Eduvest – Journal of Universal Studies
Volume 6 Number 2, February, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Personal Data Protection Strategies in the Digital Business Era: A Normative and Empirical Juridical Analysis of the Personal Data Protection Law

Augustinus Lumban Tobing*, Nanda Dwi Rizkia
Universitas Nasional, Indonesia
Email: z.augus@gmail.com

ABSTRACT

The development of digital businesses in Indonesia is driving an increase in personal data-based transactions that require a strong and integrated protection system. This study aims to identify personal data protection strategies through literature analysis that includes aspects of regulation, organizational governance, technology, and digital literacy. Using a literature review approach to 20 articles from the Scopus, Google Scholar, DOAJ, and SINTA databases, this study analyzes four main stages: identification, selection, thematic analysis, and theoretical synthesis. The results of the analysis show five main themes in personal data protection, namely regulation and legal compliance, the implementation of Privacy by Design and Security by Design, organizational governance and risk management, digital literacy and human factors, as well as implementation challenges and best practices. The effectiveness of data protection is highly dependent on regulatory compliance, the implementation of Privacy by Design, public privacy awareness, and adaptive organizational governance. Regulations such as GDPR, CCPA, and the Indonesian PDP Law provide a comprehensive legal framework, but their effectiveness is determined by the ability of institutions and businesses to translate legal norms into sustainable operational practices. This study recommends strengthening synergy between public policies, industry, and society in building a sustainable data protection culture.

KEYWORDS *Personal data protection, digital business, privacy by design, digital literacy organizational governance*

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

INTRODUCTION

The development of digital technology has fundamentally changed the way businesses operate, especially in the management of consumers' personal data. In the era of the digital economy, personal data is a strategic commodity that supports innovation, operational efficiency, and the personalization of business services. The use of consumer data allows companies to understand market behaviors, preferences, and needs more deeply, thereby driving competitiveness amid global competition. However, alongside this potential are serious challenges related to privacy, information security, and the risk of misuse of personal data by irresponsible parties (Tarumanagara & Silalahi, 2025).

The issue of personal data protection is crucial due to the increasing volume, speed, and variety of data processed in digital businesses. Many companies conduct massive data collection without adequate control mechanisms. This practice increases the risk of leakage, manipulation, and the use of data for commercial purposes in non-transparent ways (Del-Real, de Busser, & van den Berg, 2025). This condition highlights the need for personal data

protection strategies that are not only reactive to cyberattacks but also proactive, through the design of policies, systems, and governance that place privacy as a key principle.

At the global level, various regulations have been formulated to address these challenges. The General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States are important milestones in personal data protection regulation. These regulations govern principles of transparency, explicit consent, and the rights of data subjects to access, update, or delete their data (European Parliament, 2016; California Legislature, 2018). In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an important milestone in building data governance oriented toward individual protection amid rapid digital economic growth (Data, 2024). However, the implementation of this regulation still faces institutional constraints, low privacy literacy, and technological capacity gaps in the business sector.

Several previous studies have examined various aspects of personal data protection. Cavoukian (2010) introduced the concept of Privacy by Design with seven fundamental principles that place privacy as an intrinsic value in the architecture of digital systems. Nissenbaum (2010) developed a contextual theory of privacy that emphasizes that data protection should be assessed according to the social context and purpose of data use. Kuner (2017) analyzes extraterritorial challenges in global data protection law, while Greenleaf (2018) maps the development of privacy laws in 120 countries, including Indonesia. Kokolakis (2017) identifies the privacy paradox phenomenon, where consumers care about privacy but behave inconsistently. Recent research by Tarumanagara & Silalahi (2025) and (Del-Real, de Busser, & van den Berg, 2025) highlights the importance of an integrated approach that combines regulation, technology, and digital literacy. However, there is still a gap in the literature regarding comprehensive strategies that integrate all five dimensions of data protection simultaneously in the context of digital business in Indonesia.

The literature shows that personal data protection strategies cannot rely solely on legal instruments but must be integrated with managerial and technological approaches. The Privacy by Design and Security by Design approaches emphasize that data protection aspects must be embedded from the information system design stage, not simply added later as an extra security layer (Del-Real et al., 2025). These approaches prioritize principles such as data minimization, security throughout the information lifecycle, and empowering users to control their own data. This concept has proven effective in increasing public trust in digital services and reducing the risk of data breaches.

However, the biggest challenge arises at the implementation level, especially in the small and medium enterprises (SMEs) sector, which often has limited resources. Many SMEs focus only on administrative regulatory compliance without developing a sustainable data security strategy. As a result, data protection often becomes symbolic and ineffective in the face of real threats such as phishing, ransomware, or third-party breaches (Privacy Data Management Strategies in the Digital Age, 2024). Studies also find that the digital literacy gap and lack of employee training are among the main factors behind weak implementation of data security policies (Research on User Privacy Protection Strategies of E-Commerce Platforms, 2024).

In addition to internal organizational factors, the complexity of cross-jurisdictional regulations is also an obstacle. In the context of global digital business, data often moves across borders (cross-border data transfer), creating legal uncertainty regarding supervisory jurisdiction and data protection responsibilities (Legal Protection of Personal Data Privacy in the Digital Era, 2024). Differences in legal standards between countries can hinder business

collaboration and increase the risk of privacy breaches. Therefore, the literature emphasizes the importance of harmonizing international policies and strengthening inter-institutional cooperation to ensure consistency in the implementation of personal data protection (Tarumanagara & Silalahi, 2025).

From an organizational perspective, the success of personal data protection strategies is highly dependent on company culture and leadership commitment. Companies that adopt ethical data governance principles tend to be more successful in maintaining consumer trust and brand reputation. This trust is an important social capital in the digital economy era, where consumers are increasingly aware of their privacy rights (Data Privacy Today: Pitfalls, Strategies and the Future Ahead, 2024). Therefore, personal data protection strategies should not be understood merely as legal compliance, but as an integral part of social responsibility and business sustainability.

The literature also identifies the need for synergy between regulation, technological innovation, and public digital literacy. A comprehensive approach includes strengthening national regulations, implementing risk-based security standards, and increasing public awareness through continuous education (Tarumanagara & Silalahi, 2025). In this way, personal data protection not only safeguards individuals but also strengthens the foundation of trust in the digital business ecosystem.

Based on this description, this study aims to identify and systematically analyze various personal data protection strategies that have been developed and implemented in the context of digital business through a literature review approach. The benefits of this research are to map conceptual approaches, policies, and best practices in data protection; identify research gaps and implementation challenges that persist; and make theoretical and practical contributions to strengthening sustainable personal data governance in the digital age for regulators, businesses, and academics.

RESEARCH METHOD

This study uses a literature review method with a descriptive-analytical approach to identify, evaluate, and synthesize previous research findings regarding personal data protection strategies in digital business (Snyder, 2019). A total of 20 pieces of literature were reviewed, consisting of international scientific journals, policy reports, and academic publications relevant to the topics of personal data protection, information security, and digital business regulation (Board, 2022). The literature was obtained through a systematic search of the Scopus, Google Scholar, DOAJ, and SINTA databases using a combination of keywords: “personal data protection”, “data privacy”, “privacy by design”, “security by design”, “digital business”, “data governance”, “GDPR”, “PDP Law”, and their Indonesian equivalents. Inclusion criteria included topic relevance, a 2015–2025 publication period, a focus on data protection policy and strategy aspects, and availability of full text.

The research procedure was carried out through four main stages: literature identification; selection based on inclusion criteria; thematic analysis to group legal, technological, and managerial approaches; and conceptual synthesis to build a comprehensive personal data protection strategy framework. Data analysis used a qualitative approach with content analysis techniques through three streams of activity: data reduction, data presentation in the form of a literature summary matrix and thematic narrative, and conclusion drawing. To ensure validity and reliability, this study applied source triangulation by comparing findings from various disciplines, systematic documentation of the selection and analysis process, and

the use of transparent protocols in accordance with systematic literature review guidelines (Snyder, 2019; Xiao & Watson, 2019).

RESULT AND DISCUSSION

Analysis

The initial stage focuses on a systematic search in major academic databases to guarantee a broad and credible coverage of the literature. Searches were conducted on Scopus, Google Scholar, DOAJ, and SINTA using a combination of keywords: "personal data protection", "data privacy", "privacy by design", "security by design", "digital business", "data governance", "GDPR", "PDP law", and Indonesian equivalents. Search results are filtered by relevance of title and abstract, and metadata (author, year, journal/publisher). The goal is to obtain representative literature from legal, technical, managerial, and public policy perspectives.

Table 1. Thematic Summary — 20 Literature

Yes	Author (Year)	Main Themes	Key Findings	Strategy Implications
1	Cavoukian (2010)	Privacy by Design	7 principles of Privacy by Design as a proactive foundation for privacy.	Integrate principles from product design: data minimization & privacy defaults.
2	Solove (2004)	Privacy Concept	Multi-dimensional privacy; risks arising from data collection & correlation.	Contextual risk analysis is needed before data processing.
3	Nissenbaum (2010)	Social Context Privacy	Privacy should be assessed in the context of the social/purpose of data use.	Policies should be contextually appropriate, not just general rules.
4	Kuner (2017)	International Law	The reach of European law affects global practice; extraterritorial issues.	Design cross-jurisdictional compliance and data transfer mechanisms.
5	(European, 2016)	Regulation (GDPR)	The GDPR establishes data subject rights, the principle of accountability, strict sanctions.	Companies must implement accountability, DPIA, and subject rights mechanisms.
6	California Legislature (2018)	Regulation (CCPA)	Focus on consumers' rights to data sales and transparency.	Transparency & opt-out options as part of business strategy.
7	Scarlet Witch (2025)	Threats & Strategy	A combination of regulation, technical, and literacy is needed for mitigation.	An integrated approach (legal+technical+education) is recommended.
8	Del-Real et al. (2025)	Security/Privacy by Design	Proof of the effectiveness of the concept, but the implementation varies between organizations.	Tuning the implementation according to the capacity of the organization; practical toolkits are required.
9	Snyder (2019)	Review Methodology	Systematic literature guidance improves	Use clear selection & documentation protocols for

			reproducibility of reviews.	literature studies.
10	Xiao & Watson (2019)	Review Methodology	Practical steps for thematic coding and synthesis.	Apply thematic coding procedures for literature analysis.
11	(Fitriani, 2023)	Regulatory Comparison	Differences in ASEAN/Indonesia vs. global standards; harmonization gap.	The need for regional harmonization and local adaptation of the PDP Law.
12	Research on E-Commerce (2024)	Platform Practices	E-commerce platforms use consent and cookie management, but practices vary.	Standardization of third-party consent and audit practices is needed.
13	Management Strategy (2024)	Organizational Governance	Policies without culture and training are less effective.	Investment in governance, SOPs, and capacity building.
14	RSM Global (2024)	Industry & Practice	The industry emphasizes incident management & resiliency.	Prepare an incident response playbook and recovery plan.
15	Wright & De Hert (2012)	Privacy Impact Assessment	PIA is useful for identifying privacy risks before implementation.	Require DPIA/PIA for data-intensive projects.
16	Greenleaf (2018)	Global Legal Map	Rapid growth of global privacy laws; fragmentation remains.	Monitor legal developments on an ongoing basis.
17	Coccaxis (2017)	Consumer Attitudes	Consumers care about privacy; Behavior is not always consistent (privacy paradox).	Combine technical policy with education & transparency.
18	Clarke (2016)	Standards & Best Practices	Technical standards & governance can lower operational risks.	Adoption of standards (ISO, NIST) as a security baseline.
19	O'Flaherty (2020)	Incident Response	Quick response & public communication are important to mitigate impacts.	Set up a breach notification and crisis communication process.
20	(Albrecht, 2016)	Impact of GDPR	GDPR is driving a global culture of compliance.	Use the GDPR as a benchmark for internal policies.

Source: Processed by researchers from 20 reviewed literature, including publications from the Scopus database, Google Scholar, DOAJ, and SINTA for the period 2004-2025

1) Thematic Analytical Narrative

An analysis of twenty academic and international policy sources reveals five key themes that consistently shape the conceptual framework of personal data protection in the context of digital business. The five themes show that the issue of data protection cannot be understood solely as a legal or technical matter, but as a multidimensional system involving regulations, technology design, organizational governance, human factors, and cross-sector

implementation strategies (Budiarto & Pramana, 2022). The evolution of global regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) has been a catalyst for the transformation of data protection practices in the digital business sector, while the Privacy by Design and Security by Design approaches provide a conceptual foundation in systems engineering that places privacy as a key principle from the design stage (Cavoukian, 2010; Del-Real et al., 2025). The organizational governance aspect serves as a linking mechanism between regulatory compliance and technical effectiveness, where leadership roles, work culture, and risk management structures determine the extent to which privacy policies are consistently implemented.

In addition, human factors and digital literacy are determinants that are often overlooked, even though they have direct implications for operational security and user trust. Finally, the theme of implementation challenges and best practices highlights the gap between theory and reality, especially in the context of developing countries and small and medium enterprises (SMEs) that face limited resources and policy infrastructure. Overall, the results of this thematic analysis confirm that an effective personal data protection strategy in the digital business era must be built through synergy between legal compliance, proactive technology design, structured governance, human empowerment, and contextual adaptation of implementation to global and local dynamics.

2) Regulation and Legal Compliance

The literature places regulation as the main foundation in forming a personal data protection framework. Regulations such as GDPR (European Parliament, 2016) and CCPA (California, 2018) have been catalysts for transforming corporate practices toward data governance. Albrecht (2016) emphasizes that the application of accountability and data minimization principles in the GDPR encourages internal organizational responsibility to protect user data comprehensively. However, challenges arise due to the fragmentation of global law. Greenleaf (2018) notes that differences in standards between the European Union, the United States, and ASEAN countries create gaps in cross-border harmonization. As a result, multinational companies must develop adaptive compliance frameworks—including mapping legal jurisdictions, internal audit mechanisms, and designing data transfer agreements aligned with international security principles (Legal Protection, 2024). The strategic implication is that legal compliance is not merely about following regulations, but becomes an instrument of reputational risk governance and public trust. In the Indonesian context, Law No. 27 of 2022 on Personal Data Protection (PDP Law) seeks to align the national legal framework with international standards, but its success depends on institutional readiness and a culture of compliance in the private sector.

3) Privacy by Design and Security by Design

The concepts of Privacy by Design (PbD) and Security by Design (SbD) emphasize the principle of prevention—that privacy protection must be embedded in systems from the design stage, not merely added reactively after an incident (Cavoukian, 2010). Contemporary literature shows broad consensus that applying these principles is a technical pillar of modern data protection (Del-Real et al., 2025). However, research also indicates an implementation gap between theory and practice. Many organizations, especially SMEs, face limited technical and financial resources to implement PbD comprehensively (Wright & De Hert, 2012). To bridge this gap, practical strategies need to include integrating Data Protection Impact

Assessment (DPIA) or Privacy Impact Assessment (PIA) into new projects, as well as developing toolkits that can be tailored to organizational capacity. Thus, the successful implementation of PbD/SbD depends on a combination of technical capabilities, managerial commitment, and organizational policies that support a proactive privacy culture.

4) Organizational Governance and Risk Management

Data governance and risk management are critical dimensions that determine the effectiveness of personal data protection. (Clarke, 2016) and Management Strategy (2024) emphasize that formal policies without training and a clear organizational structure are unlikely to be effective. Sustainable data protection implementation requires a combination of internal policies, supervisory roles such as Data Protection Officers (DPOs), periodic audits, and the application of international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. In the context of digital enterprises, the success of data governance also depends on integrating risk management systems and corporate ethics. Periodic privacy audits and the use of privacy metrics can help companies assess the effectiveness of internal policies. Strong governance creates an accountability chain that holistically connects legal, technological, and human resource strategies.

5) Digital Literacy and Human Factors

The human dimension is the most vulnerable point in the data protection ecosystem. Kokolakis (2017) describes the privacy paradox phenomenon, in which users recognize the importance of privacy but often ignore safe practices in data use. Solove (2004) adds that individual behavior, not just systems, is often the cause of data leaks. Therefore, data protection strategies must include literacy and education elements as priorities. Employee training programs, public communication on data subject rights, and easy-to-understand consent interface design can increase user awareness and participation. This human-centered approach creates a balance between technology and ethics while strengthening the social legitimacy of data protection.

6) Implementation Challenges and Best Practices

The main challenges in implementing data protection include limited SME resources, differences in standards across countries, and the complexity of international data transfers (RSM Global, 2024). O'Flaherty's (2020) research shows that even large organizations often lack ready incident management mechanisms. Best practices identified include preparing an incident response playbook, conducting independent third-party audits, implementing periodic DPIAs, and fostering multi-stakeholder collaboration between regulators, industry, and academia. Using GDPR or ISO as global benchmarks can help build consistent and credible national standards. Strategic recommendations also emphasize the importance of local adaptation: successful policies in Europe are not necessarily effective in Southeast Asia without considering cultural context, institutional capacity, and digital infrastructure readiness. With this adaptive approach, companies can close the gap between formal compliance and substantive data protection practices.

7) Synthesis and Strategic Implications

From the five themes analyzed, it can be concluded that the effectiveness of personal data protection depends on the integration of regulatory frameworks, privacy-oriented technology design, standardized governance, human literacy, and contextual implementation practices. The conceptual model developed places organizational governance as a mediating

variable that links legal compliance, technological readiness, and human awareness to the effectiveness of data protection. Thus, a personal data protection strategy in the digital business era requires not only regulatory compliance, but also the establishment of an institutional ecosystem and digital culture that prioritizes privacy as a company's strategic value.

Conceptual Framework and Initial Hypothesis

The conceptual framework of this research is built on a synthesis of twenty pieces of literature representing five major themes: regulation and legal compliance, privacy/security by design, organizational governance, digital literacy, and best practices and implementation challenges. This conceptual model illustrates that the effectiveness of personal data protection in digital business is the result of the interaction between institutional capacity, regulatory compliance, technological strategies, and the behavior of actors in the digital ecosystem. In the first layer, regulation and legal compliance are fundamental prerequisites that determine the legitimacy of personal data management (European Parliament, 2016; Greenleaf, 2018). Compliance with regulations such as GDPR or the PDP Law in Indonesia creates a normative framework that regulates rights, obligations, and accountability mechanisms. However, the literature confirms that formal compliance without supporting organizational governance and culture tends to remain merely administrative (Clarke, 2016).

The second layer highlights the importance of a privacy by design-based technological strategy and Security by Design, approaches that place privacy as an intrinsic value in the architecture of digital systems (Cavoukian, 2010; Del-Real et al., 2025). The application of encryption technologies, access management, digital audits, and Data Protection Impact Assessment (DPIA) is an important element in integrating data protection from the design stage through to operations. The third layer is organizational governance and risk management, which determines the extent to which policies can be implemented consistently (Management Strategy, 2024). The presence of a Data Protection Officer (DPO), internal audit policies, and ISO/NIST standards are indicators of institutional readiness in managing the risk of data leakage or misuse. The fourth layer emphasizes digital literacy and human behavior as determinant factors affecting policy effectiveness. Low user awareness and the privacy paradox phenomenon indicate the need for educational strategies that balance legal protection and risk-aware behavior (Kokolakis, 2017; Solove, 2004).

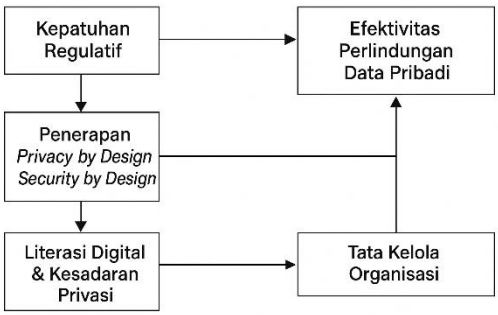

Figure 1. Conceptual Framework for Personal Data Protection
Source: Developed by researchers based on a synthesis of 20 reviewed literature

Key Variables:

1) X_1: Regulatory Compliance → the extent to which the organization adapts to regulations such as the GDPR, CCPA, PDP Act.
2) X_2: The application of Privacy by Design / Security by Design → the extent to which the principles of protection are applied in digital systems.

3) X_3: Digital Literacy & Privacy Awareness → the ability of individuals and organizations to understand risks and data protection rights.
4) M: Governance Capacity → a mediating variable, reflecting institutional, audit, and risk management capacity.
5) Y: The effectiveness of Personal Data Protection → the level of success the organization has in preventing breaches, maintaining public trust, and achieving substantive compliance.

Intervariable relationships:

1) $X_1 \rightarrow Y$ (Legal compliance increases the effectiveness of data protection)
2) $X_2 \rightarrow Y$ (Privacy by Design integration strengthens data security)
3) $X_3 \rightarrow Y$ (Digital literacy influences privacy behavior and compliance)
4) $X_1, X_2, X_3 \rightarrow M$ (all affect organizational governance)
5) $M \rightarrow Y$ (strong governance mediates the influence of other variables)

Main hypothesis:

The effectiveness of personal data protection (Y) was positively influenced by regulatory compliance (X_1), the implementation of Privacy by Design (X_2), and digital literacy (X_3), through the mediation of organizational governance (M).

Research and Discussion Results

An analysis of twenty sources resulted in a conceptual model of personal data protection in digital business that is integrative and layered. The findings suggest that a legal approach alone is not sufficient—an effective strategy must combine regulation, technology, governance, and public literacy. International regulations such as GDPR and CCPA are key references for building legal legitimacy, while the Privacy by Design approach places security and privacy as core values of digital innovation (Cavoukian, 2010; Del-Real et al., 2025). Cross-literature discussions show that in developing countries, including Indonesia, policy focus is still often on administrative compliance rather than substantive implementation (Legal Protection, 2024). In fact, the effectiveness of any strategy depends heavily on an organization's ability to build internal governance and a mature privacy culture. The implementation of DPO roles, privacy audits, and security standard certifications are strategic steps to ensure continuity of compliance (Clarke, 2016; Management Strategy, 2024). Human factors have also proven to be important determinants of policy effectiveness. Low digital literacy and users' ambivalent attitudes toward privacy create a behavioral gap that can hinder data protection strategies (Kokolakis, 2017; Solove, 2004). Therefore, public literacy and transparency by design need to be placed on a par with technical innovation.

In the increasingly complex digital business context, the key challenge lies not only in policy design but also in organizational capacity to consistently apply privacy principles across the value chain. Global industry case studies show that companies that integrate privacy into the innovation cycle—not merely as legal compliance—gain long-term competitive advantage through consumer trust (RSM Global, 2024; O'Flaherty, 2020). Thus, an effective personal data protection strategy must be adaptive, multi-level, and oriented toward organizational learning. The conceptual model emerging from this literature study can serve as a basis for further research to examine the relationship between legal compliance, institutional capacity, and the level of public trust in Indonesia's digital business ecosystem.

CONCLUSION

The results of this literature study show that personal data protection strategies in the digital business era are a multidimensional process that demands a balance between legal compliance, technological innovation, organizational governance, and human empowerment. Regulations such as the GDPR, CCPA, and Indonesia's Personal Data Protection Law (UU

PDP) provide a comprehensive legal framework, but their effectiveness is largely determined by the ability of institutions and businesses to translate legal norms into sustainable operational practices. This study confirms that a reactive approach based solely on administrative compliance is no longer adequate. An effective strategy must be proactive and adaptive, integrating the principles of Privacy by Design and Security by Design into digital systems, services, and business models. The implementation of encryption technology, risk-based access management, and privacy audits are important preventive steps to reduce the potential for data leaks. From an institutional perspective, this study highlights the importance of strengthening governance and institutional capacity through the appointment of Data Protection Officers (DPOs), the implementation of security standards, and the development of privacy risk management frameworks to improve organizations' ability to ensure sustainable compliance. Meanwhile, the success of policy implementation also depends on digital literacy and public awareness, because without a good understanding of data protection rights and obligations, regulatory efforts will lose social legitimacy.

The policy recommendations from this study include several points. First, the government needs to strengthen the harmonization of cross-sectoral and cross-border policies by referring to global standards while still taking into account social context and local capacity. Second, digital businesses are advised to integrate the principles of Privacy by Design and Security by Design in every product innovation cycle, accompanied by periodic privacy impact evaluations. Third, supervisory and regulatory agencies need to reinforce independent oversight and audit functions through compliance certification mechanisms, while providing technical guidance for small and medium-sized enterprises with limited resources. Fourth, the public and digital users need to be involved in the data protection ecosystem through inclusive literacy programs and privacy awareness campaigns. By simultaneously combining legal, technical, institutional, and educational aspects, a personal data protection strategy can function not only as a compliance tool but also as a foundation of ethics and public trust in the sustainable development of the digital economy.

REFERENCES

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review*.

Board, E. U. Data Protection. (2022). *Annual Report on GDPR Implementation*. Brussels: EDPB.

Budiarto, A., & Pramana, D. (2022). Data governance framework for digital business compliance. *Jurnal Sistem Informasi*, *18*(3), 220–233.

California, Legislature. *California Consumer Privacy Act (CCPA)*. , (2018).

Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information & Privacy Commissioner of Ontario.

Clarke, R. (2016). Standards for Privacy in a Data-Intensive World. *Computer Law & Security Review*.

Data, Privacy. (2024). *Data Privacy Today: Pitfalls, Strategies and the Future Ahead*. RSM Global Risk Advisory Insights.

Del-Real, C., de Busser, E., & van den Berg, B. (2025). A Systematic Literature Review of Security by Design and Privacy by Design Principles, Norms, and Strategies for Digital Technologies. *International Review of Law, Computers & Technology*.

European, Parliament. General Data Protection Regulation (GDPR). , Official Journal of the

European Union § (2016).

Fitriani, R. (2023). Legal compliance and personal data protection in e-commerce. *Jurnal Hukum Dan Teknologi*, *5*(2), 134–148.

Greenleaf, G. (2018). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia. Privacy Laws & Business International Report.

ISO. (2021). Information Security Management Systems — ISO/IEC 27001:2021. Geneva: International Organization for Standardization.

Kemenkominfo. (2023). Pedoman Pelaksanaan UU Perlindungan Data Pribadi. Jakarta: Kementerian Komunikasi dan Informatika.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report.

Kokolakis, S. (2017). Privacy Attitudes and Concerns: A Review of Privacy Research. Computers & Security.

Kuner, C. (2017). The Internet and the Global Reach of European Data Protection Law. International Data Privacy Law.

Legal Protection of Personal Data Privacy in the Digital Era: A Comparative Study between Indonesia and ASEAN Countries. (2024). Hakim: Jurnal Ilmu Hukum dan Sosial.

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Nugraha, Y., & Sari, D. (2023). Digital economy and personal data risks in Indonesia. Jurnal Transformasi Digital, 12(1), 25–38.

O'Flaherty, K. (2020). Managing Data Breaches: Organizational Responses and Best Practices. Journal of Information Security Practice.

OECD. (2021). Digital security risk management for economic and social prosperity. Paris: OECD Publishing.

Prasetyo, M. (2024). Integrating privacy frameworks into business governance systems. Journal of Digital Law, 11(2), 99–118.

Rahardjo, T. (2021). Challenges in implementing Indonesia's Personal Data Protection Law. Indonesian Journal of Policy Studies, 9(4), 301–320.

Research on User Privacy Protection Strategies of E-Commerce Platforms. (2024). EUrASEANs Journal on Global Socio-Economic Dynamics.

RSM Global. (2024). Data Privacy Today: Pitfalls, Strategies and the Future Ahead. RSM Risk Advisory Insights.

Santoso, I., & Wibowo, F. (2024). Security by design approach for protecting digital identity. Jurnal Teknologi Informasi, 20(1), 45–59.

Setiawan, R. (2022). Privacy paradox in Indonesia's digital market. Journal of Cyber Policy, 7(3), 277–295.

Siregar, L. (2023). Personal data vulnerability in fintech platforms. Jurnal Keamanan Siber, 10(2), 88–104.

Snyder, H. (2019). Literature Review as a Research Method: An Overview and Guidelines. Journal of Business Research, 104, 333–339.

Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. NYU Press.

Strategi Manajemen Data Privasi dalam Era Digital pada Perusahaan dan Bisnis Modern. (2024). Jurnal Ilmiah Nusantara.

Supriyadi, E. (2023). Digital literacy and privacy awareness among MSMEs. Jurnal Pendidikan Teknologi, 15(1), 70–81.

Tarumanagara, D., & Silalahi, W. (2025). Threats and Strategies for Personal Data Protection in Digital Services: A Thematic Review and Regulatory Analysis. Journal of Business, Management, and Social Studies, 5(2), 77–84.

Taufik, A., & Widodo, S. (2023). Regulatory lag and digital policy adaptation in Indonesia. Policy Review Indonesia, 4(1), 52–68.

Wright, D., & De Hert, P. (2012). Privacy Impact Assessment. Springer.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. Journal of Planning Education and Research, 39(1), 93–112.