INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 09 Issue 11 November 2026

DOI: 10.47191/ijmra/v9-i11-19, Impact Factor: 8.685

Page No. 7593-7598

Dispute Resolution Efforts and Legal Obstacles Faced by Customers in Claiming Compensation for Personal Data Breaches in the Banking Sector

Bagus Rahmanda[1], Melati Alya Putri[2], Benedictus Satryo Wibowo[3]

[1,2,3]Faculty of Law, Universitas Diponegoro, Jl. dr. Antonius Suroyo, Tembalang, Semarang, Indonesia

ABSTRACT: The increasing frequency of personal data breaches, particularly in the banking sector, underscores the urgent need for legal protection of personal data transfer mechanisms, especially where data is transferred as a risk-mitigation measure when a breach occurs. This study analyzes the prevailing regulation of personal data transfer and the forms of legal protection available to bank customers when data is transferred in the context of a data breach. It employs a normative juridical method with descriptive-analytical and prescriptive-analytical specifications, using secondary data consisting of primary, secondary, and tertiary legal materials collected through library research and analyzed qualitatively. The findings show that Indonesia's regime on personal data transfer, namely Law No. 27 of 2022 on Personal Data Protection, does not technically regulate the end-to-end mechanism of data transfer, thereby creating a legal vacuum. This vacuum is currently filled by cooperation agreements between the parties, without any definitive standard clauses to refer to. The legal protection available to bank customers is both preventive and repressive. Preventive legal protection can be pursued through the application of banking principles and the ISO 27001:2022 standard, whereas repressive legal protection takes the form of criminal sanctions and civil liability for breach of contract or unlawful acts. Accordingly, the personal data protection framework needs to be amended to make it more comprehensive, and the implementing regulations of Law No. 27 of 2022 need to be enacted in order to provide long-term legal certainty.

KEYWORDS: personal data transfer, legal protection, bank customers, data breaches

I. INTRODUCTION

Digitalization in the era of the Industrial Revolution 4.0 has driven many aspects of life toward network-based information systems. Easier access to information has also affected the banking sector, where banks have come to rely on digital storage to manage customers' personal data, such as names, places of residence, and occupations. Every prospective customer who registers is deemed to have agreed to the data processing terms set out in the relevant bank's privacy policy.

The processing of personal data in Indonesia is governed principally by Law No. 27 of 2022 on Personal Data Protection (the PDP Law). This law regulates not only the collection and storage of data, but also the rights and obligations of the parties, the mechanism for reporting data breaches, sanctions, and the transfer of personal data. In practice, data processing generally involves two main parties, namely the data controller and the data processor, whose responsibilities are set out in a cooperation agreement.

The transfer of personal data is a form of data processing that allows data to be moved from one place to another. Under Chapter VII of the PDP Law, data may be transferred within or outside the territory of Indonesia subject to certain conditions, such as the obligation to ensure that the destination country has a level of data protection that is equivalent to or higher than Indonesia's. If this requirement is not met, the data controller must obtain the consent of the data subject.

The banking sector has not escaped the threat of personal data breaches. One case that attracted attention was the alleged hacking of Bank Rakyat Indonesia (BRI) customer data by the Bashe Ransomware group in 2024, although this was later confirmed to be false information. Nevertheless, the 2020 BRI data leak has remained confirmed as genuine because the data could be accessed through platforms such as Scribd, which indicates negligence on the part of the bank in protecting its earlier data (Sario et al., 2023).

A similar case occurred at BRI Life in 2021, when 250 gigabytes of sensitive customer data were hacked and sold for US$7,000. In addition, the BPJS data leak caused losses estimated at as much as Rp600 trillion. These events show that data breaches harm not only institutions but also cause material and immaterial losses to customers as the owners of the data.

One risk-mitigation mechanism that banks can adopt is the transfer of personal data in order to move customer data to a more secure server. This mechanism is consistent with Article 3 point 6 of Law No. 8 of 1999 on Consumer Protection, which guarantees customers' right to comfort, security, and safety in using banking services.

At present, there is no regulation that technically governs the mechanism of personal data transfer from upstream to downstream (end to end), whether within the banking sector or generally. The personal data transfer clauses in banking contracts are merely exoneration clauses that give the bank unilateral freedom without transparency to the customer. This lack of clarity creates a legal vacuum that has the potential to produce uncertainty for customers, which prompted the authors to examine further the optimal form of legal protection for customers in the context of personal data transfer when a data breach occurs in the banking sector.

This study uses the theory of legal protection as its main foundation for analyzing the problems under study. According to Philipus M. Hadjon, legal protection takes two forms, namely preventive and repressive legal protection (Hadjon, 1987, p. 25). Preventive legal protection aims to prevent disputes by giving legal subjects the opportunity to raise objections before a decision becomes definitive (Waluyo et al., 2025), whereas repressive legal protection aims to resolve disputes that have already occurred through the imposition of sanctions in the form of imprisonment, fines, and other additional penalties (Risnaldi et al., 2026). In the context of this study, both forms of legal protection are used to analyze how bank customers can be protected, both before and after a personal data breach resulting from data transfer activities carried out by the bank. Satjipto Rahardjo, through his progressive legal theory, reinforces this framework by emphasizing that law functions not merely as a deterrent but also as a response to events that have caused harm in society (Rahardjo, 2011), so that law must be flexible and adaptive to the evolving needs of society, including in the protection of banking customers' personal data.

Based on this background, this legal research addresses two research questions. First, what dispute resolution efforts and legal obstacles do customers face in claiming compensation for personal data breaches in the banking sector? Second, what legal consequences arise for the bank, as the data controller, and for the customer, as the data subject, when data protection fails in the transfer process?

II. RESEARCH METHODS

Research is an activity aimed at collecting data to be processed and from which conclusions are drawn in order to answer a problem (Ashshofa, 2004). Conducting research requires a procedure so that the research proceeds in a directed manner and in accordance with applicable standards. The procedure used in research is called the research method.

This study uses a normative juridical or doctrinal approach, that is, research conducted by examining various sources in the form of norms, doctrines, principles, theories, and prevailing legal rules as *law in books* (Suteki, 2018) in order to answer the legal issues that are the object of the study. This approach was chosen because the study aims to analyze the legality of the transfer of bank customers' personal data and the forms of legal protection available to customers when a data breach occurs, all of which can be answered by examining the applicable regulations and legal literature.

The research specification used is both descriptive-analytical and prescriptive-analytical. The descriptive-analytical specification is used to describe the legal facts existing in society (Adi, 2021) with regard to personal data breaches and the mechanism of personal data transfer, while the prescriptive-analytical specification is used to assess what is ideal in law, in terms of norms, principles, doctrines, and legal theories, so as to produce constructive recommendations for resolving the problems under study (Moleong, 2018).

The type of data used in this study is secondary data, namely data obtained indirectly by the researchers through intermediaries in the form of documents, literature, and internet sources relevant to the research topic (Kurniawati et al., 2022). The secondary data consist of three types of legal materials. First, primary legal materials, which are binding, comprise the Indonesian Civil Code, the 1945 Constitution, Law No. 10 of 1998 on Banking, Law No. 8 of 1999 on Consumer Protection, Law No. 11 of 2008 on Electronic Information and Transactions as amended, Law No. 27 of 2022 on Personal Data Protection, Bank Indonesia regulations on know-your-customer principles and anti-money laundering, Financial Services Authority (OJK) Regulation No. 22 of 2023 on Consumer Protection in the Financial Services Sector, and Law No. 30 of 1999 on Arbitration and Alternative Dispute Resolution. Second, secondary legal materials, which are not directly binding but serve as additional references in analyzing legal problems, comprise books, scientific journals, expert opinions, and other literature relevant to personal data protection and personal data transfer. Third, tertiary legal materials, which complement the understanding of the primary and secondary legal materials, namely the *Kamus Besar Bahasa Indonesia* (the Great Dictionary of the Indonesian Language) and *Black's Law Dictionary*.

The data collection method used in this study is library research or document study, that is, collecting data by examining various relevant documents and literature to obtain the information needed to answer the research problems (Adi, 2021). This method was carried out through a series of activities consisting of identifying statutory regulations, searching scientific journals, and reading books and other sources, which were then selected according to their relevance to the research topic.

The collected data were analyzed using a qualitative method, which, as Bogdan and Taylor (as cited in (Moleong, 2018)) argue, produces descriptive data about the object observed. This method was chosen because the study is based on non-numerical data in the form of narratives of personal data transfer events, which were then analyzed systematically and correlated with the primary legal materials to identify whether a legal vacuum exists in such personal data transfer events, and from which conclusions and recommendations were ultimately drawn to answer all the problems in this study.

III. RESULTS AND DISCUSSION

Based on the theoretical framework used, two main discussions can be produced, namely:

A. Regulation of Bank Customers' Personal Data Transfer in Force in Indonesia

Modernization has given rise to a need for law that is adaptive, especially in the fields of technology and personal data protection. The progressive legal theory propounded by Prof. Satjipto Rahardjo asserts that law functions not only to prevent what has not yet occurred, but is also formed in response to events that have caused harm in society. Therefore, good law must be flexible and able to adapt to the evolving needs of society, rather than forcing society to adapt to rigid law. In the context of personal data protection, this means that existing regulations must be able to keep pace with the rapid development of information technology, including in regulating the mechanism of personal data transfer, which is occurring ever more frequently across sectors, particularly banking.

Historically, personal data protection in Indonesia began with the second amendment of the 1945 Constitution through Article 28G paragraph (1), which states that everyone has the right to personal protection. Then, in 2008, the government enacted Law No. 11 of 2008 on Electronic Information and Transactions (the EIT Law) in response to the rapid development of electronic activities in society, such as social media and *e-commerce*. This first-generation regulation introduced a number of new terms relating to the electronic world, such as electronic systems, electronic signatures, and electronic contracts. Although the EIT Law does not specifically regulate the transfer of personal data, Article 32 of that law provides that the transfer of electronic information without right or in violation of the law is a prohibited act, thereby indirectly providing initial protection for data transfer activities.

A further development came with the enactment of Law No. 19 of 2016 amending the EIT Law, which regulates the obligation of data controllers to delete data of subjects that is no longer relevant or at the request of its owner. Subsequently, the increasingly pressing public need for comprehensive personal data protection led to the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law), which explicitly and specifically regulates the rights of data owners, the obligations of data controllers and processors, complaint mechanisms, sanctions, and the transfer of personal data. The PDP Law updates the definition of personal data as information about an individual who can be identified through either electronic or non-electronic systems, while at the same time regulating more comprehensively all aspects of personal data processing, including personal data transfer as a form of processing that allows data to be moved from one place to another, whether domestically or across borders (Rachayu et al., 2023).

With regard to cross-border personal data transfer, Article 56 of the PDP Law in conjunction with Article 21 of OJK Regulation 22/2023 hierarchically sets out three requirements that the data controller must fulfill. First, the destination country of the transfer must have a level of personal data protection that is equivalent to or higher than Indonesia's. Second, if the first requirement is not met, the data controller must ensure that personal data protection in the destination country remains adequate and binding through a cooperation agreement between controllers. Third, if neither of the preceding requirements can be met, the data controller must obtain the direct consent of the personal data owner (Zahra et al., 2024).

In the banking sphere, the regulation of personal data transfer becomes more complex because of the application of the principle of *lex specialis derogat legi generali*. To date, the Banking Law has not been amended to explicitly regulate the mechanism of customers' personal data transfer. The provisions of the Banking Law only regulate access to customer data for investigative purposes by certain parties such as the police, prosecutors, and judges where a customer is involved in a criminal case. Consequently, the regulation of personal data transfer in the banking sphere still relies entirely on the PDP Law as its legal basis, while the standard-form contract signed by customers upon registration contains only exoneration clauses that give the

bank the freedom to determine how and where data will be transferred, without any mechanism for further consent from the customer.

This regulatory limitation ultimately gives rise to a significant legal vacuum in the practice of personal data transfer in Indonesia. To date, there is no specific regulation governing the technical steps for how personal data transfer must be carried out from upstream to downstream, from the delivery mechanism, the responsible parties, and the standard clauses that must be included in the agreement, to the security standards that must be met throughout the transfer process. This legal vacuum is temporarily filled by cooperation agreements between the parties based on the principle of *pacta sunt servanda* as provided in Article 1320 of the Indonesian Civil Code, but without any definitive standard clauses to refer to, which has the potential to give rise to multiple interpretations and legal uncertainty for all parties involved, especially for customers as the owners of personal data.

The legal vacuum becomes even more apparent when we look at the experience of other countries in dealing with similar problems. The case of Meta Platforms Ireland Limited, which was fined 1.2 billion euros by the European Data Protection Board in 2023 for transferring the personal data of European citizens to the United States without meeting protection standards equivalent to those of the General Data Protection Regulation (GDPR), shows that the absence of technical regulation of personal data transfer can have very significant legal consequences. Therefore, the enactment of implementing regulations of the PDP Law that technically and comprehensively regulate the mechanism of personal data transfer is urgently needed in order to create long-term legal certainty, particularly for banking customers whose personal data is sensitive and vulnerable to misuse.

B. Forms of Legal Protection for Bank Customers Against Personal Data Transfer by Banks in the Event of a Data Breach

The issue of data breaches is becoming increasingly widespread and affects various sectors. Banking is one of the sectors in which data breaches frequently occur in Indonesia. This calls for concrete legal protection for customers, especially in the context of personal data transfer. The causes of personal data breaches are highly varied, ranging from weak data storage security systems and the lack of two-factor authentication to cyberattacks and even negligence on the part of the customers themselves (Lesmana1 et al., 2025). The low digital literacy of the public is also a contributing factor, because many users do not understand privacy settings or the risks inherent in their digital activities.

Through various regulations the state has sought to protect the personal data of its citizens, but the legal vacuum on the technical mechanism of personal data transfer remains a gap that has yet to be closed. Therefore, according to (Hadjon, 1987), legal protection for customers can be divided into two main forms, namely preventive legal protection and repressive legal protection.

Preventive legal protection in the banking sphere is realized through the application of banking principles, which are obligations of the bank as the personal data controller. Under Article 29 of the Banking Law in conjunction with Article 35 of the PDP Law, banks must apply the principles of trust, prudence, and confidentiality in every customer data processing activity, including personal data transfer. The principle of trust requires banks to maintain the trust of customers who voluntarily hand over their personal data, and to provide information where there is a risk of loss in the transactions carried out. The principle of prudence requires banks to align all of their operational activities, including data processing, with the applicable laws and regulations. The principle of confidentiality requires banks to protect customer information from unauthorized access, with limited exceptions for taxation, judicial purposes, and the bank's operational interests that are strictly regulated in the Banking Law(Yuspin et al., 2023).

In addition to the application of banking principles, preventive legal protection can also be realized through the application of the international standard ISO/IEC 27001:2022 (*ISO/IEC 27701:2025 - Information Security, Cybersecurity and Privacy Protection — Privacy Information Management Systems — Requirements and Guidance*, n.d.) as a reference for information security in personal data transfer activities. The standard covers ten important aspects, namely: information security policy; organization of information security through the appointment of a Data Protection Officer (DPO); data asset management; access control based on the principle of least privilege; encryption and data protection in transit; operational security through periodic audits; application system security, including penetration testing; third-party security management; compliance with applicable regulations; and information security incident management. The application of ISO/IEC 27001:2022 is important because it gives banks a structured technical framework to ensure that every stage of personal data transfer is carried out securely and responsibly in accordance with the PDP Law.

In particular, the incident management aspect of ISO/IEC 27001:2022 requires banks to provide clear procedures when a data security breach occurs, including the obligation to notify the personal data owner, the government, and the public. Where personal data transfer is necessary as a security measure following a data breach, the bank must give each customer detailed

notice of who the parties involved are, where the data will be moved, how the process will be carried out, and when the transfer will take place. This transparency cannot be replaced merely by the exoneration clause signed by the customer when registering an account, because its purpose is to ensure that the personal data owner knows that his or her information is being processed lawfully and responsibly, as mandated by Article 16 of the PDP Law.

Meanwhile, repressive legal protection can take two forms, namely liability for breach of contract and liability for unlawful acts. Liability for unlawful acts can serve as an instrument of dispute resolution after a violation of the rights of the customer as the owner of personal data has occurred. Articles 67 to 73 of the PDP Law expressly provide that a person who violates the rights of a personal data subject may be subject to imprisonment of up to 6 years, a fine of up to Rp6 billion, confiscation of the proceeds of the crime, suspension of business activities, revocation of the business license, and even dissolution of the institution. In addition, the Banking Law provides for heavier sanctions where a bank intentionally discloses customer information, namely imprisonment of up to 10 years and a fine of up to Rp100 billion. A bank may also be subject to administrative sanctions by Bank Indonesia if it is proven not to have fulfilled its obligation to safeguard customer data.

In addition to liability for unlawful acts, repressive legal protection may also take the form of liability for breach of contract. Liability for breach of contract arises when the bank fails to fulfill its obligations as stated in the data privacy contract with the customer, for example by negligently failing to protect customer information and thereby causing loss. On the basis of such breach of contract, the customer is entitled to claim compensation, both for material loss, such as the misuse of data for fraud or for illegal loans taken out in the customer's name, and for immaterial loss, such as anxiety and reputational damage, which can be measured by the cost of psychological treatment incurred by the customer as a victim (Baidhowi et al., 2025).

The forms of legal protection that currently exist remain very limited and depend on the good faith of the bank. This is due to the legal vacuum, which has not technically regulated the mechanism of personal data transfer from upstream to downstream, so that the available protection still rests on the PDP Law, the Banking Law, and the Indonesian Civil Code in general. The data transfer clauses in banking contracts that have been used so far are merely exoneration clauses that give the bank latitude without adequate transparency obligations toward the customer.

IV. CONCLUSION

Based on the foregoing discussion, two conclusions can be drawn. First, the regulations that form the foundation for personal data transfer in Indonesia remain limited to basic matters, such as the rights and obligations of the parties involved in personal data processing, and do not yet extend in depth to the technical matters required for personal data transfer from upstream to downstream. To date, the limited regulation has been accommodated by using contracts as something that 'binds' the parties involved. However, there is no definitive reference as to which standard clauses must be included in a personal data transfer agreement. In the banking sphere in particular, where standard-form contracts are often used as the basis for personal data transfer agreements, such contracts are insufficient to accommodate 'transparency' toward customers. This is because the personal data transfer clause serves only as an exoneration clause that gives the bank the freedom to determine how and where data will be transferred without further consent from the customer.

Second, as a result of personal data protection regulation that is not comprehensive, the legal protection of customers when personal data is about to be transferred depends on the will of the bank concerned because of the data transfer exoneration clause. Therefore, the legal protection available when data is transferred, even where it is prompted by the urgency of a data breach, is still the legal protection under the PDP Law, the Banking Law, and the Indonesian Civil Code. It cannot be denied that the risk of the customers' data being hacked again at the 'destination' of the transfer may recur.

REFERENCES

1) Adi, R. (2021). *METODOLOGI PENELITIAN SOSIAL DAN HUKUM* (4th ed.). Yayasan Obor.
2) Ashshofa, B. (2004). *Metode Penelitian Hukum*. Rineka Cipta.
3) Baidhowi, Ramadhani, R., & Yudhayana, S. W. (2025). Implementasi Prinsip Kehati-hatian dalam Praktik Kredit Perbankan: Tinjauan Yuridis terhadap Tanggung Jawab Bank. *PENG: Jurnal Ekonomi Dan Manajemen*, *2*(3), 3407–3416. https://doi.org/10.62710/GMCQNV91
4) Hadjon, P. M. (1987). *Perlindungan Hukum bagi Rakyat di Indonesia : Sebuah Studi tentang Prinsip-Prinsipnya, Penanganannya oleh Pengadilan Dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*. Bina Ilmu.

5) *ISO/IEC 27701:2025 - Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*. (n.d.). Retrieved November 2, 2026, from https://www.iso.org/standard/27701?utm_source=google&utm_medium=ppc_paid_social&utm_campaign=ISO27701&utm_content=gads01&gad_source=1&gad_campaignid=23119986168&gbraid=0AAAABtQACE8XY0QbcgM-UYVgITMiUPbF&gclid=CjwKCAjwxpvXBhASEiwAue4B4egLG4xmqI-zRlzjNCR2vP3oKxBAWqvEd3ETQzzWyB37embXYEulExoC690QAvD_BwE
6) Kurniawati, N., Fathurrohman, I., & Roysa, M. (2022). Analisis Semiotika Budaya Jawa Tengah pada Film Mangkujiwo Karya Azhar Kinoi Lubis. *Buletin Ilmiah Pendidikan*, *1*(1), 45–54. https://doi.org/10.56916/BIP.V1I1.217
7) Lesmana[1], R., Irwan, M., & Nasution[2], P. (2025). Kebocoran Data di Media Sosial: Analisis Pola dan Strategi Pencegahannya. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *2*(10). https://doi.org/10.5281/ZENODO.15388529
8) Moleong, L. J. (2018). *Metodologi Penelitian Kualitatif*. PT Remaja Rosdakarya.
9) Rachayu, V., Rani, M., & Hidayat, M. F. (2023). Perlindungan Data Pribadi Pengguna Layanan Pinjaman Online di Indonesia. *Jurnal Studi Ilmu Sosial Dan Politik (Jasispol)*, *3*(2), 89–97. https://doi.org/https://doi.org/10.35912/jasispol.v3i2.2338
10) Rahardjo, S. (2011). Hukum Progresif: Hukum yang Membebaskan. *Jurnal Hukum Progresif*, *1*(1), 1–24. https://doi.org/10.14710/HP.1.1.1-24
11) Risnaldi, O., Toguan, Z., Oemar, A., & Ghifari, A. (2026). Perlindungan Hukum terhadap Investor dalam Kegiatan Penanaman Modal di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *4*(1), 366–380. https://doi.org/10.59246/9P0ARP34
12) Sario, S., Lamangida, T., & Gintulangi, S. L. (2023). Analysis of Good Corporate Governance in Banking Digitalization Transformation in Bank People of Indonesia (BRI) Unit Paguyaman. *Journal of Asian Multicultural Research for Social Sciences Study*, *4*(2), 11–19. https://doi.org/10.47616/JAMRSSS.V4I2.382
13) Suteki. (2018). *Metode Penelitian Hukum Filsafat Teori dan Praktik* (G. Taufani, Ed.). Rajawali Pers.
14) Waluyo, T., Prawesthi, W., & Amiq, B. (2025). PERLINDUNGAN HUKUM TERHADAP INVESTOR PADA INVESTASI. *COURT REVIEW: Jurnal Penelitian Hukum (e-ISSN: 2776-1916)*, *5*(05), 1–25. https://doi.org/10.69957/CR.V5I05.1995
15) Yuspin, W., Wardiono, K., & A Nurrahman. (2023). Personal data protection law in digital banking governance in Indonesia. *Studia Juridica*. https://doi.org/10.17951/sil.2023.32.1.99-130
16) Zahra, R. A., Abdurrahman, L., & Husnoh, A. U. (2024). Perlindungan Hukum Bagi Nasabah Bank Selaku Konsumen Ditinjau dari Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. *Indonesian Journal of Law and Justice*, *1*(4), 9–9. https://doi.org/10.47134/IJLJ.V1I4.2376

There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non-Commercial 4.0 International (CC BY-NC 4.0) (https://creativecommons.org/licenses/by-nc/4.0/), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.