International Journal of Applied and Scientific Research (IJASR)
Vol. 4 No. 8, 2026: 607-622

Public Perceptions of Personal Data Security in Digital Service Utilization in Indonesia and Thailand: A Comparative Analysis of Regulatory Frameworks, Risks, and User Trust

Ar Rahiim Innash[1]*, Arista Candra Irawati[2], Vicentius Simon Suyanto[3], Sudijono Sastroatmodjo[4], Prattana Srisuk[5]
[1234]University Ngudi Waluyo
[5]Thai Global Business Administration College, Thailand
Corresponding Author: rahmiiinash@gmail.com[1]

A R T I C L E I N F O

Keywords: Personal Data, Public Perception, Digital Security, Indonesia PDP Law, Thailand PDPA, Digital Services

Received : 27, June
Revised : 28, July
Accepted: 30, August

A B S T R A C T

Digital transformation in Southeast Asia has increased public reliance on digital services while simultaneously heightening the risk of personal data breaches. This article analyzes public perceptions of data security in Indonesia and Thailand through a comparative approach covering regulations, recent incidents, and user trust frameworks. Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (PDP), while Thailand has implemented the Personal Data Protection Act (PDPA) since 2022. Public perception in both countries is shaped by three key factors: digital literacy, experiences with data breaches, and the effectiveness of law enforcement. Incidents such as the hacking of the Temporary National Data Center and tax data breaches in Indonesia have heightened public concern. Conversely, the imposition of administrative fines in Thailand demonstrates stronger enforcement of accountability. Public trust is heavily influenced by transparency, incident handling, and consistent law enforcement.

DOI: https://doi.org/10.59890/ijasr.v4i8.292
E-ISSN: 3025-7670
https://nvlmultitechpublisher.my.id/index.php/ijasr/index

INTRODUCTION

The digitalization of public and private services has transformed the way people in Indonesia and Thailand interact with the state, businesses, and social communities. In Indonesia, the Indonesian Internet Service Providers Association (APJII) reported that the number of internet users reached 221,563,479 in 2024, with an internet penetration rate of 79.5% (APJII & Indonesia, 2024). Meanwhile, DataReportal recorded 63.21 million internet users in Thailand at the beginning of 2024, representing an internet penetration rate of 88.0% (Team, 2024). While the high level of internet penetration has expanded the benefits of digital services, it has also increased exposure to risks associated with personal data breaches, including identity theft, digital fraud, phishing, misuse of population data, and the trading of personal information on illegal forums. Data breach incidents throughout 2023-2024 in Indonesia (TEMPO, 2025), such as the alleged leak of civil registration data (Dukcapil), cyberattacks targeting PT Kereta Api Indonesia (PT KAI), breaches involving the National Civil Service Agency (BKN), ransomware attacks on the Temporary National Data Center, and the alleged leakage of Taxpayer Identification Number (NPWP) data (Katadata.co.id, 2024), demonstrate that personal data has become both a highly valuable asset and a prime target of cyberattacks.

Thailand has faced similar challenges, including the alleged sale of nearly 20 million Thai citizens' personal records in 2024, data breaches involving JIB customers, the alleged leakage of Senate candidate data, cyberattacks targeting Black Canyon's databases, and claims of stolen data belonging to Central The 1 Card members (ASIA-PACIFIC, 2025). However, Thailand has demonstrated greater progress in regulatory enforcement through the imposition of the first administrative fine under the Personal Data Protection Act (PDPA), amounting to THB 7 million on July 31, 2024, against a data controller company found to have failed to appoint a Data Protection Officer (DPO), implement adequate security measures, and provide timely notification of data breach incident. (Somwaiya et al., 2024) (Mondaq, n.d.). The central issue addressed in this article is how the public perceives the security of personal data when using digital services in two countries experiencing rapid digital growth while operating at different stages of regulatory enforcement. Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI, 2022), whereas Thailand is governed by the Personal Data Protection Act B.E. 2562 (PDPA 2019) ([Official Emblem of Royal Command] Personal Data Protection Act, B.E. 2562 (2019), 2019)

The widespread adoption of digital services has generated significant benefits, including greater efficiency, easier access to services, enhanced financial inclusion, expanded market opportunities, and improved social connectivity. However, at the same time, digitalization has also increased the risks associated with the misuse of personal data. These risks include data breaches, identity theft, online fraud, phishing attacks, unauthorized data processing, misuse of personal information by third parties, excessive tracking of user behavior, and a lack of transparency by digital platforms regarding the purposes for which data are collected and processed. In the e-Conomy SEA 2024 report, Google, Temasek, and Bain emphasized that maintaining digital trust is a critical factor for the sustainability of Southeast Asia's digital economy, particularly as online fraud remains a persistent challenge despite growing user awareness and the increasing implementation of anti-fraud controls. This highlights that the growth of the digital economy cannot be separated from issues of security and user trust. If individuals perceive that their personal data are not adequately protected, their participation in digital services may decline or be accompanied by significant concerns regarding privacy and security (Company, n.d.)

Thailand presents an interesting case due to its exceptionally high level of internet and digital service usage. The Digital 2025: Thailand report indicates that more than nine out of ten Thai residents are internet users, with an internet penetration rate of 91.2%. Furthermore, Thailand's digital economy ecosystem continues to expand, particularly through e-commerce, online travel services, digital payments, and digital financial services. The e-Conomy SEA 2024 report identifies e-commerce as one of the primary drivers of Thailand's digital economic growth. At the same time, government initiatives such as the digital wallet program, along with national strategies related to data centers and artificial intelligence, demonstrate a strong commitment to strengthening the country's digital infrastructure(Kemp, 2025a). This growth indicates that Thai citizens are increasingly engaging with digital services that require the collection, processing, and management of large volumes of personal data. Consequently, public perceptions of personal data security in Thailand warrant careful examination, as a high level of digital adoption does not necessarily correspond to an equally high level of trust in digital services or awareness of data protection issues. Understanding these perceptions is therefore essential for assessing the effectiveness of personal data protection frameworks and the sustainability of Thailand's rapidly evolving digital economy (Company, n.d.)

This issue has become increasingly urgent because perceptions of personal data security significantly influence user trust, intention to use digital services, willingness to share personal information, and compliance with security practices such as the use of multi-factor authentication, password management, and vigilance against suspicious links (Davis, 1989). From a theoretical perspective, these perceptions can be explained through the Technology Acceptance Model (TAM), which emphasizes perceived usefulness and perceived ease of use, as well as Privacy Calculus Theory, which suggests that individuals weigh the benefits of digital services against potential privacy risks before deciding to disclose their personal data (Dienlin, 2023). These developments have transformed personal data into a strategic asset, as nearly every digital interaction involves the collection, storage, processing, and exchange of user information. Such data may include names, addresses, telephone numbers, location data, transaction histories, consumption patterns, and even sensitive information such as health records and biometric data. In this context, personal data security is no longer merely a technical issue; rather, it has evolved into a broader social, legal, economic, and governance concern that directly affects public trust in the digital ecosystem.

From a regulatory perspective, Thailand has established a comprehensive legal framework for personal data protection through the Personal Data Protection Act B.E. 2562 ([Official Emblem of Royal Command] Personal Data Protection Act, B.E. 2562 (2019), 2019), commonly known as the Thailand PDPA. This legislation was enacted in 2019 and came into full effect on June 1, 2022, following several postponements of its implementation. The PDPA sets out the fundamental principles of personal data protection, including lawful bases for data processing, data subject consent, data subject rights, obligations of data controllers and data processors, and breach notification mechanisms in cases of personal data violations (Masagee & Boonnark, 2026). Thailand has further strengthened its data protection governance through the Personal Data Protection Master Plan 2024-2027, issued by the Personal Data Protection Committee (PDPC). The master plan emphasizes enhancing organizational compliance, reducing data breaches, increasing public awareness, developing PDPC electronic services, and strengthening Thailand's competitiveness in the field of personal data protection. Accordingly, Thailand can be regarded as a country that has progressed beyond the legislative stage and entered a phase characterized by the implementation and institutional strengthening of personal data protection measures (Lalitkomon et al., 2024).

However, the existence of regulatory frameworks does not automatically eliminate the risks of data breaches. In Thailand, the enforcement of the PDPA has begun to demonstrate significant progress. On July 31, 2024, Thai authorities imposed the first administrative fine under the PDPA, amounting to THB 7 million approximately USD 212,000, on a data controller company for violations involving a personal data breach, failure to appoint a Data Protection Officer (DPO), inadequate data security measures, and delayed notification of the incident to the Personal Data Protection Committee (PDPC). This case signals that personal data protection in Thailand has moved beyond a stage focused primarily on awareness and education and has entered a phase of more concrete legal enforcement. This development is highly relevant to the present study, as public perceptions of personal data security may be influenced by the extent to which regulations are perceived as effective, regulatory authorities are viewed as proactive, and digital service providers are regarded as accountable in safeguarding users’ personal information. Consequently, the effectiveness of regulatory enforcement may play an important role in shaping public trust and confidence in the protection of personal data within the digital environment (Somwaiya et al., 2024)

Indonesia has experienced similar developments in the field of personal data protection. The country enacted Law Number 27 of 2022 concerning Personal Data Protection PDP Law as its first comprehensive legal framework specifically governing the protection of personal data (Recording, 2026). The PDP Law came into force on October 17, 2022, with a two-year transition period, meaning that compliance obligations for data controllers and data processors became fully effective after October 17, 2024. Prior to the enactment of the PDP Law, personal data protection in Indonesia was regulated through various sectoral regulations, including those governing electronic systems, electronic transactions, the financial sector, and other administrative provisions(PIPER, 2026b) (PIPER, 2026a). The introduction of the PDP Law represents a significant milestone in strengthening the rights of data subjects, enhancing the obligations of data controllers, improving transparency in data processing activities, establishing consent mechanisms, and providing both administrative and criminal sanctions for certain violations. However, several challenges remain, particularly regarding the establishment of an independent personal data protection supervisory authority, the effectiveness of implementation and enforcement mechanisms, and the readiness of organizations to comply with personal data protection principles and regulatory requirements. Consequently, although Indonesia has made substantial progress in developing its legal framework for personal data protection, the effectiveness of its implementation continues to be a critical issue in ensuring public trust and safeguarding personal information within the digital ecosystem (PIPER, 2026a).

LITERATURE REVIEW

A comparison between Indonesia and Thailand is particularly important because both countries have enacted personal data protection regulations, yet they operate within different social, institutional, and levels of digital maturity. Indonesia has a very large internet user base, reaching approximately 212 million users in 2025 (Kemp, 2025a), which increases the likelihood that data breaches may affect a substantial portion of the population. Thailand, on the other hand, has a higher internet penetration rate of 91.2% (Kemp, 2025b), indicating a more widespread and evenly distributed use of digital services across its population. From a regulatory perspective, Thailand has fully implemented the Personal Data Protection Act (PDPA) since 2022 and has begun to demonstrate active enforcement through the imposition of administrative sanctions. In contrast, Indonesia has only recently entered the post-transition phase of its Personal Data Protection Law (PDP Law) following the end of the transition period in October 2024, while still facing challenges related to institutional strengthening and the development of implementing regulations (PIPER, 2026b). These differences provide an important basis for examining whether a more mature regulatory framework and more visible enforcement mechanisms can influence public perceptions of personal data security and shape the level of trust that individuals place in digital services (PIPER, 2026a).

In studies of digital service user behavior, perceptions of personal data security are closely linked to user trust. Trust is shaped not only by users' direct experiences with a platform but also by their knowledge of relevant regulations, the reputation of service providers, exposure to reports or personal experiences of data breaches, the transparency of privacy policies, and the extent to which users are able to control their personal information. Users who perceive that they have control over their personal data tend to be more comfortable using digital services, whereas those who do not understand how their data are collected, processed, and utilized may experience uncertainty and concern. In the context of digital services, a lack of trust can lead to protective behaviors, such as limiting the information shared with service providers, using alternative identities, avoiding certain digital transactions, or even refusing to use digital services that are perceived as risky. Therefore, studying public perceptions is of considerable importance, as data protection regulations and security technologies must not only exist formally but must also be understood, experienced, and trusted by users in order to effectively foster confidence in the digital environment.

A comparative study of Indonesia and Thailand is also highly relevant because, although both countries are located within the same region, they differ in their policy approaches and the characteristics of their digital markets. Thailand has introduced the Personal Data Protection Master Plan 2024-2027, which aims to enhance regulatory compliance, increase public awareness, and strengthen data governance across priority sectors such as e-commerce, telecommunications, finance, healthcare, tourism, education, and government services. These sectors are particularly data-intensive, relying heavily on the collection and processing of personal information. Indonesia likewise has a rapidly expanding digital sector, particularly in e-commerce, digital financial services, digital public services, and social media platforms. However, it continues to face challenges in rebuilding public trust following a series of data breach incidents and cases involving the misuse of personal information. Under these circumstances, this study can provide valuable insights into how people in the two countries perceive personal data security, whether primarily as a legal issue, a technical concern, a matter shaped by personal experience, or as an issue of trust in governmental institutions and digital service providers. By examining these perceptions comparatively, the study contributes to a deeper understanding of the factors that influence public confidence in personal data protection within rapidly evolving digital environments (Lalitkomon et al., 2024)

The research gap addressed in this article lies in the limited number of studies that directly compare public perceptions of personal data security in Indonesia and Thailand by simultaneously examining three interconnected dimensions: regulation, risk, and user trust. Existing studies tend to focus primarily on legal frameworks or organizational compliance, while the dimension of public perception has rarely been explored through a cross-country comparative perspective. In fact, the effectiveness of personal data protection depends not only on the existence of legislation but also on public awareness, trust in protection mechanisms, and users' experiences when interacting with digital services. By comparing Indonesia and Thailand, this study seeks to explain how differences in regulatory frameworks, levels of digital service adoption, and experiences with data-related risks shape public perceptions of personal data security. Such a comparative analysis is expected to contribute to a more comprehensive understanding of the relationship between regulatory development, perceived risk, and user trust in the digital environment, while also providing insights into the factors that influence public confidence in personal data protection in rapidly digitalizing societies

METHODOLOGY

This study employs a qualitative-comparative approach based on a literature review. Data were collected from regulations, official reports, legal articles, digital publications, and reports of data breach incidents in Indonesia and Thailand (Team, 2024). This approach is appropriate because the study aims to compare regulatory contexts and public perceptions based on patterns of risk, experiences with data breach incidents, and institutional responses in both countries. The primary sources utilized in this research include Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI, 2022), the Personal Data Protection Act B.E. 2562 (2019) of Thailand([Official Emblem of Royal Command] Personal Data Protection Act, B.E. 2562 (2019), 2019), the APJII Internet Survey Report 2024 (APJII & Indonesia), 2024), DataReportal Thailand 2024, as well as reports on data breach incidents obtained from media sources and legal institutions. The analysis was conducted in four stages: (1) identification of regulatory frameworks, (2) mapping of recent data breach cases, (3) analysis of factors influencing public perceptions, and (4) comparative assessment between Indonesia and Thailand. The validity of the analysis was strengthened through source triangulation, which involved comparing legal sources, digital statistical data, and case reports from multiple independent sources. This triangulation process was employed to enhance the reliability and comprehensiveness of the findings regarding personal data security perceptions in the two countries.

RESULTS AND DISCUSSION

Development of Digital Services in Indonesia and Thailand

Indonesia has a very large digital user base, with 221.56 million internet users in 2024 and an internet penetration rate of 79.5%. The size of Indonesia's digital population creates substantial opportunities for the growth of the digital economy; however, it also generates significant risks, as increasing volumes of personal data are collected and processed by e-commerce platforms, fintech services, public service systems, transportation applications, and social media networks (APJII & Indonesia), 2024). Thailand, by contrast, recorded a higher internet penetration rate of 88.0% at the beginning of 2024, with approximately 63.21 million internet users and 49.10 million social media users. The extensive use of the internet and social media in Thailand indicates a highly digitally connected society, making personal data protection a fundamental requirement for the secure and sustainable provision of online services (Team, 2024).

A key difference between Indonesia and Thailand lies in the level of institutional development and regulatory enforcement. Indonesia has already enacted the Personal Data Protection Law (PDP Law) (Deradjat et al., 2025); however, a dedicated supervisory authority is still undergoing institutional development and strengthening following the conclusion of the transition period. In contrast, Thailand has established the Personal Data Protection Committee (PDPC) and has begun demonstrating active administrative enforcement measures under the Personal Data Protection Act (PDPA) (Somwaiya et al., 2024). This distinction suggests that while both countries have adopted comprehensive personal data protection frameworks, Thailand has progressed further in terms of implementation and enforcement, whereas Indonesia remains in the process of consolidating its institutional capacity and regulatory mechanisms.

Public Perceptions of Personal Data Security in Indonesia

Public perceptions of personal data security in Indonesia tend to be shaped by collective experiences with numerous data breach incidents. Media reports in 2024 documented several major cases, including cyberattacks against PT Kereta Api Indonesia (PT KAI), disruptions affecting the General Elections Commission's (KPU) Sirekap system, data breaches involving Biznet and the National Civil Service Agency (BKN), a ransomware attack targeting the Temporary National Data Center (PDNS 2) in Surabaya, and the alleged leakage of Taxpayer Identification Number (NPWP) data (TEMPO, 2025); (Katadata.co.id, 2024). The PDNS incident attracted particular public attention because it affected hundreds of government agencies and public services, including immigration and educational services. This incident reinforced the perception that data breaches are not merely problems faced by technology companies but are also indicative of broader challenges in the governance and security of public information systems (Katadata.co.id, 2024). Within society, perceptions of risk are often reflected in concerns regarding the potential misuse of National Identification Numbers (NIKs), telephone numbers, addresses, taxpayer identification numbers, financial information, and biometric data for fraud, identity theft, or other illegal activities. When individuals perceive that government institutions or private organizations are not transparent in notifying the public about security incidents, their trust in digital services may decline (Dienlin, 2023). Transparency and accountability are therefore essential factors influencing public confidence in the digital ecosystem.

Despite these concerns, Indonesians continue to rely heavily on digital services for everyday activities, including payments, communication, employment, education, transportation, and access to government services. This situation illustrates the concept of privacy calculus, whereby individuals are willing to accept certain privacy and security risks because they perceive the benefits of digital services to outweigh the potential harms (Li et al., 2010). As a result, although concerns about personal data security remain significant, these concerns do not necessarily prevent users from engaging with digital platforms; instead, they influence the level of trust and caution with which digital services are utilized.

Public Perceptions of Personal Data Security in Thailand

In Thailand, public awareness of personal data protection has increased significantly since the Personal Data Protection Act (PDPA) came into full effect on June 1, 2022, and began to be enforced more actively. DLA Piper reported that Thailand launched its Personal Data Protection Master Plan 2024-2027, aimed at strengthening the country's data protection framework, enhancing public awareness, and aligning national standards with global best practices (PIPER, 2026b). At the same time, several data breach incidents reported in 2024, including the alleged sale of nearly 20 million Thai citizens' personal records, data breaches involving JIB customers, and alleged cyberattacks affecting Black Canyon and Central The 1 Card databases, demonstrate that data security risks remain a significant concern in Thailand (ASIA-PACIFIC, 2025). Nevertheless, public perceptions in Thailand may be more favorable regarding the effectiveness of regulatory protection because the Personal Data Protection Committee (PDPC) has already imposed its first administrative fine of THB 7 million on a data controller that failed to comply with PDPA requirements. The violations included inadequate data protection measures and non-compliance with statutory obligations under the PDPA. This enforcement action sent a clear message that violations of personal data protection laws can lead to tangible legal consequences for organizations (Somwaiya et al., 2024).

Visible regulatory enforcement has the potential to strengthen public trust because users may feel that their rights are actively protected by a competent and responsive authority. From the perspective of public perception, the existence of an active regulator is as important as the existence of the law itself. Individuals tend to evaluate the effectiveness of personal data protection not only through the legal provisions established by legislation but also through the concrete actions taken by authorities in responding to violations and holding organizations accountable (Mondaq, n.d.). Consequently, Thailand's recent enforcement efforts may contribute to a greater sense of confidence among users regarding the security and protection of their personal data within the digital environment.

Comparison of Personal Data Protection Regulations in Indonesia and Thailand

Indonesia and Thailand have both enacted comprehensive legislations governing personal data protection. Indonesia has adopted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI, 2022), while Thailand has implemented the Personal Data Protection Act B.E. 2562 (2019) (PDPA) ([Official Emblem of Royal Command] Personal Data Protection Act, B.E. 2562 (2019), 2019). Indonesia's PDP Law regulates a broad range of personal data protection issues, including fundamental principles, categories of personal data, the rights of data subjects, personal data processing activities, the obligations of data controllers and processors, cross-border data transfers, administrative sanctions, institutional arrangements, international cooperation, dispute resolution mechanisms, prohibitions on the misuse of personal data, and criminal provisions for specific violations (PIPER, 2026b). Similarly, Thailand's PDPA governs the collection, use, disclosure, and retention of personal data, as well as data subject rights, the responsibilities of data controllers and processors, cross-border data transfers, and the imposition of administrative, civil, and criminal penalties for non-compliance (Na, 2022).

From a comparative perspective, Thailand has advanced further into the active enforcement phase of personal data protection regulation. The PDPA became fully effective on June 1, 2022, and the Thai regulator has already demonstrated its enforcement authority through the imposition of administrative fines against organizations that failed to comply with statutory requirements. In contrast, Indonesia only entered the full compliance phase following the expiration of the PDP Law's transition period on October 17, 2024 (PIPER, 2026a). Although Indonesia now possesses a comprehensive legal framework for personal data protection, significant challenges remain in relation to institutional strengthening, the development of implementing regulations, and the consistency of enforcement mechanisms (Raidi, 2024). These differences suggest that while both countries share a similar commitment to strengthening personal data protection, they are at different stages of regulatory maturity. Thailand has moved further toward the consolidation of enforcement and institutional implementation, whereas Indonesia is still in the process of enhancing regulatory infrastructure and ensuring the effective operationalization of its personal data protection regime. As a result, the effectiveness of regulatory implementation may influence public perceptions of personal data security and shape levels of trust in digital services in different ways across the two countries.

Table 1. Comparison of Personal Data Protection Regulations in Indonesia and Thailand

Aspect	Indonesia	Thailand
Primary Regulation	**Law No. 27 of 2022 on Personal Data Protection (PDP Law)** (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI, 2022)	**Personal Data Protection Act B.E. 2562 (2019) (PDPA)** (Somwaiya et al., 2024)
Effective Date	Enacted on **17 October 2022**; transition period ended on **17 October 2024**	Enacted in **2019**; fully effective on **1 June 2022**
Regulatory Authority	A Personal Data Protection Authority is mandated by the PDP Law; supervisory functions during the transition period have remained under relevant ministries and government authorities	**Personal Data Protection Committee (PDPC)** (PIPER, 2026b)
Data Subject Rights	Right to access, rectify, erase data, withdraw consent, restrict processing, and obtain compensation	Right to access, rectify, erase data, object to processing, data portability, restrict processing, and withdraw consent
Sanctions	Administrative and criminal sanctions; administrative fines may be imposed in accordance with the PDP Law	Administrative, civil, and criminal sanctions; administrative fines may

Aspect	Indonesia	Thailand
		reach up to **THB 5 million** per violation
Implementation Stage	Full compliance phase following the transition period, accompanied by ongoing institutional strengthening	Active enforcement phase, including the imposition of the first administrative fine in 2024

Factors Shaping Public Perceptions

Several factors contribute to shaping public perceptions of personal data security in digital services. First, digital literacy influences individuals' ability to understand and assess personal data risks. Users with higher levels of digital literacy tend to be more aware of application permissions, suspicious links, password security, multi-factor authentication, and privacy policies. As a result, they are generally better equipped to identify potential threats and adopt appropriate security measures. Second, previous experiences with security incidents significantly affect levels of concern regarding personal data protection. Individuals who have experienced or been exposed to fraud conducted through telephone calls, phishing messages, fake notifications, or the misuse of personal information are likely to be more sensitive to security issues when using digital services. Such experiences often increase awareness of potential vulnerabilities and strengthen concerns about privacy risks. Third, the transparency of service providers plays a crucial role in building user trust (Somwaiya et al., 2024). Users are more likely to trust digital platforms that clearly explain the purposes of data collection and processing, provide users with meaningful privacy controls, and communicate data breach incidents promptly and transparently. Transparency helps reduce uncertainty and fosters confidence in the responsible handling of personal information. Fourth, legal enforcement influences public perceptions of fairness and accountability. Thailand has demonstrated that the imposition of administrative fines can serve as a visible signal of regulatory accountability and commitment to personal data protection. In contrast, Indonesia must ensure that the Personal Data Protection Law (PDP Law) functions not merely as a formal legal framework but is also implemented consistently and effectively against violations (Raidi, 2024). Effective enforcement can strengthen public confidence by demonstrating that organizations are held responsible for failures in data protection. Fifth, institutional reputation is an important determinant of public trust. Public and private organizations that repeatedly experience data breaches may suffer a decline in credibility and public confidence. Even when users continue to utilize these services due to a lack of viable alternatives, repeated security incidents can negatively affect perceptions of the organization's ability to protect personal information. Therefore, maintaining a strong reputation for data security is essential for sustaining public trust in digital services.

Overall, public perceptions of personal data security are shaped by the interaction of digital literacy, personal experience, organizational transparency, regulatory enforcement, and institutional reputation. These factors collectively influence how individuals assess risks, evaluate trustworthiness, and decide whether to engage with digital services

CONCLUSIONS AND RECOMMENDATIONS

Public perceptions of personal data security in the use of digital services in Indonesia and Thailand are shaped by a combination of technological factors, experiences with data breach incidents, digital literacy, service transparency, and the effectiveness of regulatory frameworks. Indonesia faces significant challenges due to its large internet user population and the recurring occurrence of data breaches across both public and private sectors. Thailand encounters similar risks; however, it has demonstrated notable progress in regulatory enforcement through the actions of the Personal Data Protection Committee (PDPC) and the imposition of administrative fines for violations of the Personal Data Protection Act (PDPA).

A comparison of the two countries highlights that the mere existence of personal data protection legislation is not sufficient to ensure public confidence. Public trust is more likely to increase when regulations are implemented consistently, supervisory authorities operate actively and effectively, digital service providers maintain transparency in their data processing practices, and citizens possess adequate levels of digital security literacy. Accordingly, personal data protection should be understood as a comprehensive ecosystem involving the state, private organizations, regulatory authorities, and users, all of whom share responsibility for safeguarding personal information and fostering trust in the digital environment**.**

Appendix 1. Examples of Recent Data Breach Cases in Indonesia

A. Ransomware Attack on the Temporary National Data Center 2 (PDNS 2) in Surabaya

In June 2024, the Temporary National Data Center 2 (PDNS 2) in Surabaya was reportedly targeted by a ransomware attack that disrupted the operations of hundreds of government agencies and public services, including immigration and educational services. This incident demonstrated that personal data security risks are not limited to commercial platforms but also affect critical government digital infrastructure. The case highlighted the vulnerability of public-sector information systems and underscored the importance of strengthening cybersecurity measures within government institutions (Katadata.co.id, 2024).

B. Alleged Data Breach Involving the National Civil Service Agency (BKN)

In 2024, data belonging to more than 4.7 million civil servants were reportedly leaked and offered for sale on hacker forums. The compromised information allegedly included employee identification numbers (Nomor Induk Pegawai or NIP) and telephone numbers. This incident heightened concerns regarding the security of government personnel databases and raised questions about the adequacy of existing safeguards for sensitive employee information.

C. Alleged Taxpayer Identification Number (NPWP) Data Breach

In 2024, more than 6.6 million taxpayer records were reportedly leaked and sold on hacker forums. This alleged breach posed significant risks because tax-related information can be exploited for financial fraud, identity theft, and other forms of cybercrime. The case drew considerable public attention due to the sensitivity of taxpayer data and its potential misuse by malicious actors.

D. Alleged Civil Registration (Dukcapil) Data Breach

In 2023, civil registration data managed by the Directorate General of Population and Civil Registration (Dukcapil) were reportedly leaked online through illegal forums. This incident is particularly significant because population data, including National Identification Numbers (NIKs), names, dates of birth, and residential addresses, constitute foundational information frequently used for identity verification across a wide range of digital services. The exposure of such data therefore presents substantial risks for identity theft, fraud, and unauthorized access to other services (TEMPO, 2025).

Appendix 2. Examples of Recent Cases in Thailand

A. The First Administrative Fine Under Thailand's PDPA

On 31 July 2024, the Expert Committee of Thailand's Personal Data Protection Committee (PDPC) imposed its first administrative fine under the Personal Data Protection Act (PDPA), amounting to THB 7 million, against a data controller company. The violations identified included the failure to appoint a Data Protection Officer (DPO), inadequate data security measures, and delayed notification of a personal data breach. This case marked a significant milestone in the enforcement of Thailand's personal data protection regime and demonstrated the authorities' commitment to holding organizations accountable for non-compliance with the PDPA (Somwaiya et al., 2024)

B. Alleged Sale of Nearly 20 Million Thai Citizens' Records

In January 2024, reports emerged concerning the alleged sale of nearly 20 million records belonging to Thai citizens, including names, national identification numbers, and telephone numbers. This incident highlighted the vulnerability of both public and private data to unauthorized access and exploitation. The case raised serious concerns regarding data security and reinforced the need for stronger safeguards to protect personal information from cybercriminal activities (ASIA-PACIFIC, 2025).

C. JIB Customer Data Breach

The JIB data breach case in Thailand illustrates how personal data incidents may also result from internal organizational factors. Reports indicated that the company acknowledged a customer data leak and subsequently initiated legal action against a former employee allegedly involved in the incident. The case underscores the importance of internal controls, employee accountability, and organizational governance in preventing unauthorized disclosure of personal information.

D. Alleged Cyberattacks on Black Canyon and Central The 1 Card

In 2024, reports in Thailand documented alleged cyberattacks involving Black Canyon Coffee and claims concerning the theft of data belonging to more than five million members of Central The 1 Card, one of the country's largest customer loyalty programs. These incidents demonstrate the substantial risks faced by the retail and customer loyalty sectors, which routinely collect and store large volumes of personal information, transaction records, and consumer identity data. The cases further highlight the growing cybersecurity challenges associated with customer relationship management systems and the protection of consumer data in Thailand's expanding digital economy.

Appendix 3. Summary of Current Personal Data Protection Legislation

A. Indonesia: Law Number 27 of 2022 on Personal Data Protection

Indonesia's Law Number 27 of 2022 on Personal Data Protection (PDP Law) regulates the protection of personal data as a means of safeguarding the constitutional rights of data subjects throughout the data processing lifecycle. The law covers a wide range of substantive provisions, including the fundamental principles of personal data protection, categories of personal data, data subject rights, obligations of data controllers and processors, cross-border data transfers, administrative sanctions, institutional arrangements, international cooperation, public participation, dispute resolution mechanisms, prohibitions on the misuse of personal data, and criminal penalties for specific violations (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI, 2022). The transition period for the implementation of the PDP Law ended on 17 October 2024, requiring all data controllers and data processors to align their data processing practices with the provisions and requirements established under the law (Raidi, 2024).

B. Thailand: Personal Data Protection Act B.E. 2562 (2019)

Thailand's Personal Data Protection Act B.E. 2562 (2019) (PDPA) serves as a comprehensive legal framework governing the collection, use, disclosure, and protection of personal data. Following several implementation delays and the establishment of the Personal Data Protection Committee (PDPC), the PDPA became fully effective on 1 June 2022. In addition to the primary legislation, Thailand has developed a number of subsidiary regulations and guidelines addressing specific aspects of personal data protection, including cross-border data transfers, the processing of criminal record data, and procedures relating to the erasure, destruction, or anonymization of personal data (Bunyamissara & Laopatarakasem, 2024). These supplementary regulations have contributed to strengthening the operational implementation of the PDPA and enhancing Thailand's overall personal data protection framework

REFERENCES

APJII, & Indonesia), (Asosiasi Penyelenggara Jasa Internet. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Https://Apjii.or.Id/Berita/d/Apjii-Jumlah-Pengguna-Internet-Indonesia-Tembus-221-Juta-Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

ASIA-PACIFIC. (2025). *5 Major Personal Data Breach Events In Thailand in 2024-A Summary Of The Risks And Impacts Organizations Face*. Saraburi Campus. https://www.apiu.edu/scamawareness/pdp-authority-thailand/

Company, B. &. (n.d.). *e-Conomy SEA 2024*. https://www.bain.com/insights/e-conomy-sea-2024/

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MISQ*, *13*(3), 319–340. https://misq.umn.edu/misq/article-abstract/13/3/319/191/Perceived-Usefulness-Perceived-Ease-of-Use-and?redirectedFrom=fulltext

Deradjat, A., Timur, M., Santoso, N. C., Kaur, D. P., & Khovey, E. (2025). Data Protection in Indonesia : Overview. *Reuters, Thomson*, *27*, 1–24.

Dienlin, T. (2023). Privacy Calculus : Theory , studies , and new perspectives. *The Routledge Handbook of Privacy and Social Media. Routledge*.

Katadata.co.id. (2024). *Tujuh Kasus Hacker dan Data Bocor 2024, Ada yang Sebabkan Layanan Publik Lumpuh Artikel ini telah tayang di Katadata.co.id dengan judul "Tujuh Kasus Hacker dan Data Bocor 2024, Ada yang Sebabkan Layanan Publik Lumpuh" , https://katadata.co.id/digital/tekn*. https://katadata.co.id/digital/teknologi/67738eeb9e7d5/tujuh-kasus-hacker-dan-data-bocor-2024-ada-yang-sebabkan-layanan-publik-lumpuh

Kemp, S. (2025a). *Digital 2025: Indonesia*. DataReportal. https://datareportal.com/reports/digital-2025-indonesia

Kemp, S. (2025b). *Digital 2025: Thailand*. DataReportal. https://datareportal.com/reports/digital-2025-thailand

Lalitkomon, N., Lamsam, R., & Somya, W. (2024). *Thailand Releases Master Plan for Personal Data Protection*. Tilleke & Gibbins. https://www.tilleke.com/insights/thailand-releases-master-plan-for-personal-data-protection/

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus Understanding situational online information disclosure as a privacy calculus. *Journal Of Computer Information Systems*, 1–29.

Masagee, S., & Boonnark, C. (2026). Data Protection Laws of the World. In *DLA PIPER*.

Mondaq. (n.d.). *Landmark Fine Imposed Under Thailand's Personal Data Protection Act*. https://www.mondaq.com/privacy-protection/1509140/landmark-fine-imposed-under-thailands-personal-data-protection-act

Na, T. R. (2022). *Thailand - Personal Data Protection (2562)*. https://regulations.ai/regulations/thailand-2019-5-personal-data-protection-act-pdpa

Official Emblem of Royal Command] Personal Data Protection Act, B.E. 2562 (2019), 1 (2019).

PIPER, D. (2026a). *Data protection laws in Indonesia*. https://www.dlapiperdataprotection.com/?t=law&c=ID

PIPER, D. (2026b). *Data protection laws in Thailand*. DLA PIPER. https://www.dlapiperdataprotection.com/?t=law&c=TH

Raidi. (2024). *Indonesia Personal Data Protection Law Takes Full Effect on October 17 2024*. Indonesial Sentinel. https://indonesiasentinel.com/indonesia-personal-data-protection-law-takes-full-effect-on-october-17-2024/

Recording, L. (2026). *Indonesia Data Privacy Laws: Complete UU PDP Compliance*

Guide (2026). https://www.recordinglaw.com/world-laws/world-data-privacy-laws/indonesia-data-privacy-laws/

Somwaiya, K., Aroonpakmongkol, W., & Ua-areetham, U. (2024). Thailand First Administrative Fine for Data Breach: An Analysis of Law and Practice. *LAWPLUSUPDATE*, *000*(September), 1–2.

Team, D. (2024). *Digital 2024: Thailand*. https://datareportal.com/reports/digital-2024-thailand

TEMPO. (2025). *Polemik Data Pribadi: 5 Kasus Kebocoran Data di Indonesia Selama 2023-2024*. https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).