ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective

Lu Sudirman [1)], Hari Sutra Disemadi [2)], Arwa Meida Aninda [3)]
[1, 2, 3)] *Faculty of Law, Universitas Internasional Batam, Indonesia*
Baloi-Sei Ladi, Jl. Gajah Mada, Tiban Indah, Kec. Sekupang, Kota Batam, Kepulauan Riau 29426
Corresponding Author: Arwa Meida Aninda, Email: 2051026.arwa@uib.edu

History: Received 27/10/2023 | Revised 30/10/2023 | Accepted 06/11/2023 | Published 30/11/2023

Abstract. The existence of violations of personal data remains a legal issue at present. The protection of personal data is of utmost importance, serving not only as a safeguard but also as the foundation for comprehensive regulations concerning personal data. This research aims to compare regulations on personal data protection between Indonesia and Thailand, with a particular emphasis on human rights aspects. The research methodology used is normative legal research. The findings of this study reveal that both Indonesia and Thailand recognize that personal data protection is an integral part of human rights. This acknowledgment is reflected in their respective constitutions and various applicable laws. Indonesia recently enacted specific legislation on personal data protection in 2022, but its implementation still faces various challenges. The results of this research indicate that while both countries recognize the significance of personal data protection as a component of human rights, there are significant differences in their approaches and implementations between Indonesia and Thailand.

Keywords: *Comparative Law; Personal Data Protection; Human Rights*

INTRODUCTION

In Indonesia, violations of personal data usage often occur, particularly in the banking sector (Kusuma & Rahmani, 2022; Ningrum, & Robekha, 2023), as exemplified by the banking crime of skimming (data theft) that befell Bank Rakyat Indonesia (BRI) customers in the city of Mataram in 2016, affecting 515 customers (Cahyadi & Gorda, 2019). In the realm of healthcare, the proliferation of E-health programs, which are technology-driven applications in the healthcare sector aimed at improving access, efficiency, effectiveness, and the quality of medical processes, has been observed (Rosadi, 2016). These E-health services, which involve the collection of sensitive patient data, can give rise to new legal challenges, particularly when healthcare service providers fail to safeguard patients' personal data, making it more susceptible to unauthorized access and dissemination. This legal issue is of paramount importance, as it contradicts the fundamental human right to privacy and the protection of personal data, which is safeguarded by international, regional, and national instruments (Utomo, Gultom, & Afriana, 2020). Furthermore, in the realm of online buying and selling transactions, a significant incident occurred in May 2020 when it was reported that 91 million Tokopedia user data were compromised and offered for sale on hacker forums for a price of US$5,000, resulting in a lawsuit against Tokopedia and the Ministry of Communication and Information Technology (KEMENKOMINFO) by the Indonesian Consumers Community (Komunitas

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

Konsumen Indonesia or KKI) for an amount of 100 billion rupiahs (Delpiero, Reynaldi, Ningdiah, & Muthmainnah, 2021). A similar case unfolded in the e-commerce platform Bhinneka.com, where 1.2 million users experienced data breaches in 2020. The personal data of these users were freely traded by a group of hackers on the dark web, with the intent to profit from the sale of this data (Firmansyah Putri & Fahrozi, 2021; Mutiara & Maulana, 2020).

The dissemination of private data can occur due to negligence or service providers (Islamy et al., 2018; Winarso, Disemadi, & Prananingtyas, 2020; Disemadi, 2022a). Many data breaches occur due to poor implementation or the lack of adequate security controls in both private companies and government organizations (Yel & Nasution, 2022). Furthermore, there are several factors that can potentially lead to data leaks, such as human error, cyberattacks, and inadequate supervision of personal data protection (Nanda & Widyaningsih, 2021). Firstly, the factor of human error. Human nature, which tends to engage in economic practices such as seeking free software or using pirated applications (often promising free trials or other bonuses), “compels” us to voluntarily enter personal data, such as phone numbers, on websites or applications that lack security guarantees. Often, we do this without realizing it, as a result of the increased use of online media (Ashari, 2022). Secondly, cyberattacks. These are criminal activities that damage, manipulate, and steal important information from an application or website (Parulian, Pratiwi, & Cahya Yustina, 2021). Cyber threats to the theft of personal data and information over the internet often occur due to the lack of regulations in place to protect personal data. According to the publication of The Global Cybersecurity Index (GCI) 2017 by the International Telecommunication Union (ITU), Indonesia's cybersecurity status still falls under the category of weak cybersecurity and is in the process of optimal improvement (Sudarmadi, Josias, & Runturambi, 2019). Thirdly, the lack of supervision, and some companies and government agencies are unaware of how to properly manage and secure data (Aswandi, Muchsin, & Sultan, 2020).

The importance of safeguarding against the misuse of personal data is crucial for security and forms the foundation of comprehensive regulations concerning personal data (Disemadi, 2021; Sautunnida, 2018; Tasman & Ulfanora, 2023). Many countries have been striving to enhance security requirements and incorporate them into their laws. However, a significant portion of security frameworks remains reactive and fails to address relevant threats (Yel & Nasution, 2022). Presently, in Indonesia, the Personal Data Protection Bill (RUU PDP) was recently enacted into law. This regulation is expected to provide a new ray of hope in addressing issues related to personal data protection in Indonesia. In contrast, Thailand

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

had already enacted the Personal Data Protection Act B.E. 2562 (2019) of Thailand (PDPA) in 2019 and has been utilizing it to shield its citizens from the misuse of personal data.

The paragraph discusses the academic legal research in the field of comparative law. Previous research has explored various aspects of data protection, such as a study on the comparison of personal data protection in Indonesia and Malaysia (Rizal, 2019), research on personal data protection as a fundamental norm in safeguarding an individual's privacy rights in Indonesia (Wulansari, 2020), personal data protection as a part of the human rights to personal protection (Mutiara & Maulana, 2020), the emergence of robust new data protection laws in Asia, particularly in Thailand (Greenleaf & Suriyawongkul, 2020), and some legal issues concerning biometric data protection in Thailand (Chuenpukdee, 2019). This study explores the newly implemented personal data protection regulations in Indonesia and compares them to the existing regulations in Thailand, offering theoretical and practical contributions. Theoretical benefits encompass a deeper comprehension of legal systems in both countries, revealing novel insights into their legal principles. Practically, this research promotes knowledge exchange between Indonesian and Thai communities in the legal context, enriching their understanding of their respective legal cultures and facilitating the adoption of best legal practices. The research article is divided into three key sections: the first section analyzes personal data violations in Indonesia and Thailand, the second section examines the regulations governing personal data protection in both countries, and the third section addresses personal data protection as a human rights concern.

RESEARCH METHODS

The research methodology employed in this study is a normative legal research method, which aims to expound upon the existing legal norms within the legal system (Tan, 2021; Noor, Arifin & Astuti 2023). The choice of this method is justified by the fact that this research intends to analyze a comparative study of the law (Disemadi, 2022b), specifically examining the comparison between the Personal Data Protection Law in Indonesia and Thailand. The approach adopted encompasses both legislative and conceptual perspectives. Secondary data, in the form of primary legal materials such as Law Number 27 of 2022 on Personal Data Protection in Indonesia and the Personal Data Protection Act B.E. 2562 (2019) of Thailand (PDPA), serve as the foundational sources.

DISCUSSION

Legal Framework for Personal Data Protection in Indonesia

The government has implemented regulations regarding personal data protection (Yuniarti, 2019; Niffari, 2020; Azhari &

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

Soetopo, 2023), although regulations concerning personal data prior to the enactment of the PDP Law were separately governed by several legislative provisions and only reflected general aspects of personal data protection (Hisbulloh, 2021; Sutrisna, 2021). These regulations can be found in various laws in Indonesia, including Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), Law Number 7 of 1971 concerning Basic Archival Provisions, Law Number 8 of 1997 concerning Company Documents, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Law Number 36 of 2009 concerning Health, Law Number 36 of 1999 concerning Telecommunications, and Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration (Anugerah & Indriani, 2018). According to research conducted by the Institute for Community Studies and Advocacy (ELSAM), there are at least thirty legal provisions regulating the obligation to provide personal data protection in Indonesia (Yuniarti, 2019). The Population Administration Law is one of the provisions that specifically govern the classification of personal data (Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013 concerning Population Administration Law). In other words, the Population Administration Law does not provide detailed regulations regarding the acquisition, processing, and storage of personal data (Rosmaini, Kusumasari, Lubis, & Lubis, 2018).

UU ITE establishes the framework for the protection of personal data obtained through electronic systems, as stated in Article 26 of the UU ITE. The consent of the data owner is a key element in the use of an individual's personal data (Sautunnida, 2018). According to Government Regulation No. 52 of 2000 concerning Telecommunications, which is the implementing regulation of the Telecommunications Law, the internet is categorized as a multimedia service, identified as a telecommunications service provider offering information technology-based services (Salsabila, Hosen, & Manik, 2022; Fikri, & Rusdiana, 2023). The law regulates several aspects related to information confidentiality. Article 22, for instance, prohibits any person from engaging in unauthorized, unlawful, or manipulative activities. Personal data protection within an electronic system under the UU ITE encompasses safeguards against unauthorized usage, protection by electronic system providers, and protection against illegal access and interference (Marune & Hartanto, 2021). Any person who violates this provision may be subject to legal action for the damages caused (Miranti, 2020).

Specific regulations regarding the protection of personal data in Indonesia were

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

recently enacted in October 2022 through Law Number 27 of 2022 on Personal Data Protection (PDP Law). The PDP Law's provisions primarily focus on safeguarding the personal data of every Indonesian citizen, whether they are located within Indonesia or abroad (Sudirman, Disemadi, Girsang, & Aninda, 2023). The introduction of the Personal Data Protection Law in 2022 signifies a significant step toward enhancing data privacy rights in Indonesia. Nevertheless, the challenges in effectively implementing and enforcing these regulations remain, as evidenced by the continuing incidents of personal data breaches. It is essential for the government, businesses, and relevant authorities to work collaboratively to establish robust mechanisms for enforcing data protection, raising awareness among the public, and ensuring that both individuals and organizations comply with the new legal framework. Addressing the existing gaps and bolstering the practical aspects of personal data protection will be crucial to ensuring the law's effectiveness and safeguarding individuals' privacy rights in the digital age.

Chapter I of the PDP Law defines personal data as information about individuals that can be directly or indirectly identify them, whether through electronic or non-electronic systems. This definition, articulated in Article 1, paragraph 1 of the PDP Law, emphasizes the importance of safeguarding personal data and preserving individuals' confidentiality and constitutional rights during its processing. Personal data controllers, as defined in Article 1, paragraph 4, are responsible for determining the purposes of data processing and controlling the entire process. In Chapter III, the PDP Law categorizes personal data into two distinct groups: specific and general. Specific personal data includes sensitive information, such as health data, biometric data, and criminal records, necessitating heightened protection due to their potential impact on privacy and rights. General personal data comprises basic information like name and gender, which, when combined, can still identify individuals. This careful categorization ensures tailored data protection with stricter measures for specific personal data, upholding privacy rights and the integrity of personal information.

The PDP Law, in its Articles 5 to 15, delineates the rights of individuals as subjects of personal data, including the right to information about the legal basis and purposes of data collection. Article 8 empowers data subjects to terminate data processing, while Article 44 mandates data controllers to destroy data in specific circumstances. Article 12, Paragraph 1 allows data subjects to seek compensation for violations, ensuring accountability in data processing. However, Article 15 enumerates five exceptions, restricting data subject rights in matters related to national defense, law enforcement, public interests, financial stability, and scientific research. This legal

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

framework seeks to balance individual data protection with compelling public interests, highlighting the complexity of modern data protection.

The PDP Law, as outlined in Article 65, strictly prohibits the acquisition or collection of personal data not belonging to oneself with the intent to benefit oneself or others, potentially causing harm to the data subject. Additionally, Article 66 explicitly forbids the creation or falsification of personal data for personal gain, potentially harming other individuals. The PDP Law enforces these prohibitions with specific sanctions, including imprisonment for up to 5 years and/or fines of up to 5 billion rupiah for unlawful data acquisition, up to 4 years and/or fines of up to 4 billion rupiah for data disclosure, and up to 5 years and/or fines of up to 5 billion rupiah for unauthorized data utilization, as well as up to 6 years and/or fines of up to 6 billion rupiah for data forgery. These stringent provisions underscore the law's commitment to safeguarding personal data and deterring any misuse, emphasizing the importance of respecting privacy and data integrity.

Legal Framework for Personal Data Protection in Thailand

The Personal Data Protection Act, B.E. 2562 (2019) (PDPA) in Thailand is a landmark piece of legislation designed to safeguard individuals from privacy violations by both government institutions and irresponsible entities (Calderwood & Popova, 2018). This consolidated data protection law, published in the Government Gazette of Thailand on May 27, 2019, and effective from May 27, 2020, represents Thailand's inaugural comprehensive data protection framework (OneTrust DataGuidanceTM, n.d.). The Thai Data Protection Law was formulated by the National Electronic and Computer Technology Center (NECTEC) in accordance with the OECD Guidelines on Privacy Protection and Cross-Border Flows of Personal Data, as well as the European Union Directives 95/46/EC on the protection of individuals concerning the processing of personal data. While the law's drafting was completed and ready for Cabinet approval, various technical delays have hindered its formal enactment. The onset of full implementation of the Smart ID card project in mid-2005 prompted questions among the public regarding whether the enforcement of the Data Protection Law should precede the government's distribution of smart ID cards (Kitiyadisai, 2005).

There are several related regulations governing personal data privacy in Thailand, such as the Telecommunications Business Act, B.E. 2544 (2001), which regulates the licensing process for telecommunications operators. Concerning privacy, Article 74 prohibits any interception or disclosure of telecommunications data. Another relevant regulation is the Act on Computer Crime B.E. 2550 (2007), which addresses various cybercrimes, including computer data

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

interception, categorized into two offenses. Firstly, Section 7 imposes liability on individuals who illegally access computer data. Secondly, Section 8 explicitly prohibits the "interception" of computer data during transmission within a computer system. Consequently, both stored and contemporary data are prohibited under the Act on Computer Crime B.E. 2550 (Greenleaf & Suriyawongkul, 2020).

The Personal Data Protection Act, B.E. 2562 (2019), also known as PDPA, received royal approval from His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira Klao Chao Yu Hua on May 24, 2019. This legislation encompasses provisions related to personal data. Personal data is defined as any information concerning an individual that allows for their direct or indirect identification, excluding specifically information related to deceased individuals. Furthermore, the PDPA introduces the terms "Data Controller" and "Data Processor." A Data Controller refers to a person or legal entity vested with the authority and responsibility to make decisions regarding the collection, use, or disclosure of personal data. On the other hand, a Data Processor is an individual or legal entity that operates in connection with the collection, use, or disclosure of personal data as instructed by or on behalf of the Data Controller, without being the Data Controller themselves (Wongphasukchot, 2017). Personal information is defined as data pertaining to an individual's specific personal matters, which includes identifiers that can be used to identify that person. Consequently, the concept of personal information is considered synonymous with privacy (Sairahu, 2019). Protected personal information includes financial status, health records, criminal records, employment records, fingerprints, photographs, voice recordings, and all other personal particulars. The right to access and rectify personal data held by government agencies is safeguarded under Articles 7, 9, 11, and 12 of the PDPA.

In the subsequent section, there exists the Committee for the Protection of Personal Data, composed of: 1) A Chairperson selected and appointed from individuals possessing specialized knowledge, skills, and experience in the fields of Personal Data protection, consumer protection, information and communication technology, social sciences, law, health, finance, or other relevant domains pertinent to and beneficial for the protection of Personal Data; 2) The Permanent Secretary of the Ministry of Digital Economy and Society, who shall serve as the Vice-Chair; 3) Five Directors, who hold positions as members, including the Permanent Secretary of the Office of the Prime Minister, the Secretary-General of the State Council, the Secretary-General of the Consumer Protection Board, the Director-General of the Department for the Protection of Rights and Freedoms, and the Attorney

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

General; and 4) Nine Honorary Directors, chosen and appointed from individuals renowned for their exemplary knowledge, skills, and experience in the fields of Personal Data protection, consumer protection, information and communication technology, social sciences, law, health, finance, or other relevant domains pertinent to and beneficial for the protection of Personal Data (Tilleke & Gibbins Team, 2022).

The General Provisions of Article 19 stipulate that Personal Data may not be collected, used, or disclosed without the explicit consent of the data subject, either before or at the time of such collection, use, or disclosure, unless permitted by the provisions of this Law or other applicable laws. Requests for consent must be explicitly made in written statements or through electronic means, unless it is not feasible due to the nature of the data. When seeking consent from the data subject, the Data Controller must also inform them of the purpose of collecting, using, or disclosing Personal Data. The request for consent must be presented in a clear and distinguishable manner from other matters, in a format and statement that is easily accessible and understandable, using clear and simple language, and must not deceive or mislead the data subject regarding its purpose. In this regard, the Committee may require the Data Controller to seek consent from the data subject in accordance with the forms and statements as determined by the Committee. The Data Controller must fully consider that the consent of the data subject is given freely. Furthermore, the signing of contracts, including any terms of service, shall not be a condition for obtaining consent for the collection, use, or disclosure of Personal Data that is unnecessary or unrelated to the signing of such contracts, including terms of service. The data subject may withdraw their consent at any time. The withdrawal of consent shall be as easy as giving consent, unless there are restrictions on the withdrawal of consent under the law or contracts that confer benefits on the data subject. However, the withdrawal of consent shall not affect the collection, use, or disclosure of personal data that has been legally consented to by the data subject (Chuenpukdee, 2019).

The Data Controller has the duty to provide appropriate security measures to prevent the loss, unauthorized access, use, alteration, correction, or disclosure of Personal Data, and these measures must be reviewed as necessary or when technology has changed to efficiently maintain security and safety (Pandagle, 2023). It must also comply with the minimum standards set and announced by the Committee. In circumstances where Personal Data will be provided to individuals or legal entities other than the Data Controller, the Data Controller must take actions to prevent such individuals from using or disclosing the Personal Data unlawfully or without permission. They should implement a review system for the

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

deletion or destruction of Personal Data when the storage period expires, or when the Personal Data becomes irrelevant or beyond the necessary purpose for its collection, or when the data subject has requested it, or when the data subject withdraws consent, unless the storage of such Personal Data is for the purposes of freedom of expression, purposes under Article 24(1) or (4) or Article 26(5) (a) or (b), determination purposes, compliance or execution of legal claims, or defense of legal claims. The provisions in Article 33 paragraph five shall be used to govern the deletion or destruction of Personal Data mutatis mutandis. The Data Controller must inform the Office of any Personal Data breach without delay and, if possible, within 72 hours of becoming aware of it, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of individuals. If a Personal Data breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Controller must also notify the data subject of the Personal Data breach and the remedial actions without delay. Notification and exemptions from notification shall be carried out in accordance with the regulations and procedures established by the Committee. In the event that the Data Controller becomes a Data Processor under Section 5(2), the Data Controller must appoint in writing a representative of the Data Processor who must be located in the Kingdom of Thailand and authorized to act on behalf of the Data Controller without limitation of responsibility in connection with the collection, use, or disclosure of Personal Data for the purposes of the Data Controller (Areejitkasame, n.d.).

Protection of Personal Data as a Fundamental Human Rights

Privacy rights, a cornerstone of human rights, are vital for upholding human dignity (Firdaus, 2022; Noor & Manantan, 2022) and are explicitly outlined in Article 12 of the Universal Declaration of Human Rights (UDHR). This article safeguards individuals from arbitrary intrusion into their privacy, family, home, and correspondence, protecting their honor and reputation. It also extends to individuals' authority over their personal information and its use, emphasizing the concept of data protection. In Indonesia, while not explicitly mentioned in the constitution, Article 28G(1) of the 1945 Constitution acknowledges international Human Rights agreements' privacy values, forming a constitutional basis for privacy rights. However, Indonesia currently lacks specific regulations for personal data protection, relying solely on general regulations. Privacy rights, as a fundamental human right, play a crucial role in preserving human dignity, reinforcing humanitarian values, empowering individuals, and preventing discrimination and excessive government authority.

The protection of personal data is an essential aspect of human rights and plays a

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

crucial role in safeguarding personal identity. Indonesia recognizes personal data protection as a human right, evident not only in its constitution but also in various legal regulations. Human rights are inherent, natural, and fundamental rights that all individuals possess, and it is the duty of every person, community, and state to uphold and protect these rights (Triwahyuningsih, 2018). This involves maintaining a delicate balance between rights and responsibilities, as well as between individual interests and the common good. Consequently, respecting, protecting, and promoting human rights is a shared obligation among individuals, the government, and the state. Therefore, the pursuit of rights must always be accompanied by a commitment to fulfill responsibilities, and individual interests should not come at the expense of the broader community's well-being.

The protection of personal rights is regulated in Article 28G paragraph (1) of the 1945 Constitution of Indonesia, which states that “Every person has the right to the protection of their personal self, family, honor, dignity, and property under their control, as well as the right to security and protection from threats and fears to do or not do something that is a fundamental right.” While Article 28 of the 1945 Constitution does not explicitly mention privacy, it is closely related to the protection of personal rights or private rights, and the protection of personal self is realized through the protection of private rights (Mutiara & Maulana, 2020). Furthermore, in Law Number 39 of 1999 concerning Human Rights, there are several articles that emphasize this principle. Starting from Article 14 paragraph 2, Article 29 paragraph 1, Article 31, all state that the government must recognize and protect personal self, family, honor, dignity, and property rights, including personal information. Therefore, when the state fails to provide protection, it commits a human rights violation. Thus, personal rights as human rights, the protection of personal rights or private rights will enhance human values, improve the relationship between individuals and their communities, enhance autonomy or autonomy to exercise control and obtain justice, promote tolerance, and distance society from discrimination and government abuse of power (Budhijanto, 2010).

The Constitution of the Kingdom of Thailand 2017, known as "The People's Constitution," is a fundamental legal document consisting of 16 chapters and 279 articles. Chapter III, titled "Rights and Liberties of the Thai People," contains approximately 24 articles specifically addressing human rights, covering civil, political, economic, social, and cultural rights (Rahmah & Purnama, 2018). One significant aspect of human rights protection in this constitution is the recognition of the right to personal data privacy, as stated in Article 32, which emphasizes the protection of privacy,

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

dignity, reputation, and family. This aligns with the Personal Data Protection Act (PDPA), which grants Thai citizens various rights regarding their personal data, including deletion (Article 33), information disclosure (Articles 19, 21, and 23), objection (Article 32), access (Article 30), and data transmission (Article 31). In summary, "The People's Constitution" plays a vital role in safeguarding the human rights of Thai citizens, particularly concerning personal data privacy, reinforcing Thailand's commitment to upholding human rights in the digital era.

In both Indonesia and Thailand, the legal recognition of personal data protection is firmly entrenched within the framework of safeguarding human rights. These two nations acknowledge the intrinsic connection between the protection of personal data and the broader realm of human rights, thus underscoring their commitment to upholding individuals' fundamental rights and freedoms. The recognition of data privacy as an integral aspect of human rights demonstrates a shared commitment to navigating the complexities of the digital age while ensuring the dignity, privacy, and security of their citizens' personal information, reflecting their dedication to protecting human rights in the modern era.

CONCLUSION

The current era necessitates robust personal data protection due to rapid technological advancements and frequent data breaches. Indonesia and Thailand have enacted personal data protection laws, aiming to grant individuals control over their data and ensure privacy, aligning with constitutional principles. These legislations emphasize a delicate balance between data-driven innovation and safeguarding personal information, imposing stringent standards on data handlers. Independent data protection authorities oversee enforcement, enhancing trust in the digital ecosystem and supporting sustainable economic growth in an increasingly data-centric world.

REFERENCES

[1] Anugerah, D. P., & Indriani, M. (2018). Data protection in financial technology services (a study in Indonesian legal perspective). *Sriwijaya Law Review*, 2(1), 82–92. https://doi.org/10.28946/slrev.Vol2.Iss1.107.pp82-92

[2] Areejitkasame, K. (n.d.). Individual Control over Alternative Credit Data via Notice-and-Consent Mechanism under the Thai Personal Data Protection Law Kriengsak Areejitkasame. 211–250.

[3] Ashari, M. (2022). Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi.

[4] Aswandi, R., Muchsin, P. R. N., & Sultan, M. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*, 3(2), 167–190. https://doi.org/https://doi.org/10.20956/jl.v3i2.14321

[5] Budhijanto, D. (2010). *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi* (PT. Refika Aditama, Ed.). Bandung.

[6] Cahyadi, I. K. P., & Gorda, A. A. . N. S. R. (2019). Perlindungan Hukum Terhadap Nasabah dari Ancaman Perbankan Skimming Melalui Layanan Electronic Banking (Studi Kasus Di Bank Rakyat Indonesia Kantor Wilayah Denpasar). *Jurnal Analisis Hukum*, 2(2), 116–128.

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

https://doi.org/https://doi.org/10.38043/jah.v2i2.2208

[7] Calderwood, F., & Popova, I. (2018). *Smartphone Cyber Security Awereness in Developing Countries: A Case of Thailand.* In R. Zitouni & M. Agueh (Eds.), *Emerging Technologies for Developing Countries*. Cotonou.

[8] Chuenpukdee, P. (2019). *Some Legal Issues of Biometric Data Protection in Thailand.* Thammasat University.

[9] Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law*, 9(1).

[10] Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177–199. https://doi.org/10.25072/jwy.v5i2.460

[11] Disemadi, H. S. (2022a). Data Ownership in Regulating Big Data in Indonesia through the Perspective of Intellectual Property. *Jurisdictie: Jurnal Hukum Dan Syariah*, 13(2), 188–209. https://doi.org/10.18860/j.v13i2.17384

[12] Disemadi, H. S. (2022b). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, 24(2), 289–304. https://doi.org/10.37253/jjr.v24i2.7280

[13] Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 4(2), 23–31. https://doi.org/10.52005/rechten.v4i2.98

[14] Firmansyah Putri, D. D., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com). *Borneo Law Review*, 5(1), 46–68.

[15] Greenleaf, G., & Suriyawongkul, A. (2020). Thailand – Asia's Strong New Data Protection Law. *SSRN Electronic Journal*, 4, 3–6. https://doi.org/10.2139/ssrn.3502671

[16] Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, 37(2), 119. https://doi.org/10.26532/jh.v37i2.16272

[17] Islamy, I. T., Agatha, S. T., Ameron, R., Fuad, B. H., Evan, & Rakhmawati, N. A. (2018). Pentingnya Memahami Penerapan Privasi Di Era Teknologi Informasi. Jurnal Teknologi Informasi Dan Ilmu Komputer, 5(3), 305.

[18] Kitiyadisai, K. (2005). Privacy rights and protection: Foreign values in modern Thai context. *Ethics and Information Technology*, 7(1), 17–26. https://doi.org/10.1007/s10676-005-0455-z

[19] Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI : Jurnal Hukum,* 5(1), 46–63. https://doi.org/10.36441/supremasi.v5i1.721

[20] Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, 2(4), 143–152. https://doi.org/10.46336/ijbesd.v2i4.170

[21] Miranti, F. W. (2020). *Perlindungan Data Pribadi Terhadap Kejahatan Cyberspace Di Era Revolusi 4.0.* Universitas Muhammadiyah Purwokerto.

[22] Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Data Diri. *Indonesian Journal of Law and Policy Studies*, 1(1), 42–54. https://doi.org/10.31000/ijlp.v1i1.2648

[23] Nanda, S. E., & Widyaningsih, W. (2021). Pengaruh Terpaan Berita Peretasan Tokopedia Terhadap Reputasi Perusahaan. *BroadComm*, 3(1), 12–22. https://doi.org/10.53856/bcomm.v3i1.215

[24] Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Hukum Dan Bisnis (Selisik)*, 6(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

[25] Ningrum, D. P. S., & Robekha, J. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, 2(4), 765–776.

[26] Noor, E., & Manantan, M. B. (2022). *Raising Satandards Data and Artificial Intelligence in South East Asia.*

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

[27] Noor, A., Arifin, M., & Astuti, D. P. W. (2023). Crypto Assets and Regulation: Taxonomy and Framework Regulatory of Crypto Assets in Indonesia. *JED (Jurnal Etika Demokrasi)*, 8(3), 303-315.
[28] OneTrust DataGuidanceTM. (n.d.). *Comparing privacy laws : GDPR v. Thai Personal Data Protection Act.* Blumenthal Richter & Sumet (BRS).
[29] Pandagle, V. (2023). *Desorden Hacker Group Claims 198GB Data Breach at AIS Thailand.*
[30] Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies* (TELNECT), 1(2), 85–92.
[31] Rahmah, C. A. M., & Purnama, E. (2018). Studi Perbandingan Jaminan Perlindungan Terhadap Hak Asasi Manusia Tentang Kebebasan Beragama Di Negara Republik Indonesia dan Negara Kerajaan Thailand. *Jurnal Ilmiah Mahasiswa Bidang Hukum Kenegaraan*, 2(4), 745–756.
[32] Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, 10(2), 218–227. https://doi.org/10.26905/idjch.v10i2.3349
[33] Rosadi, S. D. (2016). Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi. *Arena Hukum*, 9(3), 403–420. https://doi.org/10.21776/ub.arenahukum.2016.00903.6
[34] Rosmaini, E., Kusumasari, T. F., Lubis, M., & Lubis, A. R. (2018). Insights to develop privacy policy for organization in Indonesia. *Journal of Physics: Conference Series*, 978(1). https://doi.org/10.1088/1742-6596/978/1/012042
[35] Sairahu, T. (2019). Factors Influencing Electronic Personal Data Protection Management and Development of Financial Institutes in Thai Banking Association. *International Academic Multidisciplinary Research Conference in Los Angeles* 2019, 36–40.
[36] Salsabila, R., Hosen, M., & Manik, H. (2022). Perlindungan Hukum Kerahasian Data Pribadi Konsumen Pengguna Produk Provider Telekomunikasi di Indonesia. *Zaaken: Journal of Civil and Business Law*, 3(1), 65–75. https://doi.org/10.22437/zaaken.v3i1.15968
[37] Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159
[38] Sudarmadi, D. A., Josias, A., & Runturambi, S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 2(2), 157–178.
[39] Sudirman, L., Disemadi, H. S., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. *Sang Sewagati Journal*, 1(2), 66-90.
[40] Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia. *Wacana Paramarta Jurnal Ilmu Hukum*, 20(5), 1–23.
[41] Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463–2478.
[42] Tasman, & Ulfanora. (2023). Perlindungan Hukum Terhadap Nasabah Bank dalam Transaksi Digital. *Unes Law Riview*, 6(1), 15. https://doi.org/10.52947/morality.v9i1.321
[43] Tilleke & Gibbins Team. (2022). *Thailand Establishes Personal Data Protection Commission.*
[44] Triwahyuningsih, S. (2018). Perlindungan Dan Penegakan Hak Asasi Manusia (HAM) Di Indonesia. *Legal Standing : Jurnal Ilmu Hukum*, 2(2), 113. https://doi.org/10.24269/ls.v2i2.1242
[45] Azhari, T. M. A. R., & Soetopo, M. G. S. (2023). Review of Legal Weakness on Protection of Personal Data in Online Transactions on Consumer-to-Consumer Concept in E-Commerce. *International Journal of Research in Engineering, Science and Management*, 6(1), 12–16.
[46] Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia. *Jurnal Ilmiah Galuh Justisi*, 8(2), 168. https://doi.org/10.25157/justisi.v8i2.3479
[47] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection Of Private Data Consumers P2p Lending As Part Of E-Commerce Business In Indonesia. *Tadulako Law Review*, 5(2), 209–221.

ISSN: p-2540-8763 / e-2615-4374
DOI: 10.26618/jed.v%vi%i.12875
Vol: 8 Number 4, November 2023
Page: 497-510

[48] Wongphasukchot, I. (2017). Online Profiling And Data Protection In Thailand. *Master of Laws Program in Business Law*, 47–55.
[49] 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.
[50] Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39-57.
[51] Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, 6(1), 92–101. https://doi.org/10.59697/jik.v6i1.144
[52] Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 1(1), 147–154.