GOLDEN RATIO OF DATA IN SUMMARY
VOLUME 6, ISSUE. 1 (2025)
Website: https://goldenratio.id/index.php/grdis

GOLDEN RATIO
ISSN [Online]: 2776-6411

DATA IN SUMMARY | LAW, POLITICS, PUBLIC ADMINISTRATION

Legal Liability of Financial Services Institutions for Personal Data Leakage Under the Personal Data Protection Act

Anindyto Rafa Kristanto[1], Sri Redjeki Slamet[2]

[1,2] Department of Law, Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia.
Email: anindytor@student.esaunggul.ac.id[1], sri.redjeki@esaunggul.ac.id[2]

ARTICLE HISTORY

Received: December 22, 2025
Revised: January 20, 2026
Accepted: January 27, 2026

DOI
https://doi.org/10.52970/grdis.v6i1.1981

ABSTRACT
The rapid digitalization of the financial services sector has improved efficiency, but it has also increased the risk of personal data breaches, which may result in financial losses, including the emergence of fake debtors. This study aims to analyze the scope of corporate legal liability as a Personal Data Controller in cases of personal data breaches and to identify obstacles in supervising personal data protection. This research employs a normative juridical method using secondary legal materials, supported by empirical data obtained through interviews. Data were analyzed using qualitative normative analysis. The findings indicate that corporate entities remain legally liable under Articles 67 and 70 of Law Number 27 of 2022 concerning Personal Data Protection, even when violations are committed by internal personnel. Such liability is based on the principles of vicarious liability and strict liability, requiring corporations to ensure data security through effective supervision and risk management systems. However, the implementation of personal data protection faces significant challenges, including weak compliance culture, low employee awareness, limited technological monitoring, and inconsistent internal policies. Therefore, strengthening data governance through technological enhancement, mandatory employee training, and consistent regulatory supervision is essential to ensure legal certainty and the protection of consumer privacy rights in the financial services sector.

Keywords: Legal Responsibility, Personal Data Breach, Personal Data Protection Act, Personal Data Protection.

I. Introduction

Along with the rapid development of digital technology, there has been a fundamental shift in the way financial service institutions operate, particularly in the management of consumers' personal data as a legal asset of high value. Digital transformation in Indonesia's financial services sector has brought efficiency and improved access to services; however, it has also generated serious risks in the form of personal data breaches that may result in financial losses, identity fraud, and the misuse of personal information. This condition necessitates heightened awareness and the implementation of effective preventive measures by the government, corporations, and society to protect individuals' right to privacy. If personal data is not managed optimally, it may potentially disrupt the stability of the digital financial ecosystem and erode public trust. (Rima et al., 2023). To date, Indonesia is in urgent need of policies or regulations on personal data

ISSN [Online]: 2776-6411

protection that are consolidated within a single, specific legal framework. Existing regulations on personal data protection remain fragmented across various laws and regulations, and generally address personal data protection only in a broad and general manner. Therefore, there should be no separation among these interrelated legal provisions. A clear and firm legal umbrella is required to enable law enforcement authorities to act effectively in response to the proliferation of online lending entities that fail to comply with their obligations toward debtors or consumers, particularly about personal data protection. With the existence of regulations that specifically and comprehensively govern law enforcement mechanisms, law enforcement agencies will have legal certainty in taking action against any conduct that harms the public in relation to personal data, which has frequently become a recurring issue in numerous cases (Widi et al., 2021).

The widespread misuse of personal data and the increasing consumer awareness of the importance of safeguarding privacy compel companies to become more vigilant and to undertake internal reforms. Companies must understand the applicable regulations, principles, and practices of personal data protection, not only to respect consumers' rights but also to avoid losing the trust and loyalty of their customers. (Thalib & Maswari, 2021). Law Number 27 of 2022 on Personal Data Protection emphasizes the obligations of data controllers and/or data processors to ensure that all personal data processing activities are conducted lawfully, transparently, accountably, and responsibly. This regulation aims to guarantee the security of individuals' personal data and to strengthen corporate responsibility in the management of sensitive information (Aulia Alayna Suvil et al., 2024). Personal data is now recognized as a strategic asset with high economic value; however, it is also highly vulnerable to misuse for illegal purposes, including cybercrimes such as fraud and identity theft. Therefore, the Personal Data Protection Law imposes criminal sanctions for any serious violations, including those committed by corporations that fail to adequately safeguard personal data (Putra et al., 2024).

Although a strong legal foundation has been established normatively, its implementation in practice continues to face various challenges, particularly the weak enforcement of personal data protection within financial companies. One prominent phenomenon is the emergence of cases involving fictitious debtors, namely, the misuse of customers' personal data by employees, such as Account Officers, to submit fraudulent financing applications. This situation indicates deficiencies in internal supervision and access control mechanisms and illustrates the tangible threat posed by insider threats. Such conditions reflect the inadequate implementation of security governance, which should constitute a concrete manifestation of compliance with the Personal Data Protection Law. These facts demonstrate a discrepancy between the normative objectives of the law (*das sollen*) and the reality of its implementation in practice (*das sein*) in the administration of personal data protection. Although companies are legally required to ensure the security and accountability of data processing activities, many have yet to adequately implement system audit principles and risk mitigation measures.

The gap between legal provisions and actual practice gives rise to a fundamental issue concerning the limits of corporate legal liability. Legal loopholes remain evident in the aspect of corporate accountability when data breaches are committed by internal individuals. There is still no uniform understanding regarding the extent to which corporations can be held legally liable, particularly when the perpetrators act beyond their formal authority. Under the doctrines of vicarious liability and strict liability, companies remain obligated to ensure the security of data under their control. In this context, the implementation of Good Corporate Governance (GCG) principles serves as a crucial instrument for ensuring accountability and comprehensive data protection. Furthermore, according to Gustav Radbruch's legal theory, a balance between justice (gerechtigkeit), expediency or utility (zweckmäßigkeit), and legal certainty (rechtssicherheit) must be maintained in order for the legal system to function effectively and fairly (Keadilan & Kepastian, 2022). Therefore, an academic study is required that not only examines the prevailing legal norms but also assesses the extent of their effectiveness and the obligations of corporations in ensuring the implementation of consumer personal data protection.

Considering the gap between legal norms and practical implementation, this study is significant in examining the legal liability of financial service institutions in their capacity as Personal Data Controllers for

ISSN [Online]: 2776-6411

data breach incidents that result in fictitious debtors, as well as in identifying the inhibiting factors in the supervision and enforcement of personal data protection. This research is analyzed using three theoretical frameworks, namely the Theory of Corporate Liability, Gustav Radbruch's Theory of Legal Certainty, and the Theory of Legal Protection as implemented through the principles of Good Corporate Governance (GCG). This study is expected to provide an academic contribution to strengthening the implementation of the Personal Data Protection Law and to serve as a reference for the development of personal data protection practices in Indonesia. Furthermore, the findings are anticipated to encourage companies to reinforce internal policies related to personal data breach risk management in order to ensure more optimal consumer protection in the digital era. As privacy protection collectively contributes to the development of a constitutional framework that not only safeguards individual rights but is also capable of effectively responding to the complexities posed by the digital era, the continuously evolving nature of technology requires legal systems to adapt consistently so that constitutional principles remain effective as safeguards of citizens' rights within an ever-changing landscape. (Aka Akbar et al., 2023).

II. Literature Review and Hypothesis Development

The Theory of Corporate Liability is employed to explain the legal accountability of corporations as legal subjects for acts committed by their organs or employees. In this context, the doctrine of *vicarious liability* affirms that a corporation may be held liable for unlawful acts committed by its employees, provided that such acts occur within the scope of their employment. Meanwhile, the principle of *strict liability* imposes responsibility on the corporation without the need to prove fault, particularly in cases involving failures in internal supervision and control systems. This principle is relevant in assessing the liability of Company "X" as a Personal Data Controller for data breaches that result in fictitious debtors, even when the violations are perpetrated by internal actors (Kurniawan & Hapsari, 2022).

Gustav Radbruch's Theory of Legal Certainty emphasizes that the law must provide clear, systematic, and consistent rules so that it can be predictable for society. Legal certainty constitutes one of the fundamental values that must be accommodated alongside the values of justice (gerechtigkeit) and utility or expediency (zweckmäßigkeit). In research on personal data protection, this theory is employed to evaluate the extent to which Law Number 27 of 2022 has provided legal certainty regarding corporate obligations and legal liability in cases of data breaches, as well as to explain the gap between ideal legal norms (das sollen) and the reality of practical implementation (das sein). The Theory of Legal Protection is analyzed through the implementation of Good Corporate Governance (GCG) principles, particularly accountability, responsibility, transparency, and prudence. GCG principles require companies to establish governance systems capable of protecting stakeholders' interests, including consumers' privacy rights and personal data security. The OECD emphasizes that sound corporate governance constitutes a crucial foundation for maintaining stability, public trust, and legal protection against operational risks, including the risk of data breaches. Accordingly, the implementation of GCG serves as an essential instrument in ensuring that personal data protection is carried out effectively and sustainably (OECD, 2023).

III. Research Method

This research employs a normative juridical research method that focuses on the examination of legal instruments, particularly statutory regulations, while also taking into account social realities that are directly related to the object of the study (Lestari, 2022). In this study, the author applies several approaches, namely the statute approach to analyze Law Number 27 of 2022 on Personal Data Protection along with other relevant regulations; the conceptual approach to examine theories of corporate liability, personal data protection, and the principles of Good Corporate Governance; and the case approach through an analysis of relevant court decisions or legal practices (Marzuki Peter Mahmud, 2005). This research utilizes secondary data consisting of:

ISSN [Online]: 2776-6411

a. Primary legal materials, namely statutory regulations and court decisions, including the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection, and Financial Services Authority Regulation Number 1/POJK.07/2013, along with its implementing regulations.
b. Secondary legal materials, in the form of books, scholarly journals, and academic publications relevant to the research topic.
c. Tertiary legal materials, consisting of legal dictionaries and legal encyclopedias.

To complement the secondary data, this research is supported by empirical data obtained through interviews. The respondent in this study is an employee of Company X who serves in the second line of defense, namely the Data Protection Officer, selected based on the relevance of the position and direct involvement in the management and supervision of personal data protection within the company. The interview was conducted with Mr. Nurman Rasyid Panusuhan Hutasuhut via Zoom as a communication medium. Data collection techniques were carried out through library research by examining primary, secondary, and tertiary legal materials, as well as interviews to support the secondary data. The collected data were analyzed using a normative qualitative analysis method, with an emphasis on the examination of legal norms, legal principles, and relevant statutory provisions. The analysis was conducted through processes of legal interpretation, systematization, and evaluation, followed by deductive reasoning to conclude addressing the research questions.

IV. Result and Discussion

4.1. Forms and Limits of the Legal Liability of Financial Service Institutions as Personal Data Controllers in Data Breach Cases Resulting in Fictitious Debtors under Law Number 27 of 2022

Personal data protection is a logical consequence of the recognition of human rights as stipulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which affirms that every person has the right to protection of their personal self, family, honor, dignity, and property under their control. The right to personal data, as an extension of the right to privacy, is inherent in every individual and must be respected by both the state and corporations engaged in data processing activities. The findings of this study at Company "X" indicate that the implementation of legal responsibilities as a Personal Data Controller has not been fully optimized in accordance with the personal data protection principles outlined in Law Number 27 of 2022, particularly about internal access supervision and data breach risk mitigation. This condition demonstrates a gap between ideal legal norms and the actual practice of personal data management in the field.

These findings further reinforce the urgency of applying the principles of vicarious liability and strict liability, under which companies may still be held legally accountable for unlawful acts committed by employees under their control when negligence in supervision and data security systems can be established. Law Number 27 of 2022 on Personal Data Protection was enacted based on constitutional considerations as mandated by the 1945 Constitution of the Republic of Indonesia. This regulation aims to ensure legal certainty and to provide protection for individuals' constitutional rights to their personal data. Such protection applies to all individuals, whether Indonesian citizens or foreign nationals residing in Indonesia, across all stages of personal data processing, including collection, use, storage, and deletion (Unggul, 2023).

The norms contained in the Personal Data Protection Law position personal data controllers, including financial service institutions, as the primary legal subjects bearing the obligation to ensure the security, integrity, and confidentiality of personal data. Companies are required to ensure that data processing is conducted lawfully, transparently, proportionally, and solely for legally legitimate purposes. These provisions establish the basis for corporate obligations to mitigate all risks of data misuse, including those originating from within the company itself (Sulistianingsih et al., 2023). In the context of financial service

ISSN [Online]: 2776-6411

institutions, such legal obligations encompass the implementation of internal data protection policies, strict access controls, and the use of adequate information technology security systems. Failure to fulfill these obligations constitutes a form of negligence that may give rise to administrative, civil, and criminal liability. In practice, data breaches that result in fictitious debtors are in fact committed by internal actors who misuse access to customers' personal data. This situation demonstrates weaknesses in internal supervision and access control mechanisms, while simultaneously indicating a serious threat posed by insider threats.

Juridically, this condition reflects corporate liability based on the doctrines of *vicarious liability* and *strict liability*. Even though the acts were committed beyond formal authority, legal responsibility remains attached to the corporation as the Personal Data Controller due to its failure to exercise adequate supervision and to secure its systems. This is consistent with the principle of corporate responsibility, which emphasizes the obligation of corporations to ensure the protection of data under their control. The misuse of personal data may constitute a criminal act involving elements such as theft, online fraud, the creation of fake accounts, money laundering, the existence of fraudulent marketplaces, and illegal transactions in digital markets (Mahameru et al., 2023). These criminal provisions are explicitly stipulated in Article 67 paragraph (3) of Law Number 27 of 2022 on Personal Data Protection, which states: *"Any person who intentionally and unlawfully uses Personal Data that does not belong to them as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of five (5) years and/or a fine of up to IDR 5,000,000,000 (five billion rupiah)."*

Furthermore, Article 70 paragraphs (1) to (4) provide that where criminal acts as referred to in Articles 67 and 68 are committed by a corporation, criminal liability may be imposed on the management, controlling persons, those who give orders, beneficial owners, and/or the corporation itself. The sanctions imposed may take the form of a criminal fine of up to ten (10) times the maximum fine prescribed, in addition to the fines stipulated under Article 67. Such sanctions may also be accompanied by additional penalties, including the confiscation of profits and/or assets obtained from or resulting from the criminal act, the suspension of all or part of the corporation's business activities, permanent prohibition from engaging in certain activities, the closure of all or part of the corporation's business premises and/or operations, the obligation to fulfill neglected duties, the payment of compensation, the revocation of licenses, and/or the dissolution of the corporation.

These provisions reflect the criminal sentencing system established under the Personal Data Protection Law, which, in principle has been formulated in accordance with the general objectives of punishment. These objectives include: (1) preventing the commission of criminal acts by upholding legal norms for the protection and safeguarding of society; (2) rehabilitating offenders through guidance and development so that they may become constructive members of society, as well as resolving conflicts arising from criminal acts; (3) restoring balance and fostering a sense of security and social peace; and (4) cultivating remorse and relieving the offender's sense of guilt. Ultimately, regardless of how well-designed the criminal and sentencing framework is as regulated under statutory law—particularly the Personal Data Protection Law—if these punitive provisions are never effectively enforced, they will give rise to various issues concerning the application of the criminal justice system and sentencing practices in Indonesia (Watkat et al., 2024).

These provisions affirm that corporate responsibility is comprehensive in nature, encompassing systems, policies, and internal supervisory mechanisms. The scope of a company's legal liability as a Personal Data Controller extends to the entire data lifecycle, including the collection, storage, processing, and deletion of personal data, whether conducted by internal units or third parties. From the perspective of Gustav Radbruch's theory of legal certainty, corporate responsibility in personal data protection represents the embodiment of the principle of *rechtssicherheit*. Inconsistencies in the enforcement of legal obligations may disrupt the balance between legal certainty, justice, and legal utility. Therefore, the imposition of sanctions is not merely repressive in nature but also aims to restore public trust and to uphold corporate accountability. Accordingly, the legal liability of Company "X" as a Personal Data Controller encompasses administrative, civil,

ISSN [Online]: 2776-6411

and criminal responsibility. At present, the company has initiated evaluations and improvements to its data security systems in order to prevent the recurrence of similar incidents.

4.2. Inhibiting Factors in the Supervision of Personal Data Protection within Financial Service Institutions

Based on the results of an interview with Mr. Nurman Rasyid Panusunan Hutasuhut, the Data Protection Officer (DPO) of Company "X", conducted on 1 December 2025, it was found that the company has established relatively comprehensive personal data governance policies, including master data handling, data ethics, and data governance, as derivatives of its internal personal data protection guidelines. These disparities are attributable to the low level of employees' understanding of and compliance with data security policies, resulting in risk mitigation measures that have not been comprehensively implemented. This condition reflects a gap between normative provisions (*das sollen*) and factual practice (*das sein*), which undermines the effectiveness of personal data protection within the corporate environment. Furthermore, the implementation of these policies has not been applied uniformly across all organizational units. There exists a disparity in enforcement between the head office and other operational units or branch offices, where incidents of data breaches and fictitious customer cases occur more frequently than at the head office. This situation is largely caused by differences in employees' levels of understanding and compliance with data security policies, thereby preventing risk mitigation measures from being implemented effectively and comprehensively.

Although, to date, no direct legal claims have been filed by the victims, the company acknowledges existing security vulnerabilities that require immediate remediation through the enhancement of verification mechanisms and credit application procedures. However, the implementation of these policies has not been applied uniformly across all organizational units. This disparity stems from gaps in knowledge and awareness between the head office, which has a relatively stronger understanding of regulatory requirements and the urgency of data security, and branch offices, which tend to perceive data management merely as a routine administrative process. where incidents of data breaches and fictitious debtor cases occur more frequently at the branch level. This is attributable to employees' low levels of understanding of and compliance with data security policies, resulting in risk mitigation measures that have not been optimally implemented. Another major obstacle is the weak compliance culture and the low level of data privacy awareness at the operational level. This condition is further exacerbated by high employee turnover, which hinders the effective transfer of knowledge regarding personal data protection. In addition, societal culture that has not yet regarded data privacy as a serious issue also contributes to the low level of awareness of the importance of personal data protection.

Furthermore, according to the statement of Mr. Nurman Rasyid Panusunan Hutasuhut in an interview conducted on 1 December 2025 via Zoom, the low level of awareness is also influenced by Indonesian societal culture, which has not yet positioned data privacy as a serious issue. This stands in contrast to the concept of the General Data Protection Regulation (GDPR) in Europe, which serves as a foundational framework for modern data protection policies. Prior to elaborating on conceptual discussions, it is essential to examine the scope and practical field of personal data protection itself. In several developed countries, personal data protection has been recognized as an integral part of human rights that must be safeguarded, and accordingly, regulatory frameworks have been established to accommodate such protection. From a technological perspective, technology-based monitoring systems have not yet been optimally integrated to detect abnormal data access behavior in real time. As a result, potential data misuse may persist for extended periods without being detected.

Referring to Financial Services Authority Regulation Number 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector, the Financial Services Authority (OJK) has the authority to conduct supervision and impose administrative sanctions. However, the effectiveness of such supervision continues to face implementation challenges, resulting in administrative sanctions being rarely applied in a consistent manner. From the perspective of Gustav Radbruch's theory of legal certainty, weak implementation and the

ISSN [Online]: 2776-6411

lack of firm sanctions diminish the value of legal certainty. Without legal certainty, the protection of personal data privacy rights cannot be effectively realized. Based on normative analysis and interview findings, the obstacles to supervising personal data protection at Company "X" lie in four main aspects, namely technology, human resources, internal governance, and organizational culture. Therefore, it is necessary to strengthen digital security infrastructure, enhance employee competence through continuous training, and harmonize operational standards across work units to ensure that personal data protection is implemented in accordance with the mandate of Law Number 27 of 2022 and the principles of Good Corporate Governance (GCG).

V. Conclusion

Based on a review of the scope and limits of legal liability, it can be concluded that Company X, in its capacity as a Personal Data Controller, bears full legal responsibility for personal data breaches that result in fictitious debtors, even when such acts are committed by internal actors. Under Law Number 27 of 2022 on Personal Data Protection, this responsibility encompasses the obligation to ensure the security, confidentiality, and integrity of personal data through strict access supervision, the implementation of adequate information security systems, and sustainable risk management. The company's failure to exercise effective internal supervision constitutes legal negligence, giving rise to administrative, civil, and criminal liability in accordance with the doctrines of vicarious liability and strict liability. Therefore, the company is required to report data breach incidents, conduct comprehensive security system evaluations, and improve data governance to ensure accountability and compliance with personal data protection principles.

The main factors hindering the supervision of personal data protection at Company X include a weak compliance culture, low levels of employee understanding of data security, the suboptimal use of technology for early detection, and inconsistencies in the implementation of data protection policies across organizational units. These conditions reflect a gap between normative legal provisions and practical implementation. Accordingly, strengthening digital security systems, implementing mandatory training for all employees, and ensuring consistent and firm supervision by the Financial Services Authority (OJK) and the government constitute strategic measures to enhance the effectiveness of the Personal Data Protection Law, reinforce legal certainty, and foster public trust in personal data governance within the financial services sector. Company X is advised to reinforce its personal data security framework through the enhancement of early detection technologies, the implementation of stricter access controls, the conduct of periodic data security audits, and the enforcement of internal disciplinary measures for any violations of data governance policies. These measures should be accompanied by mandatory and continuous training programs for all employees in order to build a consistent and sustainable compliance culture.

The Financial Services Authority (OJK) is expected to intensify its supervisory role and to apply administrative sanctions consistently against financial service providers that fail to adequately protect personal data, thereby ensuring the more effective implementation of the Personal Data Protection Law and providing legal certainty for the public. Meanwhile, the government should strengthen public outreach and technical assistance concerning the obligations of data controllers, as well as encourage the standardization of data security systems within the financial services sector in order to minimize the risk of data breaches and enhance public trust in personal data governance in the digital era.

References

Aka Akbar, R., Mulyana, A., & Amalia, M. (2023). Legal Challenges in The Age Of Social Media: Protecting Citizens From Misuse Of Information. Golden Ratio of Law and Social Policy Review, 3(1), 14–25. https://doi.org/10.52970/grlspr.v3i1.328

Aulia Alayna Suvil, Firdaus, Ramadhan, M. A., Putra, W. D., & Lestarika, D. P. (2024). Implementasi perlindungan data pribadi berdasarkan Undang-Undang Nomor 11 Tahun 2020. Jurnal Hukum, Politik dan Ilmu Sosial, 3(4), 70–80. https://doi.org/10.55606/jhpis.v3i4.4235

ISSN [Online]: 2776-6411

Keadilan, T., & Kepastian, D. A. N. (2022). Implementasi aturan perlindungan data pribadi oleh penyelenggara sistem elektronik dikaitkan dengan teori keadilan dan kepastian hukum. Jurnal Hukum, 7(2), 86–103.

Kewarganegaraan, J., Setiawan, H. B., Najicha, F. U., Fakultas Hukum, & Universitas Sebelas Maret. (2022). Perlindungan data pribadi warga negara Indonesia. Jurnal Kewarganegaraan, 6(1), 976–982.

Kurniawan, K. D., & Hapsari, D. R. I. (2022). Pertanggungjawaban pidana korporasi menurut vicarious liability theory. Ius Quia Iustum Law Journal, 29(2), 328–347. https://doi.org/10.20885/iustum.vol29.iss2.art5

Lestari, D. P. (2022). Analisis yuridis normatif pemberian kompensasi perjanjian kerja waktu tertentu (PKWT) berdasarkan Undang-Undang Cipta Kerja. Jurnal Hukum Lex Generalis, 3(5), 339–349. https://doi.org/10.56370/jhlg.v3i5.160

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). Implementasi Undang-Undang perlindungan data pribadi. Jurnal Hukum, 5(2), 115–131.

Marzuki, P. M. (2005). Penelitian hukum. Jakarta: Prenadamedia Group.

OECD. (2023). G20/OECD principles of corporate governance. OECD Publishing.

Pribadi, D. (2021). Pentingnya Undang-Undang perlindungan data pribadi sebagai perlindungan hukum terhadap privasi di Indonesia. E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha, 4(3), 1056–1064.

Putra, R. K., Idris, M. F., & Widhiati, G. (2024). Perlindungan data pribadi dalam era big data: Implikasi hukum di Indonesia. Jurnal Kajian Ilmu Hukum dan Politik, 2(4), 31–44. https://journal.stekom.ac.id/index.php/jaksa

Radbruch, G. (2006). Legal philosophy. Oxford University Press.

Rima, K., Suari, A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. Jurnal Analisis Hukum, 6(1), 132–146. https://doi.org/10.38043/jah.v6i1.4484

Sulistianingsih, D., Ihwan, M., & Setiawan, A. (2023). Tata kelola perlindungan data pribadi di era metaverse (Telaah yuridis Undang-Undangz Perlindungan Data Pribadi). Jurnal Hukum, 1(52), 97–106.

Thalib, E. F., & Maswari, K. L. (2021). Perlindungan Hukum Terhadap Data Pribadi Perusahaan Akibat Penyalahgunaan Data Digital Oleh Karyawan Perusahaan. Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020, Vol 1(No 1), 55–66. https://money.kompas.com/read/2020/11/09/2135

Unggul, U. E. (2023). Perlindungan data pribadi dalam perspektif hukum. Jurnal Multidisiplin Indonesia, 2(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Watkat, F. X., Ingratubun, M. T., Apriyanti, A., & Pribadi, D. (2024). PERLINDUNGAN DATA PRIBADI MELALUI PENERAPAN. 5(1).

Widi, F., Qahar, A., & Aswari, A. (2021). Legal Protection Against Personal Data In Online Loan Transactions. Golden Ratio of Law and Social Policy Review, 1(1), 17–25. https://doi.org/10.52970/grlspr.v1i1.152