ISSN 2988-2125

Personal Data Protection in Digital Business Activities: Corporate Compliance Challenges and Global Consumer Trust Opportunities

Radea Respati Paramudhita
Faculty of Economics and Business, Widyatama University, Indonesia
Email: radea.respati@widyatama.ac.id

The rapid transformation of the digital economy has positioned personal data as both a strategic asset and a significant legal liability. This study aims to analyze the challenges faced by Indonesian corporations in implementing Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and explore how compliance can be transformed into opportunities to gain global consumer trust. Using normative legal research methods with a statutory and comparative approach, this study identifies key corporate barriers, ranging from the innovation versus security paradox, the burden of administrative sanctions of up to 2% of annual revenue, the need for expert Data Protection Officers (DPOs), to the complexity of cross-border data transfers. The research findings indicate that while compliance requires significant investment, the implementation of Privacy by Design principles and international standards (ISO/IEC 27001) can create strong reputational differentiation. Transparency in data processing has been shown to increase customer loyalty and mitigate long-term legal risks. The study concludes that aligning internal corporate policies with the mandates of the PDP Law is key to mitigating cyber risks while strengthening companies' competitive positions in the global digital supply chain.
Keywords: Personal Data Protection, PDP Law, Corporate Compliance, Consumer Trust, Digital Business, Risk Mitigation.

Corresponding Author:
Radea Respati Paramudhita
Faculty of Economics and Business, Widyatama University, Indonesia
radea.respati@widyatama.ac.id

1. Introduction

The era of digital transformation has fundamentally changed the global business landscape, with personal data now a strategic asset driving the economy. In Indonesia, massive digital business activity requires a strong legal framework to ensure the security of public information (Delia et al., 2026). The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) marks a new chapter for the national digital ecosystem, requiring businesses to align their operations with strict data protection principles (Suyahman, 2025).

In the corporate context, consumer personal data is often the primary fuel for the development of marketing algorithms and data-driven decision-making (Rismayadi et al., 2025). However, before the enactment of the PDP Law, many companies operated without uniform security standards, often leading to overlapping authorities and legal uncertainty. Now, corporations acting as Personal Data Controllers have full legal responsibility to ensure that all data processing has a valid legal basis (Syifa & Adam, 2024).

Compliance challenges are a central issue because the PDP Law sets high standards for corporations in data management. Companies are required to have a Data Protection Officer (DPO), conduct data protection impact assessments, and guarantee the rights of data subjects (Ajiraga, 2026). This transition process is not easy, as it requires IT system restructuring and significant operational cost adjustments to avoid falling into regulatory violations that could result in severe sanctions (Khair & Wiraguna, 2025).

ISSN 2988-2125

The sanctions provisions in Indonesia's Data Protection Law cannot be underestimated. Corporations that fail to comply with these obligations can be subject to administrative sanctions in the form of fines of up to 2% of annual revenue, and even criminal sanctions for corporate managers (Tanudjaja, 2024). These legal risks create pressure for businesses to go beyond formalities and truly integrate data security into the core of their business models to avoid financial and reputational losses (Situmeang et al., 2025).

However, despite these stringent regulations, the Data Protection Law actually opens up significant opportunities for corporations to build global consumer trust (Hidayat, 2025). With legal standards now on par with international regulations like the GDPR, Indonesian companies have greater bargaining power in cross-border collaboration. Compliance with the Data Protection and Privacy Law demonstrates a corporation's credibility and ability to manage data with globally recognized security standards (Simanjuntak, 2024).

Despite these real opportunities, the implementation of the Data Protection and Privacy Law still faces challenges in the field, particularly related to human resource readiness and technical understanding of the data security standards stipulated by the law (Rinjani & Firmansyah, 2025). Many companies are still in the adaptation phase and require more comprehensive technical guidance. Therefore, synchronizing internal company policies with the mandates of the Data Protection and Privacy Law is crucial for business innovation to continue without violating citizens' privacy rights (Afifah, 2024).

Against this backdrop, this study will focus on analyzing the challenges facing corporate compliance in implementing the Data Protection and Privacy Law and how such compliance can be transformed into opportunities to gain trust in the global market. It is hoped that the results of this study will provide strategic recommendations for businesses in Indonesia to align profitability with personal data protection responsibilities.

2. Literature Review

Personal Data Protection

Personal Data Protection (PDP) is an effort to protect individual data in every processing process to guarantee citizens' constitutional rights, as comprehensively regulated in Law Number 27 of 2022. This regulation covers various important aspects, from the definition and scope of personal data to the rights and obligations of the parties involved (Niffari, 2020). Personal data is divided into two categories: general data such as name and gender, and specific data such as health, biometric, and financial information. Furthermore, individuals, as data subjects, have the right to access, correct, delete, and restrict the processing of their personal data (Sulistianingsih et al., 2023).

Conversely, data controllers are obligated to ensure that data processing is conducted on a legal basis, maintain data security, and report any data breaches (Priliasari, 2023). Violations of these provisions can have serious consequences, including criminal sanctions, fines, and even corporate dissolution. Therefore, it is crucial for the public to protect their personal data through measures such as using a VPN, creating strong and unique passwords, and activating two-factor authentication (2FA). In addition to the PDP Law, data protection is also supported by the Electronic Information and Transactions Law (UU ITE) Number 11 of 2008, which regulates the misuse of electronic data. With the full implementation of the PDP Law in 2024, all business actors are required to comply to avoid legal consequences.

Digital Business

According to Priliasari (2023), digital business can be defined as the dramatic adjustment of conventional businesses that is inevitable in the digital business ecosystem, such as the Internet of Things (IoT), cloud-

 ISSN 2988-2125

based services, smartphones, and others. The existence of digital business means that all organizations must inevitably reimagine how they will grow, survive, compete, and thrive in the digital era. Organizations that cannot adapt will be naturally selected and collapse. According to Forbes magazine (Suma et al., 2023), digital business is the result of the creation of a new business design by blurring the digital and physical worlds. Digital business is driving unprecedented changes in people, businesses, and events. The fundamental difference between digital business and e-business lies in the presence of people and the intelligent integration of connected things between people and the business itself.

According to Chaffey & Ellis-Chadwick (2019), in their book "Digital Business and Ecommerce Management: Strategy, Implementation, and Practice," digital business is a broader term, referring to how technology can benefit all internal business processes and interactions with third parties. This includes buy-side and sell-side e-commerce and the internal value chain. Based on the definitions above, it can be concluded that digital business is a business that is created and adapted from a new business design that is closely related to the digital ecosystem (current technology), integrated and digitally connected from the seller side, through the transaction process, to the buyer. The existence of digital business provides opportunities for all companies to achieve and surpass things that were previously impossible for conventional businesses.

3. Method

This research is a normative-legal research that focuses on the analysis of written legal norms, both in the form of laws and other supporting literature (Soekanto, 2007). The primary approach used is a statute approach to deeply analyze Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and its implementing regulations. Furthermore, a comparative approach is used to examine the extent to which Indonesian compliance standards align with international regulations such as the GDPR, and a conceptual approach is used to understand the correlation between data protection and consumer loyalty.

The data used in this study is sourced entirely from secondary sources, grouped into three main legal sources. Primary legal sources consist of legally binding laws and regulations in Indonesia. Secondary legal sources include scientific journals, textbooks, and research reports that provide critical explanations of corporate challenges in digital business. Meanwhile, tertiary legal sources, in the form of legal dictionaries and encyclopedias, are used to clarify technical terminology. All data was collected through library research, inventorying and classifying documents relevant to data privacy and market trust issues.

The final stage was qualitative data analysis, conducted using deductive reasoning. Researchers analyzed general legal facts regarding data protection regulations and then related them to specific issues, namely the operational challenges facing corporations in the digital age. This analysis aimed to produce comprehensive legal arguments regarding how compliance with the Data Protection Law can be a strategic tool for companies to gain global consumer trust. The results of the analysis were presented descriptively to provide a clear picture of the ideal direction of business policies and practices.

4. Result And Discussion

Corporate Compliance Challenges in Indonesia

1. The Compliance vs. Innovation Paradox

In Indonesia's competitive digital economy ecosystem, a phenomenon known as the regulatory compliance and business innovation paradox has emerged. Many companies, particularly in the startup and fintech sectors, tend to focus their financial and technical resources heavily on product feature development and market expansion to achieve rapid growth (growth hacking). As a result, investment allocation for

 ISSN 2988-2125

strengthening personal data protection infrastructure is often sidelined or considered a secondary priority, as it is perceived as not providing immediate financial benefits compared to innovative features that appeal to users.

This tendency to prioritize innovation speed over security creates cybersecurity gaps that are highly vulnerable to exploitation. The lack of implementation of Privacy by Design principles in the digital product development process means that security systems are often patchwork or reactive after an incident occurs. In Indonesia, where cyberattacks and data breaches are increasing in frequency, neglecting strong encryption standards and strict data access management during the innovation phase can have fatal consequences, not only for individual privacy but also for the continuity of corporate operations.

This imbalance ultimately places corporations at significant legal and reputational risk, especially with the strict administrative sanctions in the Personal Data Protection Law (PDP Law). Corporations must begin to recognize that investment in data protection systems is not a barrier to innovation, but rather an integral component of sustainable innovation. Without robust security, even the most sophisticated innovation will lose its market value when consumer trust is eroded by companies' failure to protect the personal data entrusted to them.

2. Legal Transition & Severe Sanctions

The transition period leading to the full implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) places corporations under unprecedented legal pressure. This regulation introduces a very severe sanction structure, with administrative fines reaching up to 2% of a corporation's annual revenue for those who violate basic provisions. The large fines, calculated on total revenue, rather than simply net profit, force directors and upper management to view data protection compliance as a systemic financial risk that could threaten the stability of the company's cash flow if ignored.

In addition to financial threats, the PDP Law also contains very harsh criminal provisions for businesses that intentionally misuse data. Imprisonment or fines of up to IDR 60 billion are imposed for serious violations such as falsifying personal data for personal gain or for others. This demonstrates that the state no longer views data breaches as merely technical issues, but rather as serious violations with criminal consequences for personnel within the corporation. These provisions aim to create a deterrent effect and emphasize that the responsibility for maintaining data integrity rests squarely with data managers.

Furthermore, the PDP Law tightens the doctrine of corporate legal liability through the concept of absolute liability for any data breaches, including those occurring through third parties or vendors (third-party risk). In an interconnected digital ecosystem, companies often partner with cloud service providers or other third parties to process consumer data. However, the PDP Law emphasizes that primary control and responsibility remain with the parent company as the data controller. This requires corporations to conduct rigorous audits and highly specific contracts across their entire supply chain, as third-party negligence now constitutes direct legal liability that can implicate the corporation as a whole.

3. The Need for a Data Protection Officer (DPO)

The mandatory appointment of a Data Protection Officer (DPO) is one of the most crucial mandates under the Data Protection Law for companies processing large-scale, regular, and systematic data. The presence of a DPO is not merely an administrative formality to meet regulatory requirements, but rather a strategic function that bridges business interests and legal compliance. However, the definition of "large-scale" and "systematic" processing in business practices often remains ambiguous, forcing corporations to conduct independent evaluations of their entire operational model to determine whether they are required to have this function permanently.

 ISSN 2988-2125

The primary challenge facing corporations in Indonesia is the scarcity of human resources with hybrid competencies across law, information technology, and risk management. A DPO is not only required to understand the articles in the Data Protection Law but also to be able to translate these legal norms into complex technical cybersecurity policies. A company's inability to recruit or train competent experts can result in ineffective data protection policies in the field, ultimately increasing the risk of accidental data breaches due to technical ignorance.

In addition to competency, the placement of the DPO position within the organizational structure also presents its own challenges. To work effectively, a DPO must have independence and a direct reporting line to the company's top management to avoid conflicts of interest with the marketing or product development departments. The need for this independent position with the authority to provide security recommendations requires a significant shift in organizational culture, where data compliance is no longer seen as a constraint on other divisions, but rather as an internal oversight function that ensures long-term business sustainability.

4. Cross-Border Data Transfer

In an interconnected global business ecosystem, cross-border data flow has become an unavoidable routine activity, especially for multinational corporations or local companies using cloud-based services. Indonesia's Data Protection Law stipulates strict regulations that transfer of personal data outside of Indonesian jurisdiction can only occur if the recipient country has a level of data protection equivalent to or higher than national standards. This forces corporations to remap the server locations and jurisdictions of their third-party service providers to ensure there are no data sovereignty violations that could lead to administrative sanctions.

Technical challenges arise when corporations must align compliance with the Data Protection Law with other international standards, such as the European Union's General Data Protection Regulation (GDPR). Differences in regulatory details between jurisdictions often create operational ambiguity, particularly regarding explicit consent mechanisms for data subjects and security protocols while data is in transit. For corporations relying on public cloud infrastructure, the responsibility to ensure that service providers comply with standard contractual clauses is crucial, as ignorance of the physical location of data storage abroad cannot be used as an excuse to absolve themselves of legal responsibility.

Non-compliance with cross-border data transfer governance risks not only financial penalties but also the threat of termination of data processing activities by supervisory authorities. Therefore, corporations need to adopt a jurisdiction-agnostic data protection strategy by consistently applying the highest security standards across all their branches and digital infrastructure. By simultaneously ensuring compliance with international and national standards, corporations not only mitigate legal risks but also facilitate smooth business operations in a global marketplace that increasingly demands transparency in the exchange of information.

Global Consumer Trust Opportunities

1. Reputation & Trust Differentiation

Amidst the rise in data breaches affecting various digital platforms globally, proactive compliance with the PDP Law is no longer simply fulfilling a legal obligation, but rather a powerful reputation differentiation strategy. While other companies only implement minimal security standards, corporations that adopt strict and transparent data protection principles will stand out in the market. A reputation as a "safe and trustworthy" entity has become a valuable intangible asset, distinguishing a brand from its competitors in an increasingly crowded and risky digital ecosystem.

Customer loyalty in the modern era relies heavily on the sense of security provided by service providers. Global consumers are increasingly aware of the high value of their personal data, making them more selective in choosing platforms. By communicating easy-to-understand privacy policies and giving users full control over their data, corporations can build emotional relationships based on trust. This will create a deeper circle of loyalty, where consumers not only use the service repeatedly but also become advocates for the platform's security within their social circles.

Furthermore, the trust built through data protection compliance serves as a shield against future reputational crises. Companies that have built a strong foundation of trust tend to be more resilient when faced with technical challenges. For the global market, compliance with standards equivalent to international regulations demonstrates mature corporate governance. This directly increases a company's bargaining power in attracting international investors, who are increasingly prioritizing data privacy and ethics as key indicators in their ESG (Environmental, Social, and Governance) assessments.

2. International Security Standards

Adopting international security standards, such as ISO/IEC 27001 for information security management systems, has become a universal language in the digital business world to ensure data integrity. For corporations, integrating these standards into the PDP Law framework is not simply a technical safeguard but a statement of professionalism to global business partners. By possessing internationally recognized certification, companies assure that their internal processes have undergone rigorous audits, thereby minimizing doubts from foreign parties when exchanging sensitive data within strategic collaborations.

In addition to certification standards, implementing Privacy by Design (PbD) principles is key to strengthening a company's position in the global digital supply chain. This principle requires that data protection be integrated from the earliest stages of product or system development, not as an add-on feature after the system is complete. In a global market that places a high premium on privacy, companies that can demonstrate that their technology is built on a strong privacy foundation will be more likely to be accepted as primary vendors in international projects with stringent compliance requirements.

Strategically, this alignment of international security standards enhances companies' competitiveness in the data-driven economy. Companies that adhere to global standards have a stronger bargaining position when negotiating with investors and partners from restrictive jurisdictions such as the European Union or the United States. This demonstrates the corporation's strong governance maturity, which ultimately facilitates market expansion and ensures the company is not isolated from the international digital trade network due to its inability to meet global privacy standards.

3. Transparency in Data Processing

The principle of transparency in data processing is a key foundation for ethical relationships between corporations and consumers in the information economy. As mandated by Law Number 27 of 2022, corporations are required to provide clear, honest, and easily accessible information regarding the purpose of collecting and managing customer personal data. This transparency is not merely an administrative obligation, but rather a mechanism for granting data subjects full control over their own information, from the right to access to withdrawing previously granted processing consent.

Providing this control directly contributes to increased public trust in a company's digital systems. When consumers feel empowered to monitor how their data is used, trust in the organization grows organically, automatically reducing the potential for future complaints or legal disputes. In the long term, this openness mitigates the risk of user resistance and builds the corporation's image as a responsible entity, which is crucial for maintaining a competitive advantage in the global marketplace.

Beyond trust, transparency also serves as an additional line of defense against the threat of cyberattacks. By involving users in monitoring their data—for example, through account access notifications or data activity reports—companies indirectly create a participatory security ecosystem that can detect anomalies more quickly. Active user involvement and clear processing documentation enable organizations to maintain high accountability, so that in the event of an illegal penetration attempt, the corporation has evidence of good governance that can mitigate legal sanctions while maintaining operational stability.

4. Long-Term Risk Mitigation

Implementing full compliance with the Data Protection and Data Protection Law serves as a crucial long-term risk management strategy for corporate sustainability. By consistently implementing the law's mandate, companies can mitigate destructive legal risks, such as the revocation of business licenses or the temporary suspension of operational activities by supervisory authorities. Early prevention through accountable data governance ensures that companies are not only prepared for regulatory audits but also protected from civil lawsuits often filed by consumers or community groups due to data protection failures.

From a financial stability perspective, risk mitigation through comprehensive compliance prevents companies from the threat of administrative fines that can drain corporate liquidity. The costs of establishing a security system and appointing a Data Protection Officer (DPO) are far lower than the total financial losses resulting from sanctions of up to 2% of annual revenue, system recovery costs, and compensation to data subjects affected by the breach. This compliance is essentially a preventative investment that safeguards a company's balance sheet from the unexpected costs of a data crisis.

Finally, the most significant risk mitigation is protecting long-term reputational value, which is often irreversible. A massive data breach has the potential to destroy brand equity instantly and trigger an exodus of customers to competitors. By complying with the standards of the Data Protection Law, corporations demonstrate a strong ethical commitment, which creates reputational resilience. Companies with a strong track record of compliance will more easily regain public trust in the event of future technical challenges, thereby maintaining business integrity in the eyes of both national and global markets.

5. Conclusion

The implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) marks a new era for the digital business world in Indonesia, where data compliance is no longer merely an option but a legal and strategic imperative. The main challenge facing corporations lies in balancing rapid technological innovation with investment in robust security systems. The risk of heavy administrative fines and managerial obligations such as the appointment of a Data Protection Officer (DPO) require a fundamental transformation in internal corporate governance to avoid legal liabilities that could threaten business continuity. Furthermore, this study shows that compliance with data protection standards is a powerful instrument for building consumer trust in the global market. By adopting Privacy by Design principles and international security standards, corporations not only mitigate the risk of data breaches but also create positive reputational differentiation. Transparency in data processing is key to increasing customer loyalty, as modern consumers tend to provide their data to organizations that can credibly guarantee the security and control of their personal information. In conclusion, the synergy between regulatory compliance and business strategy is key to success in the data-driven digital economy. Corporations that can transform compliance burdens into competitive advantages will have greater long-term resilience against reputational crises and cyberattacks. By viewing the PDP Law as an operational gold standard, Indonesian companies have a significant opportunity to compete with global players in the

international digital supply chain, while ensuring that business innovation remains aligned with the protection of human rights to data privacy.

6. References

Afifah, N. (2024). Tanggung jawab hukum platform e-commerce terhadap keamanan data pribadi pengguna: Analisis berdasarkan UU PDP 2022. *Jurnal Legalitas*, *2*(1), 29-38.

Ajiraga, H. (2026). Peran dan Tanggungjawab Data Protection Officer dalam Pelaksanaan Perlindungan Data Pribadi. *Asas Wa Tandhim: Jurnal Hukum, Pendidikan Dan Sosial Keagamaan*, *5*(1), 261-290.

Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital marketing*. Pearson uk.

Delia, D., Tan, D., & Agustini, S. (2026). Regulasi Hukum Ekonomi Digital: Implikasi Undang-Undang Nomor 1 Tahun 2024 Terhadap E-Commerce dan Start-Up di Indonesia. *Unes Journal of Swara Justisia*, *10*(1), 41-54.

Hidayat, R. S. (2025). Transformasi hukum bisnis di ekosistem digital: Studi atas perlindungan data pribadi konsumen. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *3*(4), 46-52.

Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment (DPIA) sebagai instrumen kunci menjamin kepatuhan UU PDP 2022 di Indonesia. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, *2*(2), 246-254.

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 Yuridis*, *7*(1), 105-119.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *12*(2).

Rachmat, Z., Rukmana, A. Y., Nurendah, Y., Ashari, D. R. W., Donoriyanto, D. S., Bait, J. F., ... & Kasmita, M. (2023). Strategi Bisnis Digital Dan Implementasinya.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70-83.

Rismayadi, D. A., SI, S., Kom, M., Faira, F., Adjani, K., Kom, S., & Kom, M. (2025). *Algoritma dan Data Driven Decision Making dalam Bisnis*. Alungcipta.

Simanjuntak, P. H. (2024). Perlindungan hukum terhadap data pribadi pada era digital di Indonesia: Studi undang-undang perlindungan data pribadi dan general data protection regulation (gdpr). *Esensi Hukum*, *6*(2), 105-124.

Situmeang, A., Weley, N. C., & Disemadi, H. S. (2025). Kepastian Pertanggungjawaban Hukum Pidana Korporasi atas Penyalahgunaan Data Pribadi di Indonesia. *Proceedings Series on Social Sciences & Humanities*, *23*, 8-15.

Soekanto, S. (2007). Penelitian hukum normatif: Suatu tinjauan singkat.

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, *52*(1), 97-106.

Suma, D., & Siregar, B. A. (2023). *Bisnis digital*. CV. Azka Pustaka.

Suyahman, S. (2025). Manajemen dan Kebijakan Keamanan Informasi. *PT Solusi Administrasi Hukum*.

Syifa, A. R., & Adam, R. C. (2024). Perlindungan Data Pribadi Nasabah Peminjam dalam Layanan Pinjaman Meminjam Berbasis Teknologi Informasi Berdasarkan Hukum Perlindungan Data Pribadi. *UNES Law Review*, *7*(2), 683-694.

Tanudjaja, T. (2024). Tanggung Jawab Pidana pada Korporasi dalam Tindak Pidana Perpajakan. *Jurnal Hukum Indonesia*, *3*(3), 96-106.