Journal of Law Perspectives Review
Volume 2, Number 2, 2026, Pp: 87-96
https://doi.org/10.64670/jlpr.v2i2.76

Catalyst Journal

Journal of Law Perspectives Review

Journal Homepage: journal.catalystindo.org

Protection of Customer Personal Data in the Standard Clauses of the Privacy Policy of the Seabank Digital Bank Application

Nimas Yuski Nur Lailli[1], Josef Purwadi[2], Yokhebed Arumdika[3]*

[1,2,3]University of Slamet Riyadi, Jl. Sumpah Pemuda Jl. Mt. Kawi VI No.18, Kadipiro, Banjarsari District, Surakarta City, Central Java 57136

ARTICLEINFO

Received: 11 March 2026
Accepted: 14 April 2026
Available Online: 23 April 2026

Keywords:
Standard Clauses; Personal Data Protection; Consumer Protection; Digital Banking; Legal Validity;

Correspondence
*Name: Nimas Yuski Nur Lailli
E-mail:

ABSTRACT

This study aims to analyze the validity of standard clauses in the privacy policy of PT Bank SeaBank Indonesia, particularly in relation to customer personal data protection, and to examine the legal consequences arising from such clauses under Indonesian law. The research employs a normative legal method with statutory and conceptual approaches, relying on primary, secondary, and tertiary legal materials analyzed qualitatively through prescriptive reasoning. The findings reveal that the standard clauses used in SeaBank's privacy policy tend to position customers in a weaker bargaining position through a "take it or leave it" mechanism, granting broad authority to the bank in processing personal data. These clauses are often general, lack transparency, and do not fully comply with the principles of legality, transparency, and informed consent as required by the Personal Data Protection Law and Consumer Protection Law. Furthermore, certain clauses potentially limit the liability of the bank, which may contradict existing legal provisions. Consequently, such clauses may be declared null and void if proven detrimental to customers, and the bank may bear legal responsibility for resulting damages. In conclusion, stronger regulatory supervision, improved transparency, and enhanced legal and digital literacy are essential to ensure effective personal data protection in digital banking services.

Introduction

Indonesia is a legal country where the laws in Indonesia use laws and regulations to enforce laws that are just, useful, and certain (Masriyani et al., 2024). Law is one of the means of community renewal that also develops in all fields of life, including in the economic and technological sectors. The basic rights of every citizen are guaranteed by the constitution and are explicitly regulated in laws and regulations, which normatively become the state's obligation to ensure its protection (Poernomo, 2022). In recent developments, advances in digital technology have driven the transformation of the banking sector towards digital-based services. The influence of globalization with the use of information and communication technology facilities has changed people's lifestyles and encouraged social, economic, cultural, security, and law enforcement changes (Juniardana & Kasih, 2022). This transformation makes it easier for people to make transactions, but at the same time poses a risk to the security and protection of customers' personal data. If previously customers had to come directly to branch offices to open an account, make transfers, or access other banking services, now almost all of these activities can be done online through smart devices.

The rapid development of information technology has changed many conventional functions in the banking sector. Processes such as depositing, withdrawing money, transferring funds, updating data, and registering new customers can now be done through information technology (Arif, 2022). These changes have both positive and negative impacts. On the positive side, the digital era makes it easier for financial transactions to be faster and more efficient. Since the arrival of mobile banking in Indonesia, customers can complete various banking transactions in minutes, anytime and anywhere (Masriyani et al., 2024). However, on the negative side, serious challenges arise regarding consumer data protection (Aprita, 2021). Within the framework of national law, Article 1 number 28 of the Banking Law states that bank secrets include all information related to their depositors and deposits. This principle initially aims to protect the interests of customers, especially related to financial conditions and personal data, as well as maintain trust in banks. However, with the development of digital technology, the management of customer data is no longer limited internally, but involves complex digital systems, thereby increasing the risk of data leakage and cybercrime (Keliat et al., 2023).

In digital banking practices, the protection of customers' personal data is generally regulated through a privacy policy in the form of a standard clause. A standard clause is an agreement whose content is determined unilaterally by the business actor and must be accepted by consumers if they want to use the service (Sakti et al., 2024). Its "take it or leave it" nature creates a potential imbalance in the legal position between the bank as a service provider and the customer as the party who needs the service. Standard clauses often put customers in a weak position because they do not have the opportunity to negotiate. In many cases, these clauses give banks broad authority to access, use, and even share customers' personal data with third parties, without adequate control mechanisms. This condition has the potential to cause violations of consumer rights, especially in the protection of personal data, and raises questions about the validity of the clause from a legal perspective.

Empirical phenomena show that these risks are not only potential, but have occurred in practice. One of the most striking incidents in digital banks occurred from the end of 2024 to early 2025, namely cyber heist or known as "tuyul digital" in Indonesia which caused losses of up to IDR 560,000,000,000. This term is used to describe a cyberattack that causes the silent loss of funds from the banking system. The modes used include ransomware, which is malware that locks the system until the ransom is paid, as well as middleware exploitation and account takeover, which allows perpetrators to legitimately take over access and commit theft without detection (Juniardana & Kasih, 2022). In addition, the case experienced by SeaBank customers shows that there are problems in data protection and system security practices. Fraudulent modes such as incorrect transfers, as well as sudden blocking of accounts without a clear explanation, cause confusion and loss for customers. In fact, the existence of suspicious communication after the incident indicates the possibility of leakage or misuse of personal data (Suleiman et al., 2022).

A number of previous studies have discussed the protection of personal data in the digital financial sector from various perspectives. First, research that focuses on regulatory aspects emphasizes the importance of having a strong legal framework in ensuring the protection of customer data (Keliat et al., 2023; Wijaya, 2023). Second, research that focuses on the technological aspect highlights the vulnerability of digital systems to various forms of cyberattacks (Tasman &

Ulfanora, 2023). Third, research from the perspective of consumer protection law examines standard clauses as instruments that have the potential to harm consumers due to their non-negotiable nature (Juniardana & Kasih, 2022). However, these studies still have limitations. Most of the research focuses only on one specific perspective and has not comprehensively examined the relationship between standard clauses in privacy policies and personal data protection in the context of digital banking. In addition, studies that specifically raise the practice of standard clauses in certain digital banks in Indonesia are still very limited.

Based on this description, it can be formulated that research on data protection in digital banking has developed in three main approaches, namely the regulatory approach, the technology approach, and the consumer protection approach. Some researchers focus on strengthening regulations as a data protection instrument, while other research focuses on the security aspect of the system as a solution to cyber threats. On the other hand, there is research that focuses on standard clauses from the perspective of consumer protection, but is still limited to general analysis and has not specifically linked it to the privacy policy of digital banks. Therefore, there is a research gap, namely there is no study that comprehensively analyzes the validity of standard clauses in digital bank privacy policies by integrating banking law perspectives, consumer protection, and personal data protection, as well as the absence of empirical studies on certain digital banks such as SeaBank.

Therefore, this study intends to fill this gap by analyzing the validity of standard clauses in digital bank privacy policies and their legal implications for customers. The novelty of this research lies in an integrative approach that combines three legal perspectives at once, namely banking law, consumer protection law, and personal data protection law in one complete analytical framework. In addition, this study also makes an empirical contribution by examining the practice of SeaBank as a representation of digital banks in Indonesia. Thus, the purpose of this study is to analyze the validity of standard clauses in digital bank privacy policies and examine the legal consequences caused to customers, especially on PT Bank SeaBank Indonesia.

Method

This research is a normative legal research that focuses on library research (Atmoko, 2023; Setiawan et al., 2022). Normative legal research is understood as a process to find legal rules, legal principles, and legal doctrines to answer the legal issues faced. The normative juridical approach is used as the main approach with an emphasis on the analysis of legal norms contained in laws and regulations and legal concepts that develop in the doctrine (Manangin, 2022).

The approach used in this study includes the legislative approach (*Statute approach*) and conceptual approaches (*conceptual approach*). The legislative approach is carried out by examining various relevant positive legal provisions, especially those related to consumer protection and personal data protection. The conceptual approach is used to examine legal concepts that develop in literature and doctrine, especially related to standard clauses, personal data protection, and legal relationships between business actors and consumers in digital banking services (Iswandari, 2023; Rahmadinata, 2022).

The legal materials used in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations related

to the research object, including the Consumer Protection Law, the Personal Data Protection Law, and other relevant regulations in the field of banking and financial services. Secondary legal materials include literature in the form of books, scientific journals, previous research results, and documents related to the privacy policies of digital banks, especially SeaBank. Meanwhile, tertiary legal materials include supporting materials that provide explanations of primary and secondary legal materials, such as legal dictionaries, encyclopedias, and other reference sources.

The technique of collecting legal materials is carried out through literature studies by inventorying, identifying, and classifying legal materials that are relevant to the research problem. Legal materials are obtained from various sources, both printed and electronic, then selected based on their relevance and credibility to be subsequently systematically compiled in accordance with the research framework.

The analysis of legal materials is carried out qualitatively using the prescriptive analysis method. Qualitative analysis is carried out through the interpretation of legal materials to obtain a comprehensive understanding of the issues being studied. Meanwhile, prescriptive analysis is used to provide legal arguments related to the validity of standard clauses in digital bank privacy policies, by referring to the provisions of laws and regulations and applicable legal principles. Thus, the analysis is focused on assessing the conformity of the standard clauses in SeaBank's privacy policy with the principles of consumer protection and personal data protection, as well as their legal implications for customers.

Results and Discussion

The Validity of the Standard Clauses in SeaBank's Privacy Policy Reviewed from the Personal Data Protection and Consumer Protection

The provisions of the Personal Data Protection Law (PDP Law) affirm that any processing of personal data must comply with the principles of legality, usefulness, openness, clear purpose, and data security. These principles provide a legal basis for data subjects to demand the fulfillment of their rights while establishing a mechanism of responsibility for the party processing the data. With the enactment of the PDP Law, the practice of processing customer data by financial institutions, including digital banking, must be subject to more comprehensive protection standards. These standards include the obligation to conduct data protection impact assessments, notification of leak incidents, and the fulfillment of access and correction rights for data subjects (Hijriani et al., 2023). This shows that personal data protection is no longer purely administrative, but has become an integral part of digital financial service governance. However, the implementation of these provisions still faces various obstacles in the field.

Empirical reality shows that personal data protection in the digital banking sector has not been running optimally. After the passage of the PDP Law, various cases of personal data leakage of mobile banking service users began to emerge. The leaked data generally includes sensitive information such as names, account numbers, addresses, and phone numbers. The leak is suspected to occur due to security gaps in the digital banking system that have not been fully protected. This condition shows that there are still weaknesses in the implementation of the data security system

(Sakti et al., 2024). In addition, the low awareness and digital literacy of the public also exacerbates the risk of data misuse. Thus, the protection of personal data is still a serious challenge in digital banking practices in Indonesia.

The results of the study show that SeaBank's privacy policy contains a standard clause as the basis for regulating the management of customers' personal data. Legally, the use of standard clauses in agreements is allowed as long as it meets the principles of balance, transparency, and does not harm consumers. These principles are as regulated in the Consumer Protection Law and the Personal Data Protection Law. However, in practice, the standard clauses in SeaBank's privacy policy show that there is an imbalance of position between business actors and consumers. Customers are only given the option to accept or reject all provisions without any room for negotiation. This condition is known as the "take it or leave it" principle which has the potential to cause injustice. As a result, customers are in a weaker position in the legal relationship.

As an illustration, a clause commonly found in digital bank privacy policies states that customers give consent to the bank to collect, use, store, and share personal data with third parties. This clause is generally used to support the operation and development of digital banking services. However, the clause often does not explain in detail the type of data processed or the third parties involved. In addition, the consent given is general or blanket consent without separation based on the type of data processing. This has the potential to lead to abuse of authority in data management. Thus, the clause does not fully reflect the principle of transparency regulated in the PDP Law.

Furthermore, it was found that some provisions in the privacy policy are still general and do not provide adequate information to customers. This can be seen from the lack of detailed explanation of the purpose of data collection, storage period, and data deletion mechanism. In addition, the data security protection system is also not comprehensively explained. In fact, the privacy policy clause ideally contains complete information about the scope of data processing, legal basis, and customer rights. This lack of clarity can cause legal uncertainty for customers. This also shows that the principle of openness has not been fully applied in the privacy policy.

In addition, there are clauses that have the potential to limit the bank's liability for customer losses. For example, the bank states that it is not responsible for losses caused by third parties. This kind of clause can unilaterally transfer the responsibility of business actors to consumers. From a consumer protection legal perspective, this clause has the potential to violate provisions that prohibit unreasonable limitation of liability. Therefore, this kind of clause can be declared null and void. Thus, customer protection becomes not optimal if the clause remains enforced.

Based on the principles in the PDP Law, the processing of personal data must be carried out lawfully, transparently, and based on clear and informed consent. Therefore, the standard clauses in SeaBank's privacy policy, which are still general, do not fully meet these standards. Non-specific consent has the potential to cause legal uncertainty for customers. In addition, the lack of transparency can reduce customer trust in digital banking services. This shows that personal data protection is still not optimally implemented. Therefore, the validity of the clause is still legally questionable.

Personal data leakage in digital banking services can occur through various mechanisms. One of the most common forms is phishing, which is fraud that aims to obtain sensitive data from

customers. In addition, data leaks can also occur through malware, system hacking, or illegal access by internal parties. The 2024 report by the State Cyber and Cryptography Agency (BSSN) shows a significant increase in phishing cases. This condition shows that threats to data security are increasingly complex. Therefore, data protection systems must continue to be strengthened to reduce these risks.

The impact of data leaks is not only limited to financial losses, but also includes privacy breaches and identity theft. In addition, data leaks can lower the level of public trust in banking institutions. The 2024 Katadata Insight Center survey shows that most respondents are worried about the security of their personal data. This shows that data protection is an important factor in maintaining public trust. Without adequate protection, the development of digital banking can be hampered. Therefore, personal data protection must be a top priority in digital banking services.

Juridically, the protection of personal data is part of the right to privacy which is included in the constitutional rights of citizens. The state has an obligation to ensure legal protection of these rights. The protection aims to realize legal certainty, justice, and utility. Therefore, various laws and regulations have regulated the protection of personal data explicitly and implicitly. With these regulations, it is hoped that people's rights can be optimally protected.

Thus, it can be concluded that the standard clauses in SeaBank's privacy policy have not fully fulfilled the principles of personal data protection and consumer protection. The imbalance in the position of the parties and the lack of transparency are the main problems in the clause. In addition, the existence of the potential limitation of the liability of business actors further strengthens doubts about the validity of the clause. Therefore, the standard clauses in SeaBank's privacy policy can still be legally questioned.

Legal Consequences and Legal Protection for Customers of the Standard Clauses of SeaBank's Privacy Policy

Standard clauses in the privacy policy that are contrary to laws and regulations can in principle be declared null and void. This provision is in line with the Consumer Protection Law which prohibits the use of clauses that harm consumers or unilaterally transfer the responsibility of business actors. In the context of digital banking, standard clauses that do not meet the principles of transparency, fairness, and balance have the potential to create legal uncertainty for customers (Risqiana et al., 2024). Therefore, the applicability of standard clauses must be tested based on their conformity with applicable legal norms, especially those related to the protection of personal data. If the clause is contrary to the law, then it does not have binding force. Thus, it is important to ensure that each clause in the privacy policy is drafted proportionately and does not harm the customer as a consumer.

The legal consequences of invalid standard clauses can be seen from the aspect of the validity of the agreement and the legal responsibility of the business actor. From the aspect of validity, clauses that are contrary to the law are considered invalid and cannot be used as a basis for imposing obligations on customers. Meanwhile, from the aspect of responsibility, the bank can be held accountable for losses arising from the misuse or leakage of personal data. This responsibility includes the obligation to provide compensation to the aggrieved customer. In addition, banks can

also be subject to administrative, civil, and criminal sanctions in accordance with applicable regulations. Therefore, the standard clause cannot be used as a tool to avoid the legal responsibility of business actors.

Within the framework of legal protection, customers as data subjects have rights guaranteed by laws and regulations. These rights include the right to object to the processing of personal data, the right to claim compensation for losses experienced, and the right to request correction or deletion of data. These rights are a form of legal protection provided by the Personal Data Protection Law and the Consumer Protection Law. However, in practice, the fulfillment of these rights often faces obstacles, such as a lack of transparency from banks and a low level of public legal literacy. This condition causes customers to not be able to fully utilize their rights optimally. Therefore, efforts to improve legal and digital literacy are needed so that legal protection can run effectively.

On the other hand, banks as business actors have an obligation to improve security systems and transparency in the management of customers' personal data. This obligation is not only normative, but also part of professional responsibility in maintaining customer trust. Violations of these obligations can lead to legal consequences in the form of administrative, civil, and criminal sanctions. In this case, the role of the government and regulatory agencies, such as the Financial Services Authority, is very important to ensure business actors' compliance with applicable regulations. In addition, effective supervision is also needed to prevent violations that can harm customers. Thus, legal protection does not only depend on legal norms, but also on the effectiveness of supervision and law enforcement.

However, until 2025, there will be no criminal court decision with permanent legal force (inkracht) that explicitly imposes sanctions for personal data leakage based on the Personal Data Protection Law. This is due to the relatively recent nature of the law, which was promulgated in 2022 and only completed the transition period in October 2024. However, the PDP Law has regulated fairly severe criminal sanctions for acts such as falsification, sale, or purchase of personal data. This provision shows that the state has a strong commitment to protecting people's personal data. In addition, the authority of the Financial Services Authority to impose administrative sanctions on banks also strengthens the law enforcement system in the banking sector. Thus, although its implementation is still developing, the existing legal framework has provided an adequate basis.

In the contractual realm, standard clauses in privacy policies have an important role in regulating the legal relationship between banks and customers. These clauses are instruments to allocate the rights and obligations of the parties, including in terms of processing and protection of personal data. However, if the clauses are drafted in an intransparent manner or provide disproportionate benefits to one of the parties, then the protection function becomes suboptimal. Therefore, more detailed technical guidelines are needed in the preparation of standard clauses to comply with the principles of consumer protection and personal data protection. In addition, increased supervisory capacity is also needed so that the accountability mechanism can run effectively. Thus, standard clauses must be positioned as an instrument of legal protection, not just an administrative tool.

The dispute resolution mechanism between customers and banks in the Indonesian banking system can be pursued through various channels. The first path is an internal mechanism through

complaints to the bank. The second path is out-of-court dispute resolution, such as mediation or arbitration, which aims to provide a quick and efficient resolution. However, if the settlement is inadequate, customers can take the litigation route through the court. In this context, civil lawsuits and class actions can be alternatives for customers. However, the litigation process often requires a lot of time and money, making it a challenge for customers. Therefore, a more effective and accessible dispute resolution mechanism is needed.

Facts show that delays in notifying data leak incidents and lack of transparency can exacerbate the impact of losses experienced by customers. In addition, these conditions can also reduce the level of public trust in banking institutions. Therefore, compliance with notification obligations is an important indicator in assessing bank accountability. In this case, the role of various parties, including the government, regulators, and business actors, is indispensable to create an effective data protection system. The rapid development of digital banking, especially after the pandemic, further emphasizes the importance of strengthening regulations and supervision. Thus, personal data protection is one of the crucial aspects in supporting the sustainability of the digital financial system in Indonesia.

Thus, it can be concluded that the legal consequences of the standard clauses in SeaBank's privacy policy are highly dependent on their conformity with laws and regulations. Clauses that are contrary to the law can be declared null and void and have no binding force. In addition, banks can be held accountable for losses suffered by customers. Therefore, it is necessary to increase transparency, accountability, and supervision in the preparation and implementation of standard clauses. With optimal legal protection, it is hoped that public trust in digital banking services can continue to increase.

Conclusion

The findings of the study show that standard clauses in the privacy policies of digital banks, including SeaBank, are conceptually permissible within the legal framework of the agreement, but their enforceability is highly dependent on the fulfillment of the principles of transparency, balance, and consumer protection. In practice, the clauses used still contain normative weaknesses, especially related to the unclear purpose of data processing, limited information regarding the storage and use of data, and the absence of a specific and informed consent mechanism. In addition, the construction of clauses that are unilateral and do not provide negotiation space to customers shows that there is an imbalance in the position of the parties. This condition indicates that the existing privacy policy does not fully reflect the principles of personal data protection and consumer protection as stipulated in laws and regulations.

From a juridical aspect, the incompatibility of the standard clause with the legal provisions has implications for the potential for the nullity of the clause and the non-enactment of legally binding force. In situations where losses occur due to misuse or leakage of personal data, legal responsibility remains inherent in the bank as the data controller. Meanwhile, customers have legal rights to obtain protection, including the right to file objections, demand compensation, and control their personal data. Therefore, it is necessary to strengthen data protection governance through increased transparency, accountability, and effectiveness of supervision by relevant authorities.

These efforts also need to be accompanied by increasing legal and digital literacy of the public in order to create a more balanced legal relationship in digital banking practices.

References

Aprita, S. (2021). Peranan Peer to Peer Lending Dalam Menyalurkan Pendanaan Pada Usaha Kecil Dan Menengah. *Jurnal Hukum Samudra Keadilan*, *16*(1), 37–61. https://doi.org/10.33059/jhsk.v16i1.3407

Arif, F. M. (2022). Actualization of Reasoning Philosophical Standars in Personal Data Protection. *Jsi*, *11*(1), 1–25. https://doi.org/10.33477/jsi.v11i1.2903

Atmoko, D. (2023). Penerapan Asas Kebebasan Berkontrak Dalam Suatu Perjanjian Baku. *Binamulia Hukum*, *11*(1), 81–92. https://doi.org/10.37893/jbh.v11i1.308

Hijriani, H., Nur, M. N. A., Al-Jasim, A. A. N., Ali, A., & Siregar, W. A. (2023). Literasi Digital Perlindungan Hukum Terhadap Data Pribadi Nasabah Pengguna Electronic Wallet. *Sultra Research of Law*, *5*(2), 85–95. https://doi.org/10.54297/surel.v5i2.59

Iswandari, F. (2023). Tanggungjawab Notaris Yang Tidak Hadir Dalam Pembuatan Akta Perjanjian Kredit Di Bank. *The Juris*, *7*(1), 74–84. https://doi.org/10.56301/juris.v7i1.831

Juniardana, I. G. A., & Kasih, D. P. D. (2022). Urgensi Regulasi Financial Technology (Fintech) Pinjaman Online Melalui Pembayaran Perbankan. *Kertha Semaya Journal Ilmu Hukum*, *10*(10), 2305. https://doi.org/10.24843/ks.2022.v10.i10.p09

Keliat, V. U., Siregar, A. P., Zulkifli, S., & Purba, I. H. (2023). Analisis Upaya Dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia. *Ilmu Hukum Prima (Ihp)*, *6*(2), 182–190. https://doi.org/10.34012/jihp.v6i2.4251

Manangin, S. A. (2022). The Clause of the Murabahah Financing Agreement in Sharia Banking. *Sign Jurnal Hukum*, *3*(2), 135–150. https://doi.org/10.37276/sjh.v3i2.160

Masriyani, M., Siregar, N. O., & Tresya, T. (2024). Tinjauan Yuridis Terhadap Penyebaran Data Pribadi Yang Dilakukan Oleh Aplikasi Pinjaman Online Ilegal. *Wajah Hukum*, *8*(1), 249. https://doi.org/10.33087/wjh.v8i1.1459

Poernomo, S. L. (2022). Perlindungan Hukum Konsumen Terhadap Praktik Teknologi Finansial Ilegal Dalam Bentuk Pinjaman Online Ilegal. *Mimbar Keadilan*, *15*(1), 134–148. https://doi.org/10.30996/mk.v15i1.6081

Rahmadinata, Y. (2022). Pengalihan Piutang Secara Cessie Sebagai Alternatif Penyelesaian Kredit Dan Akibat Hukumnya Terhadap Jaminan Hutang Debitur. *Recital Review*, *4*(1), 25–61. https://doi.org/10.22437/rr.v4i1.15273

Risqiana, R., Hayfa, J., Rani, R. V. R. P., & Wungkana, S. R. (2024). Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions. *Jurnal Penelitian Ilmu-Ilmu Sosial*, *5*(1), 19–33. https://doi.org/10.23917/sosial.v5i1.2375

Sakti, M., Utami, K., & Sulastri, S. (2024). The Urgency of Standardizing the Open Application Programming Interface in Implementation of Open Banking for Customer Protection. *Jurnal Hukum Samudra Keadilan*, *19*(1), 29–44. https://doi.org/10.33059/jhsk.v19i1.7471

Setiawan, R. R. B., Firdiansyah, M. R. D., & Hidayatullah, M. S. (2022). Perlindungan Hukum Bagi Konsumen Pdam Surya Sembada Kota Surabaya Atas Penetapan Tarif Dalam Kontrak Baku. *Bureaucracy Journal Indonesia Journal of Law and Social-Political Governance*, *2*(1), 687–702. https://doi.org/10.53363/bureau.v2i1.161

Suleiman, A., Audrine, P., & Dewaranu, T. (2022). *Pengaturan Bersama Dalam Perlindungan Data Pribadi:*

Potensi Peran Asosiasi Industri Sebagai Organisasi Regulator Mandiri. https://doi.org/10.35497/555906

Tasman, T., & Ulfanora, U. (2023). Perlindungan Hukum Terhadap Nasabah Bank Digital. *Unes Law Review*, 6(1), 1624–1635. https://doi.org/10.31933/unesrev.v6i1.962

Wijaya, T. (2023). *Berkembangnya Sistem Innovative Credit Scoring Di Indonesia Menilai Risiko Dan Tantangan Kebijakan*. https://doi.org/10.35497/560781