P-ISSN: 2987-8071 | E-ISSN: 2987-8063 | DOI: https://doi.org/10.53955/jsderi.v3i3.97

Journal of Sustainable Development and Regulatory Issues (JSDERI)
http://journal.contrariusactus.com/index.php/JSDERI/index

| Research Article |

The Accountability Principle in Personal Data Protection in Sweden and Indonesia

Wardah Yuspin [1], *, Kelik Wardiono [1], Arief Budiono [1], Andria Luhur Prakoso [1], Trisha Rajput [2]

[1] Faculty of Law, Universitas Muhammadiyah Surakarta, Sukoharjo, Indonesia.
[2] School of Business, Economics and Law, University of Gothenburg, Sweden.

** Correspondence: wy204@ums.ac.id*

Received: June 23, 2025 / Accepted: October 14, 2025 / Published: October 16, 2025

Abstract: Digital transformation presents significant challenges in safeguarding the personal data of banking customers, particularly when banks collect and manage extensive personal information without ensuring adequate protection. This study examines the implementation of the accountability principle by personal data controllers within the banking sector. The objective is to assess how far this principle has been integrated into the obligations stipulated by data protection regulations. Using a qualitative legal research method combined with a comparative approach, this study analyzes the Personal Data Protection Law (PDPL) in Indonesia and the General Data Protection Regulation (GDPR) in Sweden. The findings reveal that Indonesia's PDPL still demonstrates several deficiencies, including limited data leakage notifications, lack of transparency in third-party data disclosure, insufficient information technology security responses, and inefficient data updates. Similarly, under the GDPR framework, challenges persist in managing data shared with third parties and in providing timely written notices in cases of data breaches. The study concludes that the weaknesses identified in both jurisdictions highlight the need for strengthening the accountability principle to enhance the effectiveness of personal data protection in the banking sector. Reinforcing this principle will ensure greater responsibility among data controllers and foster public trust in digital financial systems.

Keywords: Accountability; Bank; Data; Indonesia; Sweden;

This is an open-access article under the CC–BY 4.0 license

INTRODUCTION

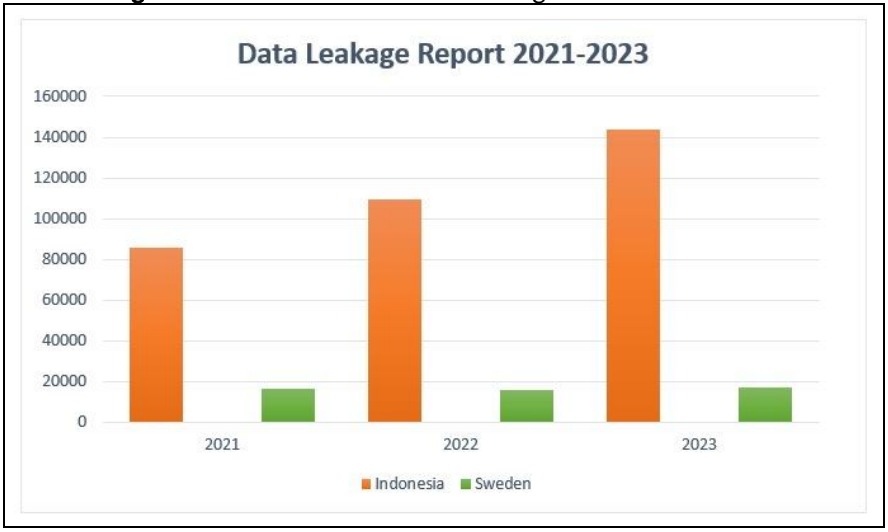
Technologies have currently become an inseparable part of daily life[1]. The quick development of technologies brings ease to human beings as users in carrying out various activities in a quick, efficient, and limitless manner[2]. Due to digitalization in all sectors, data and data analysis have become "the new oil". This is because data has a high economic value, replacing the value of oil. This technological advancement that supports all aspects of life changes human beings' patterns of social behavior. It creates significant impacts, especially in the banking sector that develops to become digital[3].

[1] Huizheng Liu and others, 'The Impact of Artificial Intelligence on Consumers' Willingness to Use CBDCs: Evidence from the Chinese Banking Sector', *Humanities and Social Sciences Communications*, 12.1 (2025) https://doi.org/10.1057/s41599-025-05067-5

[2] WenGuang Ma and others, 'Research on Credit Card Fraud Detection System Based on Federated Learning', in *Proceedings of the 2024 3rd International Conference on Frontiers of Artificial Intelligence and Machine Learning* (New York, NY, USA: ACM, 2024), pp. 242–45 https://doi.org/10.1145/3653644.3680500

[3] Mohammed Abdulrahman Kaid Zaid and others, 'The Future of Green Finance: How Digital Transformation and FinTech Drive Sustainability', *Discover Sustainability*, 6.1 (2025) https://doi.org/10.1007/s43621-025-01356-w

Figure 1. The Number of Data Leakage Cases in Indonesia



Source: From various sources, processed by the researcher

Digital development allows banks to create services to increase operational efficiency, speed up transaction processes, and provide superior services to customers[4]. In the digital era, banks will keep on innovating to fulfill customers' demands and strive to stay relevant with digitalization[5]. However, in line with the development of digital services, personal data protection becomes more crucial[6]. The Republic of Indonesia's Law No. 27 of 2022 on Personal Data Protection Law (PDPL) obliges every personal data controller, such as banks, to fulfill the obligation of protecting customers' data, especially amid the rampant cases of data leakage[7]. This research will compare personal data protection in Indonesia and Sweden. Sweden was chosen as a comparison country for three reasons. First, the similarities in the legal system used by Sweden, as Sweden uses a civil law system, the same legal system as Indonesia. Furthermore, Sweden is one of the first countries to have personal data protection regulations in the world. The third reason for choosing Sweden is that this country has an excellent level of personal data protection and a very low rate of data breaches[8]. The purpose of comparing by two country to develop a theory of implementation model of accountability in personal data law especially in banking nature[9].

Based on data from the Republic of Indonesia's Ministry of Communication and Informatics, there has been a significant increase in data leakage cases, one of the

[4] Yunjiao Zheng, 'Bank Data Protection and Fraud Identification Based on Improved Adaptive Federated Learning and WGAN', *Scientific Reports*, 15.1 (2025), 1–17 https://doi.org/10.1038/s41598-025-06807-y

[5] Istianah Zainal Asyiqin, 'Islamic Economic Law in the Digital Age: Navigating Global Challenges and Legal Adaptations', *Media Iuris*, 8.1 (2025), 95–112 https://doi.org/10.20473/mi.v8i1.61800

[6] Marta Beltrán, 'AI Algorithms under Scrutiny: GDPR, DSA, AI Act and CRA as Pillars for Algorithmic Security and Privacy in the European Union', *Computers and Security*, 158.August (2025), 104628 https://doi.org/10.1016/j.cose.2025.104628

[7] Indonesia, *Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*, *Indonesia, Pemerintah Pusat*, 2022.

[8] Peter Palm, 'Practice Briefing: Environmental, Social and Governance (ESG) and Real Estate Valuation - the Case of Sweden', *Journal of Property Investment & Finance*, 43.2 (2025), 255–64 https://doi.org/10.1108/JPIF-12-2024-0163

[9] Israel Cedillo Lazcano, 'Explainability and Operational Resilience in the Design of Central Bank Digital Currencies: A New Generation of Money-Laundering Deterrence Software', *Journal of Payments Strategy & Systems*, 18.2 (2024), 179 https://doi.org/10.69554/BDTD2604

notorious cases was when Bank Syariah Indonesia (BSI) experienced data leakage cases. This incident started off with transaction service disorders on May 2023, where a hacker group called Lock bit claimed to have stolen 1.5 TB of customers' personal data. In its development, this group has carried out extortion efforts by asking for ransom with an amount of 18 million USD to the bank[10]. When the negotiation did not reach an agreement, this sensitive data was threatened to be spread in the black market[11].

Meanwhile, in Sweden, there has also been an incident of personal data protection which happened in 2007. Nordea is one of the banking data theft cases that occurred in Sweden. This case is important to study because Sweden, as a country that has had personal data regulations since the 1970s, still experiences personal data theft that is quite a blow to IMY, a public authority responsible for enforcing GDPR and other data protection laws, monitoring data handling, and protecting individual privacy in the information society. IMY was previously known as the Swedish Data Protection Agency and was established in 1973 following the introduction of the world's first national data protection law, the Data Act. In addition, the number of personal data thefts in Sweden is very low compared to other countries. This case is very interesting to study. In this case, Nordea Swedish bank lost more than 7 million crones after cybercriminals succeeded in sending phishing emails to the bank's customers[12]. These emails contained a Trojan virus named "Haxdoor," which was disguised as anti-spam software[13]. After that software was installed, the Trojan installed a key logger in the victims' computers to record all the keys they typed, including the credentials of their bank login[14].

The criminals then directed customers to a fake website that seemed like Nordea's official website. When customers tried to log in, the hackers succeed in stealing their login information[15]. Then, they used such information to illegally access the customers' bank accounts[16]. This case, which is known as the largest online bank theft

[10] Wardah Yuspin, Kelik Wardiono, and others, 'Personal Data Protection Law in Digital Banking Governance in Indonesia', *Studia Iuridica Lublinensia*, 32.1 (2023), 99–130 https://doi.org/10.17951/sil.2023.32.1.99-130

[11] Yasser Ali Mezal and Amis Mohammed Bahgat, 'Digital Transformation and Its Impact on Banking Operations (A Study of a Sample of Private Iraqi Banks)', 2026, pp. 234–49 https://doi.org/10.1007/978-3-032-01592-1_14

[12] Cynthia Sin Tian Ho and Björn Berggren, 'The Effect of Accessibility to Bank Branches on Small- and Medium-Sized Enterprise Capital Structure: Evidence from Swedish Panel Data', *Journal of Risk and Financial Management*, 18.1 (2024), 14 https://doi.org/10.3390/jrfm18010014

[13] Tuan Thanh Nguyen and others, 'Application of a Locally Developed Open-Access Digital Monitoring System for the Human Milk Bank Network in Vietnam', *International Breastfeeding Journal* , 20.1 (2025), 1–16 https://doi.org/10.1186/s13006-025-00745-1

[14] Meenakshi Shunmugam, Satya Rajesh Kunchaparthy and Baby Kalpana, 'High Protection Bank Locker Security Alert System Using Voice Authentication Based on Wireless Sensor Network', 2023, p. 020027 https://doi.org/10.1063/5.0115687

[15] Lawrence G. Goldberg, Richard J. Sweeney and Clas G. Wihlborg, 'Evaluating the Nordea Experiment: Evidence from Market and Accounting Data', *Journal of Banking & Finance*, 31.4 (2007), 1265–86 https://doi.org/10.1016/j.jbankfin.2006.10.010

[16] Jawahitha Sarabdeen and Mohamed Mazahir Mohamed Ishak, 'A Comparative Analysis: Health Data Protection Laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)', *International Journal of Law and Management*, 67.1 (2025), 99–119 https://doi.org/10.1108/IJLMA-01-2024-0025

by McAfee, showed the effectiveness of phishing attacks in deceiving victims and stealing important data[17].

Data theft has a very severe impact on the banking sector[18]. The advancement of technologies in the banking sector makes customers vulnerable to suffering from great losses[19]. This may happen if the customer data in the form of sensitive information such as bank account numbers and credit card details are collected, processed, and misused by invalid parties[20]. Such data leakage does not only lead to the violation of data security[21]. However, it also leads to identity theft and financial abuse which will in the end damage customers' trust in banking institutions, significantly decreasing the bank's reputation[22]. Banks as one of the controllers of personal data have the absolute responsibility to process and protect the personal data of their customers, without consideration of whether it is the fault of the bank or the fault of other involved parties[23]. As a personal data controller, banks have the obligation to prevent invalid access to customer data according to stipulations PDPL[24].

Even though PDPL has been enacted, its implementation in banks still faces many obstacles. Many factors cause this lack of implementation[25]. One of the factors that causes this issue is the lack of a detailed implementing regulation as well as the absence of a special independent institution that has the job of supervision[26]. These factors become obstacles to effectively applying this law. It is crucial to conduct an analysis of how banks apply their obligations in PDPL in their operations to know whether their application is already according to the standard determined by the law[27].

[17] Kazuo TAKARAGI and others, 'Secure Revocation Features in EKYC - Privacy Protection in Central Bank Digital Currency', *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E106.A.3 (2023), 2022CIP0008 https://doi.org/10.1587/transfun.2022CIP0008

[18] Zhangyu Wang and Li Du, 'An Empirical Study on Personal Data Protection in the Banking Sector across Hong Kong, Macau, and Mainland China', *The Chinese Journal of Comparative Law*, 13 (2025) https://doi.org/10.1093/cjcl/cxae021

[19] Nurfitriyani, Siti Hamidah and Reka Dewantara, 'Analysis of Economic Law on Banking Regulation in Customer Legal Protection', *Jurnal IUS Kajian Hukum Dan Keadilan*, 9.2 (2021), 460–71 https://doi.org/10.29303/ius.v9i2.911

[20] Amjad Ghazi Al-Habashneh and others, 'Impact of the Quality of Financial and Banking Applications Used on Smartphone on the Customer Satisfaction of Jordanian Islamic Bank', *International Review of Management and Marketing* , 15.1 (2025), 99–106 https://doi.org/10.32479/irmm.17706

[21] Xin Chen, 'Privacy Protection in the Context of CBDC: Development Trends and China's Practice', *Journal of East Asia and International Law*, 16.2 (2023), 211–32 https://doi.org/10.14330/jeail.2023.16.2.01

[22] F. de Elizalde, *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, *Journal of Consumer Policy* (Springer US, 2025), XLVIII https://doi.org/10.1007/s10603-025-09584-3

[23] Fanghua Li, Jiewei Liu and Haiyue Liu, 'Institutions Empowerment for Sustainability: ESG Performance and Enterprise Green Innovation—Evidence from China', *Journal of Environmental Management*, 388 (2025), 125947 https://doi.org/10.1016/j.jenvman.2025.125947

[24] Zulkifli, Wetria Fauzi and Arya Putra Rizal Pratama, 'Pengawasan Terhadap Perlindungan Hukum Konsumen Perbankan Oleh Otoritas Jasa Keuangan Di Kota Padang', *Jurnal Hukum Bisnis Bonum Commune*, 5.1 (2022), 25–41 https://doi.org/10.30996/jhbbc.v5i1.5781

[25] Sheila Kusuma Wardani Amnesti, Siti Zulaichah and Nurul Istiqomah, 'Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective', *Legality : Jurnal Ilmiah Hukum*, 33.1 (2024), 1–19 https://doi.org/10.22219/ljih.v33i1.34623

[26] Arzu Galandarli, 'Mitigating AI Risks: A Comparative Analysis of Data Protection Impact Assessments under GDPR and KVKK', *Journal of Data Protection & Privacy*, 7.3 (2025), 252 https://doi.org/10.69554/ATTT2755

[27] Muhammad Khaeruddin Hamsin and others, 'Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection', *Al-Manahij: Jurnal Kajian Hukum Islam*, 17.1 (2023), 53–66 https://doi.org/10.24090/mnh.v17i1.7633

There are previous studies on personal data protection, especially in banking, which are relevant to this research[28]. Personal data protection compliance assessment: A privacy policy scoring approach and empirical evidence from Thailand's SMEs[29]. This study is relevant because it provides a quantitative framework for evaluating privacy policy compliance (privacy policy scoring), which I use as a reference in assessing the policy elements and transparency that financial institutions should have[30]. Bank data protection and fraud identification based on improved adaptive federated learning and WGAN[31]. This article is relevant from a technical perspective because it describes data protection mechanisms and machine learning-based fraud detection methods that can reduce the risk of customer data leakage or reconstruction[32].

Impact of the Quality of Financial and Banking Applications Used on Smartphones on Customer Satisfaction of Jordanian Islamic Bank[33]. This study is relevant because it confirms that perceived security and application quality influence customer trust and satisfaction critical factors that are compromised when data breaches occur[34]. Customer Explicit Consent Under Indonesian Open Banking Regulations[35]. This document is directly relevant to the issue of explicit consent, which is a crucial part of the accountability principle; it helps explain how consent is recorded and managed in the open banking ecosystem[36]. Financial technology and the legal protection of personal data: The case of Malaysia and Indonesia[37]. This study is relevant because it provides a comparative context for data protection regulations in Indonesia an important basis for assessing domestic banks' accountability obligations[38].

---

[28] Anežka Karpjáková, 'Protection of a Bank's Clients against Payment Frauds Based on Social Engineering', *Jusletter-IT*, 2024 https://doi.org/10.38023/f6597dc5-b5b8-4c73-ae59-1ae55d1827cf

[29] Thanwa Wathahong and others, 'Assessing Disruptive Potential of Retail Central Bank Digital Currency and Influence of Design Considerations: An Open Innovation Approach in Thailand', *Journal of Open Innovation: Technology, Market, and Complexity*, 11.1 (2025), 100502 https://doi.org/10.1016/j.joitmc.2025.100502

[30] Muhammad Ilham Mahrudin Zamzam, Rofadan Mina Arsyada and Nadya Eka Amalia Al'azza, 'The Validity of Electronic Contractual Relationships in E-Commerce and Legal Liability for Leakage of Users' Personal Data', *Jurnal Suara Hukum*, 5.2 (2023), 130–48 https://doi.org/10.26740/jsh.v5n2.p130-148

[31] Ramona Rupeika-Apoga and others, 'Regulation and Innovation in Digital Finance: The Transformation of Latvia's Banking Sector', *Digital Business*, 5.2 (2025), 100147 https://doi.org/10.1016/j.digbus.2025.100147

[32] Lilia Kurmanova and others, 'Development of Digital Services and Information Security of Banks', in *IV International Scientific and Practical Conference* (New York, NY, USA: ACM, 2021), pp. 1–6 https://doi.org/10.1145/3487757.3490911

[33] K.Krithiga Lakshmi, Himanshu Gupta and Jayanthi Ranjan, 'Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges', in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (IEEE, 2020), pp. 1028–32 https://doi.org/10.1109/ICRITO48877.2020.9197954

[34] Yang Liu and others, 'Navigating Fintech and Banking Risks: Insights from a Systematic Literature Review', *Humanities and Social Sciences Communications*, 12.1 (2025), 1–16 https://doi.org/10.1057/s41599-025-05055-9

[35] Ali Vafaei-Zadeh and others, 'Cybersecurity Awareness and Fear of Cyberattacks among Online Banking Users in Malaysia', *International Journal of Bank Marketing*, 43.3 (2025), 476–505 https://doi.org/10.1108/IJBM-03-2024-0138

[36] Hao Wu, Norzieiriani Ahmad and Nazlina Zakaria, 'Green Banking Initiatives: The Role of CSR in Aligning with the SDGs and Shaping Sustainable Consumer Choices', *Acta Psychologica*, 258 (2025), 105195 https://doi.org/10.1016/j.actpsy.2025.105195

[37] Nurhasanah Nurhasanah and Indra Rahmatullah, 'Financial Technology and the Legal Protection of Personal Data: The Case of Malaysia and Indonesia', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 20.2 (2020), 197–214 https://doi.org/10.30631/alrisalah.v20i2.602

[38] Wardah Yuspin, Alda Oktalivia Putri, and others, 'Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities', *International Journal of Safety and Security Engineering*, 14.6 (2024), 1699–1706 https://doi.org/10.18280/ijsse.140605

The difference between that previous research with this research are This research adds concrete case evidence of breaches in Indonesia and Sweden, demonstrating the gap between legal provisions (statutory text) and banks' institutional practices. I also offer concrete sectoral recommendations to improve accountability. Apart from that, in this paper, the authors will also analyze the application of personal data security which is the main job of data controllers in Sweden through the GDPR as a model[39]. This is to provide a good perspective on what the role of data controllers in Indonesia should be like in protecting personal data so that it may effectively be carried out.

METHOD

This study adopts a qualitative legal research approach that emphasizes doctrinal and normative analysis to examine the implementation of personal data protection obligations within banking institutions. The research employs a descriptive–analytical method to provide a comprehensive understanding of banks' responsibilities as personal data controllers under the Personal Data Protection Law (PDPL) and the General Data Protection Regulation (GDPR) frameworks. A multiple case study design was utilized to compare the regulatory and institutional practices of selected banking institutions in implementing personal data protection standards. The qualitative and doctrinal approach is appropriate for this research because it allows an in-depth exploration of legal norms, policy frameworks, and compliance mechanisms related to data protection[40]. Qualitative case study methods are particularly effective for understanding complex regulatory settings and institutional behaviors within their real-life legal context [41] [42]. This approach enables the integration of statutory interpretation and empirical observation of regulatory practices, thereby addressing the research objective of assessing how PDPL and GDPR principles are operationalized within the banking sector[43].

Data were collected entirely through documentary research, focusing on primary and secondary legal materials. Primary sources included statutory instruments (PDPL, GDPR, and related implementing regulations), regulatory circulars issued by supervisory authorities, and institutional compliance documents publicly available from banks' annual and sustainability reports [44]. Secondary sources comprised academic journal articles, legal commentaries, books, and official reports discussing the implementation and challenges of personal data governance in the financial sector [45]. Data analysis was conducted through qualitative content analysis and

[39] Karol Schulz, Vincent Karovič and Peter Veselý, 'Options to Improve the General Model of Security Management in Private Bank with GDPR Compliance', 2021, pp. 343–70 https://doi.org/10.1007/978-3-030-62151-3_8

[40] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research', *Deakin Law Review*, 17.1 (2012), 83 https://doi.org/10.21153/dlr2012vol17no1art70

[41] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2018.

[42] R. K. Yin, *Case Study Research: Design and Methods (5th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2014.

[43] C. N. Creswell, J. W., & Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2018.

[44] U. Flick, *An Introduction to Qualitative Research (6th Ed.). London: SAGE Publications.*, 2018.

[45] T. Hutchinson, *Doctrinal Research: Researching the Jury and Legal Methodology. In M. McConville & W. H. Chui (Eds.), Research Methods for Law (2nd Ed., Pp. 7–31). Edinburgh University Press. Hutchinson, T. (2018). Doctrinal Research: Researching the Jury and Legal Metho*, 2018.

normative legal interpretation[46]. The process involved several stages: Compilation of relevant legal and institutional documents; Systematic coding of provisions, principles, and compliance measures related to data protection obligations; Thematic categorization of findings based on recurring issues such as data subject rights, lawful processing, consent mechanisms, and supervisory oversight; Comparative analysis of PDPL and GDPR to identify areas of convergence, divergence, and implications for banking compliance.

RESULT AND DISCUSSION

The PDPL is the regulatory basis for personal data protection in Indonesia[47]. As a footstep and a legal basis for the personal data protection practice, it contains several principles of personal data protection that must be fulfilled in all forms of personal data processing[48]. The PDPL regulates that there are some personal data protection principles that must be complied with in all personal data processing activities[49]. The first principles that the parties that conduct personal data processing must pay attention to are validity, justice, and transparency[50]. This means that data processing must be conducted in a clear and careful manner[51]. Personal data owners must provide their agreement to have their data processed[52]. Apart from these principles, this law also determines that the accountability principle is used as one of the methods to maintain the responsibility of personal data controllers as the party that keeps personal data subjects' personal data[53].

This accountability principle regulates that organizations must be responsible for personal data processing[54]. This principle encourages organizations to adopt accountable practices, creating an environment where the compliance to regulations becomes a priority[55]. With this accountability principle, data controllers are responsible for the security of the personal data under their control[56]. Thus, the usage

[46] M. Schreier, *Qualitative Content Analysis in Practice. London: SAGE Publications.*, 2012.
[47] Moh Hamzah Hisbulloh, 'Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi', *Jurnal Hukum Unissula*, 37.2 (2021), 119–33 https://doi.org/10.26532/jh.v37i2.16272
[48] Paul Kariuki, Lizzy Oluwatoyin Ofusori and Maria Lauda Joel Goyayi, 'Internet of Things on Banking Processes in South Africa: A Systematic Reflection on Innovations, Opportunities and Challenges', *Digital Business*, 5.1 (2025), 100097 https://doi.org/10.1016/j.digbus.2024.100097
[49] Carlos Goettenauer, 'The Brazilian Financial System, Cyber Security Policy and Personal Data Protection', *Law, State and Telecommunications Review*, 12.2 (2020), 172–86 https://doi.org/10.26512/lstr.v12i2.34716
[50] Harun R Khan, 'Banking Sector Banking Sector', 2014, 1–15.
[51] Intan Audia Priskarini, Pranoto and Kukuh Tejomurti, 'The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia', *Padjadjaran Jurnal Ilmu Hukum*, 6.3 (2019), 556–75 https://doi.org/10.22304/pjih.v6n3.a7
[52] Martin Zahariev and others, 'KEY TAKEAWAYS From The Most Significant GDPR Personal Data Breaches In The Republic Of Bulgaria', *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, 5 (2025), 353–61 https://doi.org/10.17770/etr2025vol5.8482
[53] Supeno Supeno, Rosmidah Rosmidah and Syed Mohd Uzair Iqbal, 'Personal Data Protection in Review of Legal Theories and Principles', *Journal of Law and Legal Reform*, 6.3 (2025), 1349–76 https://doi.org/10.15294/jllr.v6i3.10252
[54] Avtar Singh and Amira Omer Ali, 'Protecting What Matters: Data Privacy Solutions for Qatar's Expanding Mobile Banking Sector', *Journal of Data Protection & Privacy*, 8.1 (2025), 24 https://doi.org/10.69554/MVIY7029
[55] Ine Van Zeeland and Jo Pierson, 'Data Protection Risks in Transitional Times: The Case of European Retail Banks', in *Data Protection and Privacy, Volume 15* (Hart Publishing, 2023) https://doi.org/10.5040/9781509965939.ch-001
[56] Atin Meriati Isnaeni, 'Premi Payment of the "Banker"S Clause Insurance in a Credit Agreement (Review of Deed of Credit Agreement Pt. Bank Danamon Mataram)', *Jurnal IUS Kajian Hukum Dan Keadilan*, 9.3 (2021), 682–96 https://doi.org/10.29303/ius.v9i3.978

and security of every data processing activity can be taken accountability for[57]. The accountability principle is also regulated in the Personal Data Protection Law that applies in Europe. This regulation aims to protect the personal data and privacy of individuals, as well as minimize the spread of data without permission. This regulation has become a guideline for many countries of the world and has extra-territorial effects. It applies to all parties, even outside of the European Union. The GDPR contains personal data processing principles that are then adopted into the PDPL, including the principles of lawfulness, fairness, transparency, and accountability[58].

The accountability principle is the core of personal data protection, as stipulated in Article 5 of the GDPR. Personal data controllers have the obligation to be responsible and show compliance towards the six other principles of data protection[59]. This means that accountability influences and guarantees the fulfillment of all personal data protection principles[60]. Therefore, as a referential regulation of Indonesia's PDPL, GDPR principles are integrated into articles of the PDPL[61]. This research focuses on the accountability principle that is contained in the GDPR and that is adopted into the Indonesian PDP Law[62]. The accountability principle guarantees that personal data controllers must fulfill other principles of personal data protection[63]. They must have the ability to show compliance to the owner of the processed data.

The accountability principle supposed provide better legal certainty and protection for personal data protection in Indonesia. Personal data controllers have full responsibility towards the processing of personal data. They must have the capability to prove their compliance towards personal data principles. This includes legal accountability and compliance with ethical codes[64]. They must make sure that the data are processed in a just manner based on the agreement of data subjects and their best interests. Data controllers are individuals or organizations that have the responsibility of holistically determining the goal and method of personal data processing. Personal data protection means all efforts to protect personal data in a series of personal data processing activities to guarantee the constitutional rights of personal data subjects. This shows that personal data controllers have the obligation to conduct personal data protection. They have the right to collect personal data

[57] Ali Farzanehfar, Florimond Houssiau and Yves-Alexandre de Montjoye, 'The Risk of Re-Identification Remains High Even in Country-Scale Location Datasets', *Patterns*, 2.3 (2021), 100204 https://doi.org/10.1016/j.patter.2021.100204

[58] Farzanehfar, Houssiau and de Montjoye.

[59] Mercurius Broto Legowo, Fangky Antoneus Sorongan and Steph Subanidja, 'Risk Management of Bank and FinTech Collaboration: A Phenomenological Research', in *2023 6th International Conference of Computer and Informatics Engineering (IC2IE)* (IEEE, 2023), pp. 94–100 https://doi.org/10.1109/IC2IE60547.2023.10331156

[60] Anoosh Mohammadzadeh and others, 'Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks', *Biopreservation and Biobanking*, 23.3 (2025), 177–85 https://doi.org/10.1089/bio.2024.0086

[61] Erman I. Rahim and others, 'Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations', *Journal of Law and Legal Reform*, 6.3 (2025), 1305–48 https://doi.org/10.15294/jllr.v6i3.12942

[62] Wilma Laura Sahetapy, 'Perlindungan Data Pribadi Anak Dalam E-Commerce Di Masa Pandemi Covid-19', *Jurnal Hukum Bisnis Bonum Commune*, 4.2 (2021), 214–25 https://doi.org/10.30996/jhbbc.v4i2.5319

[63] Tapiwa V Warikandwa, 'Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared', *Potchefstroom Electronic Law Journal*, 24 (2021), 1–32 https://doi.org/10.17159/1727-3781/2021/v24i0a10727

[64] Dwi Edi Wibowo, 'Penerapan Konsep Utilitarianisme Untuk Mewujudkan Perlindungan Konsumen Yang Berkeadilan Kajian Peraturan Otoritas Jasa Keuangan Nomor: 1/Pojk.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan', *Syariah: Jurnal Hukum Dan Pemikiran*, 19.1 (2019), 15–30 https://doi.org/10.18592/sy.v19i1.2296

with the aim of collecting clear and valid data according to the agreement of the related individual[65]. Banks are personal data controllers that have the responsibility to determine the goal of processing their customers' personal data. In this case, banks have control over the personal data. They have the obligation to implement the protection of their customers' personal data that were collected and processed to provide services that their customers may access[66].

The obligations of personal data controllers are regulated in Article 20 to Article 54 of law. This regulation may be understood as an implementation of the concept or theory of the privacy dimension. Therefore, the obligations regulated in these regulations are strongly linked to the individual rights of personal data subjects in controlling information (personal data) as well as accessing their data [67]. Data controllers have the obligation to provide information related to the legality of personal data processing, the objective of that processing, the type and relevance of the data that will be processed, as well as the storage period of documents containing personal data. Apart from that, the delivered information must also encompass details on the collected data, the duration of personal data processing, and the rights of processing subjects. Further, personal data controllers must inform the related individuals as personal data subjects before changes in information[68]. Personal data controllers have the obligation to process personal data in a limited, specific, legally valid, and transparent manner. In other words, personal data controllers are legally obligated to apply the accountability principle in processing personal data. Apart from that, personal data controllers have the obligation to process personal data[69].

Another obligation related to personal data processing for personal data controllers is the obligation to carry out validation of the risks of personal data protection if the data processing has the potential to lead to high risks for personal data subjects[70]. Personal data controllers must carry out measurable and reliable assessments. This includes personal data controllers' obligation to protect and guarantee the security of the personal data they process. This protection may be carried out by designing and implementing operational technical steps to prevent the processing of personal data that violates legal stipulations[71]. Apart from that, personal

[65] Oktaria Wim Kusuma and Abraham Ferry Rosando, 'Urgensi Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online', *Jurnal Hukum Bisnis Bonum Commune*, 5.1 (2022), 123–41 https://doi.org/10.30996/jhbbc.v5i1.6087

[66] Neha Garg and Kapil Gupta, 'Data Privacy in Online Banking Using Blowfish Algorithm: A Review', in *Progressive Computational Intelligence, Information Technology and Networking* (London: CRC Press, 2025), pp. 888–91 https://doi.org/10.1201/9781003650010-145

[67] Ali Alibeigi, Abu Bakar Munir and Adeleh Asemi, 'Compliance with Malaysian Personal Data Protection Act 2010 by Banking and Financial Institutions, a Legal Survey on Privacy Policies', *International Review of Law, Computers & Technology*, 35.3 (2021), 365–94 https://doi.org/10.1080/13600869.2021.1970936

[68] Ebrahim Mohammed Alrawhani and others, 'Integrating Information Security Culture and Protection Motivation to Enhance Compliance with Information Security Policies in Banking: Evidence from PLS-SEM and FsQCA', *International Journal of Human–Computer Interaction*, 2025, 1–22 https://doi.org/10.1080/10447318.2025.2464900

[69] Tamer Bani Amer and Mohammad Ibrahim Ahmed Al-Omar, 'The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector', *International Journal of Advanced Computer Science and Applications*, 14.8 (2023) https://doi.org/10.14569/IJACSA.2023.0140841

[70] Cao Dinh Lanh Cao, 'Legal Framework for Banking Activities in Digital Enviroment. A Case Study of Vietnam', *PRAWO i WIĘŹ*, 53.6 (2025) https://doi.org/10.36128/PRIW.VI53.950

[71] Diego André Cerqueira and others, *Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law*, *Empirical Software Engineering* (Springer US, 2025), xxx https://doi.org/10.1007/s10664-025-10681-7

data controllers must also determine the level of security that is in line with the characteristics and risks of the processed personal data. In this case, personal data controllers must prevent invalid access to personal data by applying a reliable, safe, and responsible security system, both in the manual processing and through the electronic system according to the stipulations of applicable legal regulations[72].

In case of failure in personal data protection, personal data controllers have the obligation to give a written notice to related personal data subjects or institutions[73]. This notice must encompass information on the disclosed personal data, the time and method of that data disclosure, as well as the steps that personal data controllers have taken in handling and recovering the condition after the disclosure of that data[74]. Meanwhile, according to the GDPR, personal data controllers refer to individuals, legal entities, public authorities, or other organizations that individually or with other parties collectively determine the goals and methods of personal data protection[75]. According to the GDPR, personal data controllers have the obligation to give information that must be delivered to data subjects during the data collection. This is clearly determined in the GDPR[76].

Data controllers and processors also have the obligation to take correct technical and organizational steps to consider the development of current technologies, implementation fees, as well as processing characteristics, scope, context, and objective, including the varied risk levels to individual rights and freedom. The GDPR provides some specific suggestions on security actions that may be deemed according to the risk[77]. Concerning the application of the accountability principle, there is a very famous case related to a personal data controller, namely Meta Platform Inc, in which at that time still be Facebook Inc. As a personal data controller, this company has been proven to have committed a violation in processing the personal data of this application's users. The Personal Data Commission of Ireland, which is the main privacy supervisor for Facebook in the European Union, has imposed fines after the parent company of Facebook has been proven to fail to follow the tight regulations to secure the things that are protected by the GDPR. This case started when Facebook experienced data leakage which went viral in 2021[78].

---

[72] M. N. Dudin and S. V. Shkodinsky, 'Challenges and Threats of the Digital Economy to the Sustainability of the National Banking System', *Finance: Theory and Practice*, 26.6 (2022), 52–71 https://doi.org/10.26794/2587-5671-2022-26-6-52-71

[73] Omar Haggag and others, 'An Analysis of Privacy Regulations and User Concerns of Finance Mobile Applications', *Information and Software Technology*, 184 (2025), 107756 https://doi.org/10.1016/j.infsof.2025.107756

[74] Avishek Kumar and Tyson Silver, 'Know, Grow, and Protect Net Worth: Using ML for Asset Protection by Preventing Overdraft Fees', in *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (New York, NY, USA: ACM, 2024), pp. 5272–82 https://doi.org/10.1145/3637528.3671628

[75] Marius Laurinaitis, Darius Štitilis and Egidijus Verenius, 'Implementation of the Personal Data Minimization Principle in Financial Institutions: Lithuania's Case', *Journal of Money Laundering Control*, 24.4 (2021), 664–80 https://doi.org/10.1108/JMLC-11-2020-0128

[76] Silvia Gioiosa and others, 'A GDPR-Compliant Solution for Analysis of Large-Scale Genomics Datasets on HPC Cloud Infrastructure', *Journal of Big Data*, 12.1 (2025) https://doi.org/10.1186/s40537-024-01047-9

[77] Vasudha Khanna and Atul Kotwal, 'Examining the Significance of the Digital Personal Data Protection Act, 2023 in the Context of the Healthcare Industry: A Comprehensive Analysis', *Discover Public Health*, 22.1 (2025), 1–13 https://doi.org/10.1186/s12982-025-00757-6

[78] Foo Nin Ho, Nga Ho-Dac and J. Sonia Huang, 'The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence', *Sage Open*, 13.3 (2023) https://doi.org/10.1177/21582440231181395

A user in a hacker forum published 533 million data of Facebook users in April 2021. These data were not results of breaching, but rather a result of scrapping. Scrapping means that these data were already available in Facebook's system and the perpetrator only needed to collect it. Digital data supervisors in Europe have a very strong position after the GDPR was enacted in May 2018. One of its authorities is to impose sanctions of up to 4% of a company's annual income. The most severe punishment imposed under GDPR so far was a record of fines reaching 746 million euros for Amazon by its main privacy supervisor in Luxembourg, followed by fines with the amount of 405 million euros for Instagram Meta[79]. Meanwhile, data leakage cases especially in banking industries in Indonesia have happened several times. The most severe case happened in 2023 when there was a theft of customer and employee data of BSI, which is the largest Sharia bank in Indonesia through ransomwarey. In this case, 1.5 TB of customers' personal data were stolen[80].

Table 1: Comparative Analysis of the Implementation of Personal Data Protection under the GDPR and the PDPL

Indicators	GDPR	PDPL
Law Enforcement	Carried out by Data Protection Authorities/DPA in each EU member state, which is then coordinated by the European Data Protection Board/EDPB to ensure consistent implementation. In Sweden, law enforcement is carried out by the Swedish Data Protection Authority (Integritetsskyddsmyndigheten) or known as IMY.	Indonesia does not have Personal Data Supervisor yet and before the establishment of the agency, the temporary personal data supervisory agency was still under the Ministry of Communication and Digital Affairs through the Directorate General of Digital Space Supervision.
The Authority of the personal data protection agency	In addition to having the authority to conduct supervision, this institution also has very broad authority, including conducting investigations and even imposing sanctions on organizations that violate the law.	The authority of the personal data supervisor in Indonesia can also impose sanctions, but this has not yet been tested because no sanctions have ever been imposed so far on personal data violators.
Forms of sanctions	GDPR violations are subject to administrative fines of up to €20 million or 4% of annual global turnover, whichever is higher, and other sanctions such as corrective measures by the supervisory authority. Lighter fines of up to €10 million or 2% of global turnover may be imposed for less serious violations. These fines are very heavy and can have a deterrent effect on personal data violators. Meanwhile, the GDPR does not provide for criminal sanctions as it focuses on administrative fines. However, it is possible for each country to impose criminal sanctions under their respective national laws. In Meta case the GDPR carries very severe penalties, particularly administrative fines. These severe penalties serve as a deterrent for those who attempt to violate personal data protection.	PDPL have administrative sanctions (warnings, suspension of data processing, data deletion, and fines of up to 2% of annual revenue) and criminal sanctions (4-6 years imprisonment and/or fines of billions of rupiah). For corporations, the fines can be 10 times the original criminal sanctions, and can even include confiscation of profits or dissolution of the business. The fines imposed are much lighter than those under the GDPR, so they do not have a deterrent effect. In the BSI case, no party was even subject to such sanctions. The advantage of this legal regulation compared to the GDPR is that there are criminal sanctions for violators of personal data protection, so the sanctions are more comprehensive.

[79] Nico Foecking, Mei Wang and Toan Luu Duc Huynh, 'How Do Investors React to the Data Breaches News? Empirical Evidence from Facebook Inc. during the Years 2016–2019', *Technology in Society*, 67 (2021), 101717 https://doi.org/10.1016/j.techsoc.2021.101717

[80] BSI, *EKSPANSI DAN AKSELERASI BISNIS UNTUK PERTUMBUHAN BERKELANJUTAN*, *Laporan Tahunan BSI 2023*, 2023.

The Response of personal data supervisor in every violation	The response from the personal data supervisory agency is considered to be quite fast because every violation must be reported immediately so that it can be responded to by the competent authorities. Therefore, it is necessary for the personal data supervisory agency in Indonesia to learn about the duties and sanctions of the GDPR.	The response of the personal data supervisory agency is considered unresponsive because there has never been any legal action taken in cases of large-scale personal data theft. This may be due to the fact that a personal data supervisory agency has not yet been established. Due to the absence of derivative regulations and a supervisory agency, the sanctions under the PDPL cannot be fully and effectively implemented.
The accountability principle of data controller	The data protection supervisor is an advisor and compliance supervisor appointed to ensure that controllers and processors of personal data comply with data protection laws and protect the rights of data subjects. And in this accountability principles have been effectively implemented in this GDPR model since the Data Supervisor has accomplished their responsibility.	Meanwhile, the implementation of accountability principles for data controllers in the PDPL model has not been effective due to the absence of an independent data supervisor tasked with overseeing the duties of data controllers.

Source: From various sources, processed by the researcher

The PDPL comprehensively regulates the obligation of data controllers, this regulation is a concrete manifestation of the privacy dimension theory, which guarantees individual rights to control and access their personal information. These articles emphasize that personal data protection is not a mere procedural thing. However, it has a substantial value in guaranteeing the security and sovereignty of each individual's personal information. For banks as data controllers, this means implementing some comprehensive obligations in processing customers' data by paying attention to legal, security, and ethical aspects. In its implementation, the obligation of personal data controllers (such as banks) must carry out, such as The Obligation to Give Information to Personal Data Subjects. Personal data controllers have the obligation to give information related to the legality of personal data processing, the goal of that processing, the type and relevance of the data that will be processed, as well as the storage period of documents containing personal data[81]. Apart from that, the delivered information must also encompass details of the collected data, the duration of personal data processing, as well as the rights that personal data owners have. Further, personal data controllers must inform the related individual as personal data subjects before changes in information.

Based on bank privacy and policies, the data collected by banks include information such as full name, gender, identification (ID) number or other identity documents, place and date of birth, address of residence, and taxpayers' ID number. Apart from that, they also collect other data including the names of customers' biological mothers, specimens of signatures, phone or mobile phone numbers, email addresses, and passwords[82]. They may also collect customers' biometric information, such as voice recordings, videos, or other data that are related to customers' interactions with banks. Banks may also collect other recorded data, including work experiences, financial information, risk profiles, investments, experiences, knowledge,

[81] Dennis Heitmann and others, 'The Impact of Central Bank Digital Currencies on the Financial Stability of Banks: Dynamic Panel Estimation', *Finance Research Letters*, 84.April (2025), 107791 https://doi.org/10.1016/j.frl.2025.107791

[82] Zhilong Guo, 'Criminalisation of the Illegal Use of Personal Data: Comparative Approaches and the Chinese Choice', *Humanities and Social Sciences Communications*, 12.1 (2025), 1–16 https://doi.org/10.1057/s41599-025-05141-y

business interests, as well as their assets[83]. Internet protocol address (IP Address), profile activities in widgets, as well as the information that customers provide to recover their accounts, such as answers to security questions, are also part of the collected data. Then, additional data encompassing cellular device identifiers, such as device ID, advertisement ID, media access control address, or international mobile equipment identity, as well as device information encompassing device name, operation system, type, and browser language[84]. Data to prevent fraud, such as reports on the misuse of the refund features or fake click activities on advertisements are also processed.

Another Obligation to Guarantee Personal Data Accuracy, In practice, banks' development of the verification mechanism reflects the implementation of the obligation to guarantee personal data accuracy. Banks apply a mechanism of customer data verification that guarantees the accuracy and accordance with data from the Department of Population and Civil Registry. If the data of the customer that used the bank application are not according to the records of this service, the system will automatically stop the process until the customer updates their data[85].

Personal data controllers have the obligation to update and/or fix errors or inaccuracies in personal data. The update or improvement processes must be completed at most in 3x24 hours after the acceptance of that personal data subject's request. After the improvement or update is carried out, personal data controllers must deliver the results to the related personal data subject[86]. Banks apply procedures that combine conventional approaches with personal data protection principles. The data-changing processes are carried out through mechanisms that require customers to directly come to the Customer Service (CS) section. For instance, when customers wish to change their ID numbers, banks have systematic procedures to accurately and correctly update customers' data[87]. The direct coming to the CS section may be perceived as an effort to guarantee the validity of the data change. It is deemed more effective than digital methods that are prone to the potential of identity forgery. However, this approach also has disadvantages, such as the potential of limited access for customers who live far away from branch offices or those who have time restrictions. To increase efficiency, banks may consider creating a combination of the face-to-face method with secure digital technologies to fulfill customers' needs without violating the principle of personal data protection[88].

[83] Marie Fréminville, *Cybersecurity and Decision Makers* (Wiley, 2020) https://doi.org/10.1002/9781119720362
[84] Kaushan Dutta and others, 'Crime Analysis and Management System', *SN Computer Science*, 6.7 (2025), 799 https://doi.org/10.1007/s42979-025-04319-0
[85] Mandira Sarma, 'Financial Digitalization in India', *Eurasian Economic Review*, 15.2 (2025), 401–24 https://doi.org/10.1007/s40822-024-00298-4
[86] Xin Liu, Jiaqi Wu and Chenghu Zhang, 'Antecedents of Consumers' Acceptance of Central Bank Digital Currency: The Role of Technology Perceptions, Social Influence and Personal Traits', *Technological Forecasting and Social Change*, 217 (2025), 124192 https://doi.org/10.1016/j.techfore.2025.124192
[87] Austin Landini and Russell Spears, 'Banks Approved Fraudulent Loans to Capture Origination Fees: Evidence from the Paycheck Protection Program', *Journal of Financial Crime*, 32.4 (2025), 763–75 https://doi.org/10.1108/JFC-07-2024-0201
[88] Ashwini L, R Poornima Lakshmi and S Pavithra, 'Cybersecurity in Banking and Cloud Computing: Threats, Defenses, and Innovations', in *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (IEEE, 2025), pp. 1–6 https://doi.org/10.1109/ICDSAAI65575.2025.11011646

Personal data controllers have the obligation to protect and guarantee the security of the personal data they process through the application of operational technical steps to prevent the processing of personal data that violate legal stipulations. Apart from that, data controllers also have the obligation to determine the level of security that is in line with the characteristics and risks of the processed personal data. In this case, personal data controllers must prevent invalid access to personal data by applying a reliable, secure, and responsible security system, both in manual processing and through the electronic system according to the stipulations of applicable legal regulations[89]. Based on policies on privacy, banks can only disclose customers' personal data to third parties under certain conditions that are permitted by the law. This disclosure is only carried out for legal interests, to increase services, to collaborate with partners in providing certain services, as well as to market or offer banks' products and services. In each of these disclosures, banks oblige partners or third parties to maintain data security, limit its use only to the objectives that have been agreed upon, and guarantee accordance with customers' agreement[90].

The granting of third parties' access to third parties is carried out with the main goal of offering certain products. The disclosed personal data are only limited to information such as names and work locations of customers. This aims to make sure that the personal data is used in a relevant manner that does not exceed the agreed-upon objective[91]. Based on privacy policies, banks have carried out their obligations to protect and guarantee personal data security that is processed through the application of technical operational steps to prevent the processing of personal data that violates legal stipulations. However, its explanation does not explicitly explain the data disclosure to third parties that is carried out with the valid and explicit agreement from personal data subjects for one or more specific goals. Even though banks disclose personal data to third parties with product marketing or offering objectives, it must still be carried out with a valid and explicit agreement from data subjects. Banks must make sure that the agreement is given clearly for every disclosure objective to maintain the trust of customers and prevent the violation of privacy rights[92].

Banks have applied the customer personal data categorization system based on three levels of security risk, namely low, medium, and high, based on the background and biodata profile of customers. This system aims to make sure that the data protection is according to the level of existing risk, so that in its management, more sensitive data may obtain special attention[93]. Banks have carried out the obligation to determine the level of security that is according to the characteristics and risks of the

[89] Ebrahim Mohammed Alrawhani, Awanis Romli and Mohammed A. Al-Sharafi, 'Evaluating the Role of Protection Motivation Theory in Information Security Policy Compliance: Insights from the Banking Sector Using PLS-SEM Approach', *Journal of Open Innovation: Technology, Market, and Complexity*, 11.1 (2025), 100463 https://doi.org/10.1016/j.joitmc.2024.100463

[90] Ana Maria Barbosa Casolaro, Gabriela Nogueira Rauber and Ursula Silveira Monteiro de Lima, 'Open Banking: A Systematic Literature Review', *Journal of Banking Regulation*, 26.3 (2025), 340–55 https://doi.org/10.1057/s41261-024-00262-x

[91] Pradeep Chintale and others, 'Weighted Extreme Gradient Boosting Based Cybersecurity Risk Assessment in Investment Banking and Financial Sector', 2026, pp. 249–60 https://doi.org/10.1007/978-3-032-00793-3_20

[92] Nadiah Tsamara, 'Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara', *Jurnal Suara Hukum*, 3.1 (2021), 53–85 https://doi.org/10.26740/jsh.v3n1.p53-84

[93] Thiago Felipe and others, 'Digital Transformation in Commercial Banks: Unraveling the Flow of Industry 4.0', *Digital Business*, 5.2 (2025), 100129 https://doi.org/10.1016/j.digbus.2025.100129

processed personal data. By dividing data into the low, medium, and high categories, banks may accurately allocate security resources to protect more sensitive data, such as financial and identity information, from more serious threats. Therefore, this categorization system may increase customers' trust and make sure that personal data management is carried out with high accountability[94].

Then, based on banks' annual reports, banks have also implemented various cybersecurity strategies to guarantee the protection of customers' data. Most banks have formed the Chief Security Officer Office Group (CSO) work unit that has the role of the center of cyber data security management. The CSO has the role of maintaining the confidentiality of customers' data, protecting the data from the potential of cyberattacks, as well as guaranteeing that the security system runs optimally[95]. The CSO has a crucial role in maintaining the data security as a whole. Banks disclose that they apply a layered security system. Thus, in case of the potential of data leakage, banks can immediately take mitigation steps that are required to decrease that risk[96].

Further, based on the annual report, it was found that most banks also use a multi-layer defense system, encompassing server-level security (R1), endpoint-level security (R3), and perimeter-level security, up to application-level security. Banks also apply technologies such as SSL 128-bit and customer-level encryptions to protect the communication between customers and servers[97]. The annual report from a bank also showed that banks have carried out the obligation to prevent invalid access to personal data by applying a reliable, safe, and accountable security system, both in manual processing and through electronic systems. The formation of the CSO, multi-layer defense systems, and encryption technologies reflect a strong commitment to protecting customers' personal data from the potential of cyber threats. Apart from that, the multi-layer defense which encompasses multi-level security starting from the server to the application shows banks' holistic approach to preventing invalid access to personal data. However, banks still need to carry out sustainable evaluations to increase the effectiveness of the applied security system, considering cyber threats keep on developing and personal data protection must always be maintained[98].

A CSO is a body that must be owned by a large-scale bank to protect the bank from online financial vulnerabilities. Therefore, at BSI Bank, the CSO is a body that already exists as part of the bank's structure. However, despite the existence of a CSO, the role of the CSO has not been very effective in protecting personal data security, as seen in the recent ransomware incident. This is because the role of data controller in each bank should be controlled and supervised by a personal data supervisory agency,

[94] Stanisław Barański, Julian Szymański and Higinio Mora, 'Anonymous Provision of Privacy-Sensitive Services Using Blockchain and Decentralised Storage', *International Journal of Information Security*, 24.3 (2025), 130 https://doi.org/10.1007/s10207-025-01052-w

[95] Nir Kossovsky, *Reputation, Stock Price, and You* (Berkeley, CA: Apress, 2012) https://doi.org/10.1007/978-1-4302-4891-0

[96] Noemí Oeding and Kara Newby, 'The Social Enterprise Craze: CSO Financial Sustainability in Ghana', *Nonprofit Policy Forum*, 16.1 (2025), 55–78 https://doi.org/10.1515/npf-2022-0035

[97] Sebastian Kokot, 'Comparative Evaluation of Public Data Sets on Average House Prices in Poland', *Folia Oeconomica Stetinensia*, 25.1 (2025), 157–79 https://doi.org/10.2478/foli-2025-0008

[98] Moh. Adenan and others, 'The Effects of Macroprudential Policies on the Performance of Conventional Banks in Indonesia', *ECONOMICS*, 13.1 (2025), 369–86 https://doi.org/10.2478/eoik-2025-0012

which has not yet been established[99]. Then, the *Otoritas Jasa Keuangan* (OJK) as Financial Service Authority (FSA) periodically carries out data sampling in banks to guarantee compliance with regulations. This sampling involves the checking of customers' data that are randomly chosen to have them verified in accordance with banks' manual procedures. For example, the FSA directly comes to the branch and checks the data of certain customers. They even carry out direct confirmation to those customers to check the data correctness. Banks have run according to regulations. This has become an effective form of external supervision[100].

Another obligation to be fulfilled is obligation to supervise third parties who processed data from bank's clients. Personal data controllers also have the obligation to supervise third parties that is involved in the processing of the personal data that are under their control. Apart from that, personal data controllers must also guarantee the protection of personal data from invalid or illegal processing methods[101]. Banks conduct daily supervision of third parties that accept access to personal data. Banks request updates regarding the results of that data usage to make sure that the data are only used according to the aim of the cooperation. Regarding the potential for violation, such as invalid access by other parties that do not cooperate with banks, such incidents are deemed criminal violations against customers' data. It must also be emphasized that banks have a full responsibility to maintain the confidentiality of customers' personal data[102].

In case of the failure to protect personal data, banks are obliged to send notifications to its clientele. In the event of the failure to protect personal data, bank have the obligation to give a written notice to related personal data subjects or institutions. This notice must encompass information on the disclosed personal data, the time and method of that data disclosure, as well as the steps that personal data controllers have taken in handling and recovering the condition after the disclosure of that data[103]. Banks still do not have a special notification system to inform customers about data leakage incidents. So far, the notifications given to customers are only limited to financial transactions, such as cash withdrawals, transfers, or deposits through the SMS (short message service) notification system[104]. Banks as data controllers have strived to fulfill most of their obligations as personal data controllers based on PDPL. However, there are still some obligations that banks have not succeeded in fully implementing or fulfilling[105].

[99] Oeding and Newby.
[100] Marsellisa Nindito and others, 'Guardians of Integrity: Exploring the Role of Corporate Governance in Preventing Financial Statement Fraud', *Journal of Governance and Regulation*, 14.1 (2025), 109–18 https://doi.org/10.22495/jgrv14i1art10
[101] Orima Davey and others, 'GREEN BONDS IN INDONESIA: SYNERGY BETWEEN BANK INDONESIA AND OTORITAS JASA KEUANGAN'S COMMITMENT', *Journal of Central Banking Law and Institutions*, 2.2 (2023), 199–220 https://doi.org/10.21098/jcli.v2i2.37
[102] Fabian Jonathan, Fajar Sugianto and Tomy Michael, 'Comparative Legal Analysis on the Competence Of The Indonesia's Financial Services Authority And Monetary Authority Of Singapore On The Enforcement Of Insider Trading Laws', *Journal of Central Banking Law and Institutions*, 2.2 (2023), 283–300 https://doi.org/10.21098/jcli.v2i2.24
[103] Fabian Jonathan, Fajar Sugianto and Michael.
[104] Wardah Yuspin and Ata Fauzie, 'Good Corporate Governance In Sharia Fintech: Challenges and Opportunities In The Digital Era', *Quality - Access to Success*, 24.196 (2023), 221–29 https://doi.org/10.47750/QAS/24.196.28
[105] Wardah Yuspin, Trisha Rajput, and others, 'The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle', *BESTUUR*, 12.1 (2024), 49 https://doi.org/10.20961/bestuur.v12i1.89742

Table 1. Banks' Weaknesses in Applying the Accountability Principle in Processing Personal Data

No.	Weaknesses in PDPL	Type of Violation	Offered Solution
1	There is no special notification system for data leakage.	The violation of personal data controllers' obligation. The obligation to give information to personal data subjects.	Develop an automatic notification system and conduct emergency response training for all branch offices.
2	The usage of customer data by third parties without the valid and explicit agreement of data subjects.	The violation against personal data controllers' obligation. The obligation to monitor third parties. The obligation to give notices in case of the failure to protect personal data.	Guarantee customers' explicit agreement before the data is used for product marketing or offers.
3	There is a slow response to security incidents in branch offices as the IT management is centered in the central office.	The violation against personal data controllers' obligation. The obligation to guarantee security and compliance with regulations.	Form regional IT teams to quickly handle incidents at the branch level.
4	The data updating process obliges customers to directly come to branch offices.	The violation against personal data controllers' obligation. The obligation to guarantee the accuracy of personal data. The obligation to update inaccurate personal data.	Provide online services through digital applications to ease the renewal of customer data without directly coming to the branch office.

Source: From various sources, processed by the researcher

Concerning the existence of some weaknesses in the application of the accountability principle in the processing of personal data, there are four main issues. First, banks still do not have a special notification system to inform customers in case of personal data leakage. So far, emergency response mechanisms to such incidents are still centered at the central office thus slowing the response in handling data leakage. To handle this, banks need to develop a notification system to inform customers in case of personal data leakage that is added with an explanation of the steps to handle the incident. There is also a need to increase emergency response training in all branch offices[106]. Second, banks have not made sure that the personal data disclosure to third parties, especially for objective product marketing or offers, is carried out with the valid and explicit agreement of data subjects. The lack of clarity on this agreement may risk violating customers' privacy rights and decrease their trust in the processing of personal data by banks. To handle this, banks need to guarantee the transparency of data uses by third parties for product marketing or offers by asking for consumers' explicit agreement before using the data. This is according to the principle of personal data protection.

Third, the management of information technology security in banks is still centralized at the central offers. Thus, branch offices have limited capabilities in quickly responding to security incidents. The dependency on the central office slows down the process of handling threats, especially at the branch level. To handle this,

[106] Bambang Waluyo and Ida Syafrida, 'Separation of Islamic Banks From Conventional Bank Ownership To Increase Market Share Of Islamic Banking In Indonesia', *Financial and Credit Activity Problems of Theory and Practice*, 2.61 (2025), 87–100 https://doi.org/10.55643/fcaptp.2.61.2025.4627

banks need to consider creating regional-level IT teams. Thus, in handling security issues, branch offices do not have to solely depend on the central office. Fourth, the data renewal process requires customers to directly come to the branch offices. This leads customers who live in isolated locations or those who have limited time to experience difficulties. This procedure does not only slow down the data renewal process but also decreases the service quality for customers with limited access. To handle this, banks need to provide online services through digital applications that ease customers in updating data without needing to directly come to branch offices. This is simpler for customers who live far away or those who do not have much time.

Personal data controllers still have some weaknesses in implementing their obligations. This shows that personal data controllers in Indonesia still need to improve themselves so that the goal of personal data processing may be achieved. The greatest weakness of the personal data controllers' accountability principle can be seen in the lack of a clear notification system to customers on the existence of data theft or leakage in a certain bank. As businesses whose reputation highly depends on society's trust, banks tend to cover the reality of the existence of data leakage by refraining from notifying their customers. Moreover, the explicit notification to customers shows that their data is in danger due to hacking[107].

In Indonesia, banks often do not clearly state that customers' personal data has been leaked. They always conduct news releases if there are difficulties in accessing a certain bank's website due to system updates. This is highly unfortunate as banks are unwise in implementing the accountability principle in personal data processing that obliges the delivery of notifications to customers in case of data leakage. Apart from that, banks also cannot guarantee that the customer data that they manage are not used or are not forwarded to third parties that are either from the same or different holding companies from that bank. For instance, in Indonesia, banking institutions usually also have non-bank financial institutions or securities where customers' data are often spread to these other institutions without notification to customers. This makes customers' personal data highly vulnerable to being misused by these other institutions as a facility to send promotions or other objectives[108]. Meanwhile, as for the application of personal data protection using the GDPR, there are still some weaknesses that are rather similar to the application of the PDP Law, such as the obligation to maintain the data that are under their control to be used by third parties. This weakness is also one of the things that become a problem. Apart from that, there is still a weakness in the form of a lack of notifications to data subjects in case of data leakage[109].

[107] Imron Mawardi, Mohammad Haidar Risyad and Muhammad Ubaidillah Al Mustofa, 'Does Economic Uncertainty Hinder or Help Business Profit? Evidence from Indonesia's Commercial Banking Industry', *International Journal of Islamic and Middle Eastern Finance and Management*, 18.4 (2025), 876–903 https://doi.org/10.1108/IMEFM-05-2024-0238

[108] Aang Kunaifi, Vera Oktari and Noorlailie Soewarno, 'ESG Disclosure and Firm Sustainable Growth Nexus in Indonesia's Emerging Markets: Does Working Capital Management Matter?', *Asian Review of Accounting*, 2025, 1–16 https://doi.org/10.1108/ARA-03-2025-0068

[109] Camila Amalia, 'Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment', *Journal of Central Banking Law and Institutions*, 1.2 (2022) https://doi.org/10.21098/jcli.v1i2.19

CONCLUSION

The PDPL determines that personal data controllers have the right to collect personal data with clear and valid reasons, and they also need individual agreement. Apart from that, personal data controllers have obligations that encompass the obligation to guarantee the legal basis for data processing, provide information on data objectives and changes, as well as process data in a valid and transparent manner. Apart from that, the processing of personal data must fulfill the accountability principle. They must process data according to the objectives and guarantee data accuracy. As personal data controllers, banks have the obligation to control the customer data under their control. Even though regulations on the accountability principle have been well contained both in the PDPL and the GDPR, there are still weaknesses in the application of this principle by data controllers. Based on the research, it was found that banks in Indonesia as personal data controllers have not fully fulfilled their obligations which encompass the lack of a special notification system for data leakage which slows down their responses to incidents; the lack of detailed information on the data disclosure to third parties that may potentially violate the principle of explicit agreement from personal data subjects; the centralized IT security system that limits the quick response at the branch level; and the data renewal procedures that obliges direct visits to branch offices that brings difficulty to customers with limited access. This weakness is due to the absence of a personal data supervisory body to oversee the performance of data controllers in each bank, resulting in the ineffectiveness of data controllers' accountability. While in Sweden the implementation of the principle of accountability is better than in Indonesia. Although there are some weaknesses in the implementation of this principle, in general Indonesia should imitate the implementation of this principle in Sweden.

ACKNOWLEDGMENT

We are grateful for the support from Lembaga Riset dan Inovasi (Research and Innovation Institute) of Universitas Muhammadiyah Surakarta which has provided financial support through International collaboration research funds with contract number 302.48/A3-III/LRI/VIII/2024, August 26, 2024.

References

Adenan, Moh, Mujab Syaiful Haq, M Abd Nasir and Thomas Soseco, 'The Effects of Macroprudential Policies on the Performance of Conventional Banks in Indonesia', *ECONOMICS*, 13 (2025), 369–86 https://doi.org/10.2478/eoik-2025-0012

Al-Habashneh, Amjad Ghazi, Suleiman Ibrahim Shelash Mohammad, Asokan Vasudevan, Ahmad Samed Al-Adwan, Anber Abraheem Shlash Mohammad and Lan Qing Jiang, 'Impact of the Quality of Financial and Banking Applications Used on Smartphone on the Customer Satisfaction of Jordanian Islamic Bank', *International Review of Management and Marketing* , 15 (2025), 99–106 https://doi.org/10.32479/irmm.17706

Alibeigi, Ali, Abu Bakar Munir and Adeleh Asemi, 'Compliance with Malaysian Personal Data Protection Act 2010 by Banking and Financial Institutions, a Legal Survey on Privacy Policies', *International Review of Law, Computers & Technology*, 35 (2021), 365–94 https://doi.org/10.1080/13600869.2021.1970936

Alrawhani, Ebrahim Mohammed, Awanis Romli and Mohammed A Al-Sharafi, 'Evaluating the

Role of Protection Motivation Theory in Information Security Policy Compliance: Insights from the Banking Sector Using PLS-SEM Approach', *Journal of Open Innovation: Technology, Market, and Complexity*, 11 (2025), 100463 https://doi.org/10.1016/j.joitmc.2024.100463

Alrawhani, Ebrahim Mohammed, Awanis Binti Romli, Mohammed A Al-Sharafi and Gamal Alkawsi, 'Integrating Information Security Culture and Protection Motivation to Enhance Compliance with Information Security Policies in Banking: Evidence from PLS-SEM and FsQCA', *International Journal of Human–Computer Interaction*, 2025, 1–22 https://doi.org/10.1080/10447318.2025.2464900

Amalia, Camila, 'Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment', *Journal of Central Banking Law and Institutions*, 1 (2022) https://doi.org/10.21098/jcli.v1i2.19

Amer, Tamer Bani and Mohammad Ibrahim Ahmed Al-Omar, 'The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector', *International Journal of Advanced Computer Science and Applications*, 14 (2023) https://doi.org/10.14569/IJACSA.2023.0140841

Amnesti, Sheila Kusuma Wardani, Siti Zulaichah and Nurul Istiqomah, 'Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective', *Legality : Jurnal Ilmiah Hukum*, 33 (2024), 1–19 https://doi.org/10.22219/ljih.v33i1.34623

Asyiqin, Istianah Zainal, 'Islamic Economic Law in the Digital Age: Navigating Global Challenges and Legal Adaptations', *Media Iuris*, 8 (2025), 95–112 <https://doi.org/10.20473/mi.v8i1.61800>

Barański, Stanisław, Julian Szymański and Higinio Mora, 'Anonymous Provision of Privacy-Sensitive Services Using Blockchain and Decentralised Storage', *International Journal of Information Security*, 24 (2025), 130 https://doi.org/10.1007/s10207-025-01052-w

Beltrán, Marta, 'AI Algorithms under Scrutiny: GDPR, DSA, AI Act and CRA as Pillars for Algorithmic Security and Privacy in the European Union', *Computers and Security*, 158 (2025), 104628 https://doi.org/10.1016/j.cose.2025.104628

BSI, *EKSPANSI DAN AKSELERASI BISNIS UNTUK PERTUMBUHAN BERKELANJUTAN*, *Laporan Tahunan BSI 2023*, 2023

Cao, Cao Dinh Lanh, 'Legal Framework for Banking Activities in Digital Enviroment. A Case Study of Vietnam', *PRAWO i WIĘŹ*, 53 (2025) https://doi.org/10.36128/PRIW.VI53.950

Casolaro, Ana Maria Barbosa, Gabriela Nogueira Rauber and Ursula Silveira Monteiro de Lima, 'Open Banking: A Systematic Literature Review', *Journal of Banking Regulation*, 26 (2025), 340–55 https://doi.org/10.1057/s41261-024-00262-x

Cerqueira, Diego André and others, *Experimental Evaluation of a Checklist-Based Inspection Technique to Verify the Compliance of Software Systems with the Brazilian General Data Protection Law*, *Empirical Software Engineering* (Springer US, 2025), xxx https://doi.org/10.1007/s10664-025-10681-7

Chen, Xin, 'Privacy Protection in the Context of CBDC: Development Trends and China's Practice', *Journal of East Asia and International Law*, 16 (2023), 211–32

https://doi.org/10.14330/jeail.2023.16.2.01

Chintale, Pradeep, Hrushikesh Deshmukh, Anirudh Khanna, Ankur Mahida and Madhavi Najana, 'Weighted Extreme Gradient Boosting Based Cybersecurity Risk Assessment in Investment Banking and Financial Sector', 2026, pp. 249–60 https://doi.org/10.1007/978-3-032-00793-3_20

Creswell, J. W., & Poth, C. N., *Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2018

Creswell, J. W., *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2018

Davey, Orima, Ria Wierma Putri, Tristiyanto, Yunita Maya Putri and Febryani Sabatira, 'GREEN BONDS IN INDONESIA: SYNERGY BETWEEN BANK INDONESIA AND OTORITAS JASA KEUANGAN'S COMMITMENT', *Journal of Central Banking Law and Institutions*, 2 (2023), 199–220 https://doi.org/10.21098/jcli.v2i2.37

Dudin, MN and S V. Shkodinsky, 'Challenges and Threats of the Digital Economy to the Sustainability of the National Banking System', *Finance: Theory and Practice*, 26 (2022), 52–71 https://doi.org/10.26794/2587-5671-2022-26-6-52-71

Dutta, Kaushan, Shouvik Parui, Subhadra Shaw, Sougata Biswas and Shirsak Das, 'Crime Analysis and Management System', *SN Computer Science*, 6 (2025), 799 https://doi.org/10.1007/s42979-025-04319-0

de Elizalde, F., *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, *Journal of Consumer Policy* (Springer US, 2025), XLVIII https://doi.org/10.1007/s10603-025-09584-3

Fabian Jonathan, Fajar Sugianto and Tomy Michael, 'Comparative Legal Analysis on the Competence of the Indonesia's Financial Services Authority And Monetary Authority of Singapore on the Enforcement of Insider Trading Laws', *Journal of Central Banking Law and Institutions*, 2 (2023), 283–300 https://doi.org/10.21098/jcli.v2i2.24

Farzanehfar, Ali, Florimond Houssiau and Yves-Alexandre de Montjoye, 'The Risk of Re-Identification Remains High Even in Country-Scale Location Datasets', *Patterns*, 2 (2021), 100204 https://doi.org/10.1016/j.patter.2021.100204

Felipe, Thiago, Rui Torres de Oliveira, Agnes Toth-Peter, Shane Mathews and Uwe Dulleck, 'Digital Transformation in Commercial Banks: Unraveling the Flow of Industry 4.0', *Digital Business*, 5 (2025), 100129 https://doi.org/10.1016/j.digbus.2025.100129

Flick, U., *An Introduction to Qualitative Research (6th Ed.). London: SAGE Publications.*, 2018

Foecking, Nico, Mei Wang and Toan Luu Duc Huynh, 'How Do Investors React to the Data Breaches News? Empirical Evidence from Facebook Inc. during the Years 2016–2019', *Technology in Society*, 67 (2021), 101717 https://doi.org/10.1016/j.techsoc.2021.101717

Fréminville, Marie, *Cybersecurity and Decision Makers* (Wiley, 2020) https://doi.org/10.1002/9781119720362

Galandarli, Arzu, 'Mitigating AI Risks: A Comparative Analysis of Data Protection Impact Assessments under GDPR and KVKK', *Journal of Data Protection & Privacy*, 7 (2025), 252 https://doi.org/10.69554/ATTT2755

Garg, Neha and Kapil Gupta, 'Data Privacy in Online Banking Using Blowfish Algorithm: A Review', in *Progressive Computational Intelligence, Information Technology and Networking* (London: CRC Press, 2025), pp. 888–91 https://doi.org/10.1201/9781003650010-145

Gioiosa, Silvia, Beatrice Chiavarini, Mattia D'Antonio, Giuseppe Trotta, Balasubramanian Chandramouli, Juan Mata Naranjo, and others, 'A GDPR-Compliant Solution for Analysis of Large-Scale Genomics Datasets on HPC Cloud Infrastructure', *Journal of Big Data*, 12 (2025) https://doi.org/10.1186/s40537-024-01047-9

Goettenauer, Carlos, 'The Brazilian Financial System, Cyber Security Policy and Personal Data Protection', *Law, State and Telecommunications Review*, 12 (2020), 172–86 https://doi.org/10.26512/lstr.v12i2.34716

Goldberg, Lawrence G, Richard J Sweeney and Clas G Wihlborg, 'Evaluating the Nordea Experiment: Evidence from Market and Accounting Data', *Journal of Banking & Finance*, 31 (2007), 1265–86 https://doi.org/10.1016/j.jbankfin.2006.10.010

Guo, Zhilong, 'Criminalisation of the Illegal Use of Personal Data: Comparative Approaches and the Chinese Choice', *Humanities and Social Sciences Communications*, 12 (2025), 1–16 https://doi.org/10.1057/s41599-025-05141-y

Haggag, Omar, Alessandro Pedace, Shidong Pan and John Grundy, 'An Analysis of Privacy Regulations and User Concerns of Finance Mobile Applications', *Information and Software Technology*, 184 (2025), 107756 https://doi.org/10.1016/j.infsof.2025.107756

Hamsin, Muhammad Khaeruddin, Abdul Halim, Rizaldy Anggriawan and Hilda Lutfiani, 'Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection', *Al-Manahij: Jurnal Kajian Hukum Islam*, 17 (2023), 53–66 https://doi.org/10.24090/mnh.v17i1.7633

Heitmann, Dennis, Jascha Alexander Koch, Mohammad Saiful Islam and Sharmin Akter Eva, 'The Impact of Central Bank Digital Currencies on the Financial Stability of Banks: Dynamic Panel Estimation', *Finance Research Letters*, 84 (2025), 107791 https://doi.org/10.1016/j.frl.2025.107791

Hisbulloh, Moh Hamzah, 'Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi', *Jurnal Hukum Unissula*, 37 (2021), 119–33 https://doi.org/10.26532/jh.v37i2.16272

Ho, Cynthia Sin Tian and Björn Berggren, 'The Effect of Accessibility to Bank Branches on Small- and Medium-Sized Enterprise Capital Structure: Evidence from Swedish Panel Data', *Journal of Risk and Financial Management*, 18 (2024), 14 https://doi.org/10.3390/jrfm18010014

Ho, Foo Nin, Nga Ho-Dac and J Sonia Huang, 'The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence', *Sage Open*, 13 (2023) https://doi.org/10.1177/21582440231181395

Hutchinson, T., *Doctrinal Research: Researching the Jury and Legal Methodology. In M.*

McConville & W. H. Chui (Eds.), Research Methods for Law (2nd Ed., Pp. 7–31). Edinburgh University Press. Hutchinson, T. (2018). Doctrinal Research: Researching the Jury and Legal Metho, 2018

Hutchinson, Terry and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research', *Deakin Law Review*, 17 (2012), 83 https://doi.org/10.21153/dlr2012vol17no1art70

Indonesia, *Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*, *Indonesia, Pemerintah Pusat*, 2022

Isnaeni, Atin Meriati, 'Premi Payment of the "Banker"S Clause Insurance in a Credit Agreement (Review of Deed of Credit Agreement Pt. Bank Danamon Mataram)', *Jurnal IUS Kajian Hukum Dan Keadilan*, 9 (2021), 682–96 https://doi.org/10.29303/ius.v9i3.978

Kariuki, Paul, Lizzy Oluwatoyin Ofusori and Maria Lauda Joel Goyayi, 'Internet of Things on Banking Processes in South Africa: A Systematic Reflection on Innovations, Opportunities and Challenges', *Digital Business*, 5 (2025), 100097 https://doi.org/10.1016/j.digbus.2024.100097

Karpjáková, Anežka, 'Protection of a Bank's Clients against Payment Frauds Based on Social Engineering', *Jusletter-IT*, 2024 https://doi.org/10.38023/f6597dc5-b5b8-4c73-ae59-1ae55d1827cf

Khan, Harun R, 'Banking Sector Banking Sector', 2014, 1–15

Khanna, Vasudha and Atul Kotwal, 'Examining the Significance of the Digital Personal Data Protection Act, 2023 in the Context of the Healthcare Industry: A Comprehensive Analysis', *Discover Public Health*, 22 (2025), 1–13 https://doi.org/10.1186/s12982-025-00757-6

Kokot, Sebastian, 'Comparative Evaluation of Public Data Sets on Average House Prices in Poland', *Folia Oeconomica Stetinensia*, 25 (2025), 157–79 https://doi.org/10.2478/foli-2025-0008

Kossovsky, Nir, *Reputation, Stock Price, and You* (Berkeley, CA: Apress, 2012) https://doi.org/10.1007/978-1-4302-4891-0

Kumar, Avishek and Tyson Silver, 'Know, Grow, and Protect Net Worth: Using ML for Asset Protection by Preventing Overdraft Fees', in *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (New York, NY, USA: ACM, 2024), pp. 5272–82 https://doi.org/10.1145/3637528.3671628

Kunaifi, Aang, Vera Oktari and Noorlailie Soewarno, 'ESG Disclosure and Firm Sustainable Growth Nexus in Indonesia's Emerging Markets: Does Working Capital Management Matter?', *Asian Review of Accounting*, 2025, 1–16 https://doi.org/10.1108/ARA-03-2025-0068

Kurmanova, Lilia, Elvira Nurdavliatova, Diana Kurmanova, Guzaliya Galimova and Rinat Khabibullin, 'Development of Digital Services and Information Security of Banks', in *IV International Scientific and Practical Conference* (New York, NY, USA: ACM, 2021), pp. 1–6 https://doi.org/10.1145/3487757.3490911

Kusuma, Oktaria Wim and Abraham Ferry Rosando, 'Urgensi Perlindungan Hukum Terhadap

Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online', *Jurnal Hukum Bisnis Bonum Commune*, 5 (2022), 123–41 https://doi.org/10.30996/jhbbc.v5i1.6087

L, Ashwini, R Poornima Lakshmi and S Pavithra, 'Cybersecurity in Banking and Cloud Computing: Threats, Defenses, and Innovations', in *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)* (IEEE, 2025), pp. 1–6 https://doi.org/10.1109/ICDSAAI65575.2025.11011646

Lakshmi, K Krithig, Himanshu Gupta and Jayanthi Ranjan, 'Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges', in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (IEEE, 2020), pp. 1028–32 https://doi.org/10.1109/ICRITO48877.2020.9197954

Landini, Austin and Russell Spears, 'Banks Approved Fraudulent Loans to Capture Origination Fees: Evidence from the Paycheck Protection Program', *Journal of Financial Crime*, 32 (2025), 763–75 https://doi.org/10.1108/JFC-07-2024-0201

Laurinaitis, Marius, Darius Štitilis and Egidijus Verenius, 'Implementation of the Personal Data Minimization Principle in Financial Institutions: Lithuania's Case', *Journal of Money Laundering Control*, 24 (2021), 664–80 https://doi.org/10.1108/JMLC-11-2020-0128

Lazcano, Israel Cedillo, 'Explainability and Operational Resilience in the Design of Central Bank Digital Currencies: A New Generation of Money-Laundering Deterrence Software', *Journal of Payments Strategy & Systems*, 18 (2024), 179 https://doi.org/10.69554/BDTD2604

Legowo, Mercurius Broto, Fangky Antoneus Sorongan and Steph Subanidja, 'Risk Management of Bank and FinTech Collaboration: A Phenomenological Research', in *2023 6th International Conference of Computer and Informatics Engineering (IC2IE)* (IEEE, 2023), pp. 94–100 https://doi.org/10.1109/IC2IE60547.2023.10331156

Li, Fanghua, Jiewei Liu and Haiyue Liu, 'Institutions Empowerment for Sustainability: ESG Performance and Enterprise Green Innovation—Evidence from China', *Journal of Environmental Management*, 388 (2025), 125947 https://doi.org/10.1016/j.jenvman.2025.125947

Liu, Huizheng, Muhammad Afaq Haider Jafri, Shuo Xu and Muhammad Farrukh Shahzad, 'The Impact of Artificial Intelligence on Consumers' Willingness to Use CBDCs: Evidence from the Chinese Banking Sector', *Humanities and Social Sciences Communications*, 12 (2025) https://doi.org/10.1057/s41599-025-05067-5

Liu, Xin, Jiaqi Wu and Chenghu Zhang, 'Antecedents of Consumers' Acceptance of Central Bank Digital Currency: The Role of Technology Perceptions, Social Influence and Personal Traits', *Technological Forecasting and Social Change*, 217 (2025), 124192 https://doi.org/10.1016/j.techfore.2025.124192

Liu, Yang, Aisyah Abdul Rahman, Syajarul Imna Mohd Amin and Roslan Ja'afar, 'Navigating Fintech and Banking Risks: Insights from a Systematic Literature Review', *Humanities and Social Sciences Communications*, 12 (2025), 1–16 https://doi.org/10.1057/s41599-025-05055-9

Ma, WenGuang, Zelong Yin, Jinyan Zhou, ChongChong Jia, HaiPing Yang, JinLong Wang,

and others, 'Research on Credit Card Fraud Detection System Based on Federated Learning', in *Proceedings of the 2024 3rd International Conference on Frontiers of Artificial Intelligence and Machine Learning* (New York, NY, USA: ACM, 2024), pp. 242–45 https://doi.org/10.1145/3653644.3680500

Mawardi, Imron, Mohammad Haidar Risyad and Muhammad Ubaidillah Al Mustofa, 'Does Economic Uncertainty Hinder or Help Business Profit? Evidence from Indonesia's Commercial Banking Industry', *International Journal of Islamic and Middle Eastern Finance and Management*, 18 (2025), 876–903 https://doi.org/10.1108/IMEFM-05-2024-0238

Mezal, Yasser Ali and Amis Mohammed Bahgat, 'Digital Transformation and Its Impact on Banking Operations (A Study of a Sample of Private Iraqi Banks)', 2026, pp. 234–49 https://doi.org/10.1007/978-3-032-01592-1_14

Mohammadzadeh, Anoosh, Samira Farjaminejad, Poonam Patel, Sandra Nanyonga, Raheelah Ahmad, Charitini Stavropoulou, and others, 'Biobanking in Sub-Saharan Africa: A Review of Data Protection Frameworks', *Biopreservation and Biobanking*, 23 (2025), 177–85 https://doi.org/10.1089/bio.2024.0086

Nguyen, Tuan Thanh, Hoang Thi Tran, Khoa Thanh Nhat Tran, Oanh Thi Xuan Nguyen, Anh Tu Thi Nguyen and Roger Mathisen, 'Application of a Locally Developed Open-Access Digital Monitoring System for the Human Milk Bank Network in Vietnam', *International Breastfeeding Journal* , 20 (2025), 1–16 https://doi.org/10.1186/s13006-025-00745-1

Nindito, Marsellisa, Ilya Avianti, Poppy Sofia Koeswayo and Nanny Dewi Tanzil, 'Guardians of Integrity: Exploring the Role of Corporate Governance in Preventing Financial Statement Fraud', *Journal of Governance and Regulation*, 14 (2025), 109–18 https://doi.org/10.22495/jgrv14i1art10

Nurfitriyani, Siti Hamidah and Reka Dewantara, 'Analysis of Economic Law on Banking Regulation in Customer Legal Protection', *Jurnal IUS Kajian Hukum Dan Keadilan*, 9 (2021), 460–71 https://doi.org/10.29303/ius.v9i2.911

Nurhasanah, Nurhasanah and Indra Rahmatullah, 'Financial Technology and the Legal Protection of Personal Data: The Case of Malaysia and Indonesia', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 20 (2020), 197–214 https://doi.org/10.30631/alrisalah.v20i2.602

Oeding, Noemí and Kara Newby, 'The Social Enterprise Craze: CSO Financial Sustainability in Ghana', *Nonprofit Policy Forum*, 16 (2025), 55–78 https://doi.org/10.1515/npf-2022-0035

Palm, Peter, 'Practice Briefing: Environmental, Social and Governance (ESG) and Real Estate Valuation - the Case of Sweden', *Journal of Property Investment & Finance*, 43 (2025), 255–64 https://doi.org/10.1108/JPIF-12-2024-0163

Priskarini, Intan Audia, Pranoto and Kukuh Tejomurti, 'The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia', *Padjadjaran Jurnal Ilmu Hukum*, 6 (2019), 556–75 https://doi.org/10.22304/pjih.v6n3.a7

Rahim, Erman I, Mohamad Afriyansyah Dukalang, Abdul Hamid Tome, Nuvazria Achir and Souad Ezzerouali, 'Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations', *Journal*

of Law and Legal Reform, 6 (2025), 1305–48 https://doi.org/10.15294/jllr.v6i3.12942

Rupeika-Apoga, Ramona, Janis Priede, Gundars Berzins and Elmars Kehris, 'Regulation and Innovation in Digital Finance: The Transformation of Latvia's Banking Sector', *Digital Business*, 5 (2025), 100147 https://doi.org/10.1016/j.digbus.2025.100147

Sahetapy, Wilma Laura, 'Perlindungan Data Pribadi Anak Dalam E-Commerce Di Masa Pandemi Covid-19', *Jurnal Hukum Bisnis Bonum Commune*, 4 (2021), 214–25 https://doi.org/10.30996/jhbbc.v4i2.5319

Sarabdeen, Jawahitha and Mohamed Mazahir Mohamed Ishak, 'A Comparative Analysis: Health Data Protection Laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)', *International Journal of Law and Management*, 67 (2025), 99–119 https://doi.org/10.1108/IJLMA-01-2024-0025

Sarma, Mandira, 'Financial Digitalization in India', *Eurasian Economic Review*, 15 (2025), 401–24 https://doi.org/10.1007/s40822-024-00298-4

Schreier, M., *Qualitative Content Analysis in Practice. London: SAGE Publications.*, 2012

Schulz, Karol, Vincent Karovič and Peter Veselý, 'Options to Improve the General Model of Security Management in Private Bank with GDPR Compliance', 2021, pp. 343–70 https://doi.org/10.1007/978-3-030-62151-3_8

Shunmugam, Meenakshi, Satya Rajesh Kunchaparthy and Baby Kalpana, 'High Protection Bank Locker Security Alert System Using Voice Authentication Based on Wireless Sensor Network', 2023, p. 020027 https://doi.org/10.1063/5.0115687

Singh, Avtar and Amira Omer Ali, 'Protecting What Matters: Data Privacy Solutions for Qatar's Expanding Mobile Banking Sector', *Journal of Data Protection & Privacy*, 8 (2025), 24 https://doi.org/10.69554/MVIY7029

Supeno, Supeno, Rosmidah Rosmidah and Syed Mohd Uzair Iqbal, 'Personal Data Protection in Review of Legal Theories and Principles', *Journal of Law and Legal Reform*, 6 (2025), 1349–76 https://doi.org/10.15294/jllr.v6i3.10252

TAKARAGI, Kazuo, Takashi KUBOTA, Sven WOHLGEMUTH, Katsuyuki UMEZAWA and Hiroki KOYANAGI, 'Secure Revocation Features in EKYC - Privacy Protection in Central Bank Digital Currency', *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E106.A (2023), 2022CIP0008 https://doi.org/10.1587/transfun.2022CIP0008

Tsamara, Nadiah, 'Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara', *Jurnal Suara Hukum*, 3 (2021), 53–85 https://doi.org/10.26740/jsh.v3n1.p53-84

Vafaei-Zadeh, Ali, Davoud Nikbin, Kit Yik Teoh and Haniruzila Hanifah, 'Cybersecurity Awareness and Fear of Cyberattacks among Online Banking Users in Malaysia', *International Journal of Bank Marketing*, 43 (2025), 476–505 https://doi.org/10.1108/IJBM-03-2024-0138

Waluyo, Bambang and Ida Syafrida, 'SEPARATION OF ISLAMIC BANKS FROM CONVENTIONAL BANK OWNERSHIP TO INCREASE MARKET SHARE OF ISLAMIC

BANKING IN INDONESIA', *Financial and Credit Activity Problems of Theory and Practice*, 2 (2025), 87–100 https://doi.org/10.55643/fcaptp.2.61.2025.4627

Wang, Zhangyu and Li Du, 'An Empirical Study on Personal Data Protection in the Banking Sector across Hong Kong, Macau, and Mainland China', *The Chinese Journal of Comparative Law*, 13 (2025) https://doi.org/10.1093/cjcl/cxae021

Warikandwa, Tapiwa V, 'Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared', *Potchefstroom Electronic Law Journal*, 24 (2021), 1–32 https://doi.org/10.17159/1727-3781/2021/v24i0a10727

Wathahong, Thanwa, Roongkiat Ratanabanchuen, Praima Israsena Na Ayudhya and Kitt Tientanopajai, 'Assessing Disruptive Potential of Retail Central Bank Digital Currency and Influence of Design Considerations: An Open Innovation Approach in Thailand', *Journal of Open Innovation: Technology, Market, and Complexity*, 11 (2025), 100502 https://doi.org/10.1016/j.joitmc.2025.100502

Wibowo, Dwi Edi, 'Penerapan Konsep Utilitarianisme Untuk Mewujudkan Perlindungan Konsumen Yang Berkeadilan Kajian Peraturan Otoritas Jasa Keuangan Nomor: 1/Pojk.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan', *Syariah: Jurnal Hukum Dan Pemikiran*, 19 (2019), 15–30 https://doi.org/10.18592/sy.v19i1.2296

Wu, Hao, Norzieiriani Ahmad and Nazlina Zakaria, 'Green Banking Initiatives: The Role of CSR in Aligning with the SDGs and Shaping Sustainable Consumer Choices', *Acta Psychologica*, 258 (2025), 105195 https://doi.org/10.1016/j.actpsy.2025.105195

Yin, R. K., *Case Study Research: Design and Methods (5th Ed.). Thousand Oaks, CA: SAGE Publications.*, 2014

Yuspin, Wardah and Ata Fauzie, 'Good Corporate Governance In Sharia Fintech: Challenges and Opportunities In The Digital Era', *Quality - Access to Success*, 24 (2023), 221–29 https://doi.org/10.47750/QAS/24.196.28

Yuspin, Wardah, Alda Oktalivia Putri, Ata Fauzie and Jompon Pitaksantayothin, 'Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities', *International Journal of Safety and Security Engineering*, 14 (2024), 1699–1706 https://doi.org/10.18280/ijsse.140605

Yuspin, Wardah, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono and Absori Absori, 'The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle', *BESTUUR*, 12 (2024), 49 https://doi.org/10.20961/bestuur.v12i1.89742

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman and Arief Budiono, 'Personal Data Protection Law in Digital Banking Governance in Indonesia', *Studia Iuridica Lublinensia*, 32 (2023), 99–130 <https://doi.org/10.17951/sil.2023.32.1.99-130>

Zahariev, Martin, George Dimitrov, Daniela Pavlova, Panayot Gindev, Vyara Savova and Radoslava Makshutova, 'KEY TAKEAWAYS FROM THE MOST SIGNIFICANT GDPR PERSONAL DATA BREACHES IN THE REPUBLIC OF BULGARIA', *ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference*, 5 (2025), 353–61 https://doi.org/10.17770/etr2025vol5.8482

Zaid, Mohammed Abdulrahman Kaid, Mohammed Farooque Khan, Abdul Wasea Abdul Ghani Saif Al-Mekhlafi, Ibraheem Saleh Al Koliby, Oussama Saoula, Hayat Atta Elmnan Mohammed Saeed, and others, 'The Future of Green Finance: How Digital Transformation and FinTech Drive Sustainability', *Discover Sustainability*, 6 (2025) https://doi.org/10.1007/s43621-025-01356-w

Zamzam, Muhammad Ilham Mahrudin, Rofadan Mina Arsyada and Nadya Eka Amalia Al'azza, 'The Validity of Electronic Contractual Relationships in E-Commerce and Legal Liability for Leakage of Users' Personal Data', *Jurnal Suara Hukum*, 5 (2023), 130–48 https://doi.org/10.26740/jsh.v5n2.p130-148

Van Zeeland, Ine and Jo Pierson, 'Data Protection Risks in Transitional Times: The Case of European Retail Banks', in *Data Protection and Privacy, Volume 15* (Hart Publishing, 2023) https://doi.org/10.5040/9781509965939.ch-001

Zheng, Yunjiao, 'Bank Data Protection and Fraud Identification Based on Improved Adaptive Federated Learning and WGAN', *Scientific Reports*, 15 (2025), 1–17 https://doi.org/10.1038/s41598-025-06807-y

Zulkifli, Wetria Fauzi and Arya Putra Rizal Pratama, 'Pengawasan Terhadap Perlindungan Hukum Konsumen Perbankan Oleh Otoritas Jasa Keuangan Di Kota Padang', *Jurnal Hukum Bisnis Bonum Commune*, 5 (2022), 25–41 https://doi.org/10.30996/jhbbc.v5i1.5781