come into force on the day after the date of publication in the Government Gazette (Greenleaf & Suriyawongkul, 2020) 11 on May 27, 2019 with a grace period of one year so that it is planned to come into force in 2020 as stated in Article 2 of the Thai PDP Act which reads:

"This Act shall come into force on the day after the date of its publication in the Gazette, except for the provisions of Chapter II, Chapter III, Chapter IV, Chapter V, Chapter VI, Chapter VII, and section 95 and section 96, which shall come into force after the lapse of one year from the date of its publication in the Gazette" (Greenleaf & Suriyawongkul, 2020). However, due to COVID-19, the Thai government made a decision to extend the deadline period until June 1, 2022.

PDPA Thailand is a regulation made by the Thai government to ensure the protection of personal data. Thailand's PDPA adheres to the 2016 General Data Protection Regulation (GDPR) so the PDPA has similarities. Prior to the issuance of the PDPA in 2019 Thailand did not have specific laws governing data privacy and data protection issues, but privacy rights were regulated in The Civil and Commercial Code (CCC) which specifically regulates financial services and telecommunications (Bumpenboon, 2020).

The PDPA applies to the provision of products or services in Thailand, outlining the commitments of data controllers and processors to inform and request data owners about any collection, use or disclosure of their personal information. Where a data subject discovers violations in data use, data disclosure the controller or processor may be subject to administrative and criminal fines. As such, the PDPA defines personal data as information that identifies a living person (Dhea Rizqi Karisma & Lina Nugraha Rani, 2023).

Both Thai and Indonesian personal data protection laws emphasize the importance of protecting data subjects' rights through effective sanction mechanisms. Thailand's PDPA explicitly regulates restrictions on individual rights and freedoms in order to efficiently protect personal data and provide more effective remedies for data subjects whose rights are violated. On the other hand, Indonesia's Personal Data Protection Law must be able to protect the interests of the Indonesian public by addressing various legal issues that have arisen and will arise, and broadly encompassing public activities related to personal data, as personal data protection regulations in Indonesia evolve (Mays, 2022). The Law regulates the types of Personal Data, among others, as stated in Chapter III Article 4, which states that:

- (1) Personal Data consists of:
 - a. Specific Personal Data; and
 - b. Personal Data of a general nature.
- (2) Specific Personal Data as referred to in paragraph [1] letter a includes:
 - a. Health;

- b. Biometric;
 - c. Genetic;
 - d. Criminal document;
 - e. Child data;
 - f. financial data; and / or
 - g. Other data in accordance with the provisions of laws and regulations.
- (3) General Personal Data as referred to in paragraph [1] letter b includes:
- a. Full name;
 - b. Gender;
 - c. Nationality;
 - d. Religion;
 - e. Marital status; and /or
 - f. Combining data to identify individual.

The regulation of the PDP Law is to provide limitations on the rights and obligations of every act of acquisition and utilization (management) of all types of personal data both carried out in Indonesia and personal data of Indonesian citizens abroad, whether carried out by individuals or legal entities.

Thailand's PDPA governs the collections, apply and disclosure of personal data (collectively, data processing acts) by data controllers or data processors in Thailand, regardless of whether the data processing acts are performed in the country (Srisawatsakul, Boontarig, & Quirchmayr, 2023).

Thailand's PDPA defines personal data as any information to identify person, directly or indirectly, but does not include information about a passed person (Greenleaf & Suriyawongkul, 2020).

There are two types of personal data – general personal data and specific data. General personal data consists of any types of personal data that is not sensitive data. However, the PDPA does not clearly explain that what constitutes sensitive data but the PDPA section 26 explains that for the collection of on race, racial origin, political opinions, cults, religious or philosophical beliefs, sexual behavior, criminal records, disabilities, trade union information, health data, genetic data, biometric data, and other information that may have a similar impact on the data subject (Dhea Rizqi Karisma & Lina Nugraha Rani, 2023).

Considering the importance of protecting personal data, both general and sensitive, such as health data, biometrics, and political and religious beliefs, it is necessary to apply proportional sanctions to various forms of violations of the provisions of the personal data protection law in Indonesia and Thailand according to the level of violation committed (Setiawati, Permata Dewi, & Ayu Astutik, 2024). The application of witnesses in addition to providing a deterrent effect is also applied to provide education to change people's behavior to understand more about the importance of respecting privacy rights over personal data. Sanctions can be in the form of criminal sanctions and civil sanctions in the form of compensation. In every data protection law, every country applies witnesses considering the many cases of personal data theft that lead to criminal acts (K.Tus, 2021). The determination of the amount of sanctions can be formulated by adjusting to the applicable laws and regulations. The determination of sanctions needs to be equipped with a law enforcement mechanism that is adjusted to the provisions of the applicable laws and regulations in the country.

Law No. 27 Year 2022 on Personal Data Protection is divided into administrative sanctions and criminal provisions:

- (1) Administrative Sanctions (Article 57 of Law No. 27 of 2022) Imposition of administrative sanctions by supervisory institutions in the form of:
- a. Warning in writing;
 - b. Temporary suspension of personal data processing activities;
 - c. Deletion or destruction of Personal Data; and/or
 - d. Administrative fines

Sanctions in the form of administrative fines at a maximum of 2 (two) percent of annual revenue are imposed on the violating party. Further provisions regarding administrative sanctions will be regulated in a Government Regulation.

(2) Criminal Provisions

Article 67 of Law No. 27 of 2022 explains that:

1. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to

him/her, and with the intention of benefiting himself/herself or others which may result in harm to the data subject. Violation of this shall be punishable by a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp 5,000,000,000.00 (five billion rupiah).

2. Every person is prohibited from unlawfully disclosing personal data that does not belong to him/her. Violation of this shall be punishable by a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp 4,000,000,000.00 (four billion rupiah)
3. Every person is prohibited from unlawfully disclosing personal data that does not belong to him/her. Violation of this shall be punishable by a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah).

Article 68 explains: "Every person is prohibited from cheating false personal data or false personal data with the intention of benefiting themselves or others which may harm others. Violation of this shall be punished with the imprisonment of 6 (six) years and/or a maximum fine of Rp 6,000,000,000.00 (six billion rupiah)."

Article 69 explains that "Additional sanctions may also be imposed in the form of confiscation of profits and/or assets obtained or proceeds of criminal acts and payment of compensation".

Article 70 also regulates criminal offenses committed by legal entities, stipulating that the criminal sanctions imposed are only in the form of fines. The fine will be imposed on the management, supervisors, coaches, beneficial owners, and/or the corporation itself. Administrative fines for legal entities can reach 10 (ten) times the maximum fine for individuals.

In addition to fines, legal entities may be sentenced to additional punishment in the form of:

- a. Forfeiture of profits and/or assets obtained or resulting from a criminal offense;
- b. Suspension of all or part of the Corporations' business;
- c. Permanent prohibition of certain acts;
- d. Closure of all or part of the place of business and/or corporate activities;
- e. Carry out obligations that have been neglected;
- f. Compensation;
- g. Cancellation of license; and/or
- h. Complete Closure of Corporation.

Thailand's PDPA has sanctions that will be applied in the event of non-compliance. The PDPA includes civil, criminal and administrative sanctions.

1) Civil/ Civil Sanctions) Section 77 PDPA B.E. 2562 (2019))

A Data Controller or Data Processor, whose operations in relation to Personal Data in violation of or failure to comply with the provisions of this Law cause damage to a data subject, shall compensate the data subject for such damage, regardless of whether such operations were performed intentionally or due to negligence, unless the data controller or Data Processor can prove that they resulted from:

- Force majeure or the data subject's own actions or omissions in action;
- Actions taken in accordance with the orders of government officials in carrying out their duties and authorities under the law.

Compensation covers all costs incurred by the data subject for the prevention of damage that may occur, or incurred to resolve damage that does occur.

Section 78 of the Thai PDPA also explains that the Court has the power to order the data controller or processor to pay damages as a punishment in addition to the compensation already awarded by the court, but shall not exceed 2 (two) times the amount of the actual compensation.

2) Criminal Sanctions

Section 79 of the Thai PDPA explains that:

- Any data controller who violates the law relating to personal data that is likely to cause another person to suffer harm, damage his/her reputation, or expose such other person shall be punished by imprisonment for not more than 6 (six) month, a fine of not more than 500,000 (five hundred thousand baht), or both.
- Any data controller who violates the provisions relating to unlawfully benefiting him/herself, or another person, shall

be punished by imprisonment for a term not exceeding 1 (one) year, a fine not exceeding 1,000,000 (one million baht), or both.

Section 80 of the Thai PDPA explains that:

- Any person who has knowledge of the Personal data of another person as a result of the person performing duties under this Act and discloses it to another person shall be punished with imprisonment not exceeding 6 (six) month, a fine not exceeding 500,000 (five hundred thousand baht) or both.

3) Administrative Sanctions

Administrative sanctions are set out in the Thai PDPA section 82 to section 90. The PDPC is authorized to order administrative fines up to a maximum of 3,000,000 (three million baht) for breaches concerning general data and 5,000,000 (five million baht) for breaches of sensitive data.

Judging from the sanctions that will be imposed on personal data violators in the State of Indonesia Thailand has a difference in which Thailand has civil, administrative and criminal sanctions whereas, Indonesia has administrative and criminal sanctions (Lestari & Mujib, 2022). In Thailand's administrative sanctions it is explained that if personal data violators impose fines on general data and sensitive data are differentiated, while administrative sanctions in Indonesia are imposed 2 (two) percent of the violator's annual income.

In accordance with the sanctions that exist in protecting personal data in Indonesia and Thailand both already have clear sanctions for violators whose sanctions have been adjusted to the laws in accordance with their respective countries which have the same goal of providing a deterrent effect on violators so that violations of personal data protection are minimal.

3.2 Personal Data Protection Supervisory Bodies in Indonesian and Thai Data Protection Laws

Adequate protection of privacy regarding data and personal data can realize public trust to provide personal data for various larger community interests without being abused or violating their personal rights. This law will thus create a balance between the rights of individuals and the community whose interests are represented by the state. The regulation of PDP will contribute greatly to the creation of order and progress in the information society (Shahrullah, Park, & Irwansyah, 2024).

The implementation of the Personal Data Protection Law requires the existence of a special commission tasked with ensuring the implementation of the Law. The Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection does not regulate the establishment of a commission that oversees the protection of personal data, but to realize the protection of personal data for data subjects, the State assigns the Ministry of Communication and Informatics to handle data privacy issues. To process and collect data, it is carried out by data controllers and data processors.

Article 4 of Law explains that the Controller of Personal Data is any person, public body, and international organization acting individually or jointly in determining the purpose and exercising control over the processing of Personal Data (Indonesia, 2022).

Article 1 point 5 explains that a Personal Processor is any person, public odd, and international organization acting individually or jointly in the processing of Personal Data on behalf of a Controller (Indonesia, 2022).

Data controllers and processors include individuals, public bodies and international organizations (Hintze, 2018). Data controllers and data processors in carrying out their duties have obligations that need to be fulfilled in order to be carried out in accordance with the PDP Law. The obligations of data controllers are contained in Articles 20 to 50 of Law No. 27 Of 2022. While the responsibilities of data processors are contained in Article 51 and Article 52. In contrast to the PDPA Thailand already has a special personal data watchdog commission called the Personal Data Protection Committee (PDPC) established to oversee the Minister of Digital Economy and Society has several key definitions contained in section 6 of the Thai PDPA:

- (1) "Personal Data" is defined as any information relating to a person, which permits the identification of that person, either directly or indirectly, but does not include information about a deceased person in particular.
- (2) "Data Controller" means a person (whether an individual or a legal entity) who has the authority and responsibility to make decisions on the collection, use or disclosure of Data.
- (3) "Data Processor" means a person (whether natural or legal) who gathers, practices or divulges Personal Data in accordance with the Data Controller's instructions or on behalf of the Data Controller.

The Thai government has appointed an agency to oversee compliance Law in accordance with the Act B.E. 2019 (Greenleaf & Suriyawongkul, 2020) as follows: 1. The Office of the Personal Data Protection Committee (PDPC) is tasked with preparing a master plan, establishing measures for the collection, use, and disclosure of information and educating the public, private and general public.

The expert panel will consider complaints, investigate, and mediate disputes and to be consistent with the Personal Data Protection Act BE 2562. The controllers must ensure that personal data remains accurate, current, complete and not misleading'. The PDPA also states that the personal collection of data should be limited to the extent necessary in relation to the legitimate purposes of the data controller. The data controller or data processor must provide appropriate security measures that meet the minimum standards specified by the PDPC, and review these measures as needed. The PDPA also provides that data controllers notify the PDPC of data breaches ("A Comparison of Data Protection Laws: Thailand," 2022). The PDPA stipulates that data controllers and data processors keep records of processing activities and provides exemptions from this obligation for small organizations. It also provides for the appointment of a DPO by a data controller or data processor (Vivitasevi, 2022).

Data controllers based outside country and involved in certain forms processing information, must appoint a Thailand-based representative in writing.

The Personal Data Protection Committee (PDPC) is tasked with drafting and issuing future sub-regulations. Previously, the PDPC was represented by the Ministry of Digital Economy and Society.

The PDPC has the following authorities and responsibilities:

- To ensure PDPA compliance, define operating procedures or strategies concerning to data protection;
- Reassure and assist in the safeguarding of personal information;
- Instruct under the PDPA; and
- Notify and set out the rules/ guidelines that controllers and processors of personal data must follow and comply with.

Judging from the Indonesian PDP Law, the Personal Data Supervisory Agency has not yet been officially established by the State, but the institution has been included in the Law and until now the Government Regulation has also not been issued. Thus, the current supervisory body is still the responsibility of the Minister of Communication and Information Technology, in contrast to Thailand's PDPA where the Personal Data Supervisory Body has been established in January 2022 which the supervisory body is under the supervision of the Minister of Digital Economy and Society, and is fully regulated in the PDPA.

Thailand's Personal Data Supervisory Agency which has been formed, also called the PDPC, whose powers and responsibilities are very clear in the PDPA, but the implementation of the supervisory body is still under the supervision of the Ministry of Economy and Digital Society, which means that it is not independent, which allows interference from other parties (Greenleaf & Suriyawongkul, 2020). Therefore, Indonesia should establish an Independent Personal Data Supervisory Agency so that there will be no interference from other parties (Doly, 2021).

4. Conclusion

Personal data is a right to privacy that must be protected by all people and the State. Legislation created specifically to provide protection for personal data in Indonesia has begun to be implemented since October 2022 after the long-designed PDP Law has come into force. A supervisory body to protect personal data is stipulated in this law but no official establishment of such a body has been made by the State. The supervisory body/ agency will be further regulated in a Presidential Regulation but until now the president has not issued the Regulation.

Thailand's PDPA has been in effect since June 1, 2022 after being inaugurated in 2019 and delayed until 2022 due to the COVID-19 pandemic. Thailand's PDPA regulates the personal data protection supervisory body which is quite complete from the structure of the body to the duties and powers as well as the election of the body. Judging from the two countries, the supervisory body that has been running to carry out its duties and authorities in the form of supervising data controllers and processors to carry out their duties in accordance with the law, creating strategies for personal data protection and implementing sanctions if there are violations committed, Thailand is more ready to create a supervisory body to protect personal data, while Indonesia is not ready for a supervisory body because until now there has been no special supervisory body that protects personal data. Kominfo has been carrying out the task of supervising data issues.

Sanctions imposed on violators of personal data protection in Indonesia are both criminal and administrative. However, Thailand has civil sanctions, which are specifically for data controllers or processors, which provide for sanctions to be imposed if the data controller or processors violates or fails to comply with this Act.

The criminal sanctions stipulated in the Indonesian PDP Law and Thai PDPA are good and have clearly formulated the imposition of imprisonment for violators of personal data protection.

Administrative sanctions in the Indonesian PDP Law and Thai PDPA are also good and have clearly formulated the imposition of administrative sanctions for violating general and sensitive data.

5. Speech Thank You

The authors would like to thank Universitas Muhammadiyah Surakarta for funding this research through PID Grant for research.

Bibliography

- A comparison of data protection laws: Thailand. (2022, July 13). Retrieved May 9, 2025, from Asia Business Law Journal website: <https://law.asia/thailand-data-protection-laws/>
- Bumpenboon, T. (2020). Thailand's Personal Data Protection Act: An Understanding from the Perspectives of the European Privacy Law. *Thammasat Review of Economic and Social Policy*, 6(1), 50–82.
- Chuasanga, A., & Victoria, O. A. (2019). Legal Principles Under Criminal Law in Indonesia Dan Thailand. *Jurnal Daulat Hukum*, 2(1), 131-138.
- Dhea Rizqi Karisma, & Lina Nugraha Rani. (2023). Comparison Analysis of Sustainable Banking Performance of Sharia Bank and Conventional Bank as Members of First Movers on Sustainable Banking in Indonesia Period 2017-2020. *Jurnal Ekonomi Syariah Teori Dan Terapan*, 10(5), 511–524. <https://doi.org/10.20473/vol10iss20235pp511-524>
- Djafar, W., & Komarudin, A. (2014). *Perlindungan Hak Atas Privasi Di Internet: Beberapa Penjelasan Kunci*. Jakarta: ELSAM.
- Doly, D. (2021). Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru. *Negara Hukum*, 12(2), 227.
- Greenleaf, G., & Suriyawongkul, A. (2020). Thailand – Asia's Strong New Data Protection Law. *SSRN Electronic Journal*, 4(February 2019), 3–6. <https://doi.org/10.2139/ssrn.3502671>
- Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3192721>
- Indonesia. Undang-undang RI No 27 Tahun 2022. , Pub. L. No. Undang-Undang Nomor 27 Tahun 2022, Perlindungan Data Pribadi 1 (2022).
- Indonesia, D. P. R. R. (2021). Data Pribadi Presiden Bocor, Puan Ingatkan Komitmen Pemerintah Selesaikan RUU PDP. Retrieved February 3, 2023, from DPR.go.id website: <https://www.dpr.go.id/berita/detail/id/34440/t/Data+Pribadi+Presiden+Bocor%2C+Puan+Ingatkan+Komitmen+Pemerintah+Selesaikan+RUU+PDP>
- K.Tus, D. S. A. (2021). Perlindungan Hukum Bagi Korban Serangan Ransomware. *Vyavahara Duta*, 16(2), 126. <https://doi.org/10.25078/vd.v16i2.2909>

- Kurnia, A. (2022). UU PDP Hadirkan Ruang Digital yang Aman. Retrieved May 23, 2023, from Infopublik website: <https://www.infopublik.id/kategori/sorot-politik-hukum/673024/uu-pdp-hadirkan-ruang-digital-yang-aman>
- Lestari, Y., & Mujib, M. M. (2022). Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 11(2), 203. <https://doi.org/10.14421/sh.v11i2.2729>
- Mays, A. (2022). Protection of Personal Data in the Care Application. *Journal of International Trade, Logistics and Law*, 8(1), 23–27.
- MK. *Undang-Undang Dasar Republik Indonesia 1945*. , (1945).
- Nasution, A. B., & Zen., A. P. M. (2006). *Instrumen Internasional Pokok Hak Asasi Manusia* (3rd ed.). Jakarta: Yayasan Obor Indonesia.
- Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal*, 4 (1), 1–9. <https://doi.org/10.22219/aclj.v4i1.24855>
- Nurhadianto, F. (2015). Sistem Hukum Dan Posisi Hukum Indonesia. *Jurnal TAPIS*, 11(1), 34–45.
- Pitriani, R. N., Az-Zahra, S., Nasution, N. K. B., Yusuf, A. M., & Martakusuma, P. N. (2024). Perbandingan Hukum Administrasi Negara Indonesia Dan Negara Thailand.
- Prastyanti, R. A., Rahayu, I., Yafi, E., Wardiono, K., & Budiono, A. (2022). Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia. *Jurnal Jurisprudence*, 11(1), 82–99. <https://doi.org/10.23917/jurisprudence.v11i1.14756>
- Setiawati, D., Permata Dewi, T., & Ayu Astutik, Z. (2024). Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins. *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang*, 7(2), 184–199. <https://doi.org/10.33474/yur.v7i2.21184>
- Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, 10(1), 1–20. <https://doi.org/10.20956/halrev.v10i1.5016>
- Srisawatsakul, C., Boontarig, W., & Quirchmayr, G. (2023). a Process Model for Data Protection Impact Assessment in Thailand'S Healthcare Sector. *ICIC Express Letters*, 17(1), 81–90. <https://doi.org/10.24507/icicel.17.01.81>
- Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, 3(1), 53. <https://doi.org/10.26740/jsh.v3n1.p53-84>
- Vivitasevi, C. (2022). A comparison of data protection laws: Thailand. Retrieved May 12, 2023, from Asia Bussiness Law Journal website: <https://law.asia/thailand-data-protection-laws/>
- Wulansari, E. M. (2020). Konsep Perlindungan Data Pribadi sebagai Aspek Fundamental Norm dalam Perlindungan terhadap Hak atas Privasi Seseorang di Indonesia. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, 7(2), 265–289. <https://doi.org/http://dx.doi.org/10.32493/SKD.v7i2.y2020.9214>
- Yudhi Priyo Amboro, F., & Puspita, V. (2021). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). *Combines- Conference on Management, Business, Innovation, Education and Social Sciences*, 1(1), 415–427. Retrieved from <https://journal.uib.ac.id/index.php/combines/article/view/4466>

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *JURNAL BECOSS (Business Economic, Communication, and Social Sciences)*, 1(1), 147–154. <https://doi.org/https://doi.org/10.21512/becossjournal.v1i1.6030>

Yusuf. (2022). Menkominfo: RUU PDP Disahkan, Kominfo Awasi Tata Kelola Data Pribadi PSE. Retrieved June 13, 2023, from Kominfo RI website: <https://aptika.kominfo.go.id/2022/09/menkominfo-uu-pdp-disahkan-kominfo-awasi-tata-kelola-data-pribadi-pse/>