Volume 10, No. 1, 2026

International Journal on Language, Research Law Education Studies
(IJLRES)

Journal Homepage : https://jurnal.uinsu.ac.id/index.php/ijlres/index

E-ISSN 2580-6785
P-ISSN 2580-6777

DOAJ

Reconstruction of Bank Secrecy Legal Liability for the Use of Consent Combined in Bancassurance

Rekonstruksi Pertanggungjawaban Hukum Rahasia Bank Atas Penggunaan Persetujuan Digabungkan Dalam Bancassurance

Salsabila Athamira[1], Sukarmi[2], Patricia Audrey Ruslijanto[3]

[1]Corresponding author: athamiraaa@student.ub.ac.id
[123]Faculty of Law, Brawijaya University, Malang
East Java, Indonesia – 65145

Abstract: The practice of *bundling consent* in *bancassurance* partnerships triggers legal uncertainty and the risk of customer personal data leaks due to the incompleteness of pre-contractual norms in the Banking Law in conjunction with the PPSK Law, which conflicts with the PDP Law. This normative legal research uses a legislative, conceptual, and case-based approach with a qualitative method of legal material analysis. The research findings indicate that the validity of *bundled consent* in standard clauses is conditional because it contains a defect of consent resulting from abuse of circumstances (*misbruik van omstandigheden*). Such bundled consent is null and void as a basis for bank secrecy exceptions unless the business entity provides separate clauses (*granular consent*) and a genuine right to *opt*-out for customers. This study concludes that there is a need to reformulate legal liability through the application of *strict liability* for banks as the primary data controllers and *joint liability* with insurance companies. This reformulation is essential to shift the legal function toward early prevention to ensure the protection of customer privacy.

Keywords: Bank Secrecy; Bundled Consent; Bancassurance; Personal Data Protection; Strict Liability

DOI: 10.47006/ijlres.v%vi%i.29889

INTRODUCTION

Digital transformation is driving the banking sector to innovate through *electronic know your customer* (e-KYC) mechanisms, which involve the processing of large volumes of customer personal data(Silalahi et al., 2025, p. 402). Legally, Article 40 of the Banking Law, as amended by Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (PPSK Law), requires banks to maintain the confidentiality of deposit customer information. However, this obligation may be waived based on the customer's written consent pursuant to

Article 40A(1)(d) of the Banking Law in conjunction with the Financial Sector Development and Strengthening Act (FSDS Act)(Rivaldo & Syailendra, 2024, p. 10661). Sociological and legal issues arise when banks use standard clauses in account opening forms that *bundle* consent for core services with data processing for third parties, such as insurance companies in *bancassurance* schemes. This practice places customers in an unequal position and potentially violates the principles of purpose limitation and data *minimization* mandated by Law No. 27 of 2022 on Personal Data Protection (PDP Law)(Siregar & Putra, 2025, p. 7).

Studies on the relationship between bank secrecy and bancassurance activities have been examined in several previous works, such as the research by Nurhikma, which analyzes bank secrecy regulations in Islamic banks acting as *bancassurance* agents using a normative legal approach and an analysis *of maqashid al-syariah*(Nurhikma, 2025, p. 1). Furthermore, Sjofjan, Antoni, Ardianto, and Charina examined civil law aspects related to the risk of breaching bank secrecy due to the unilateral disclosure of customer phone numbers for the *telemarketing* purposes of insurance companies(Sjofjan et al., 2022, p. 128). Meanwhile, Njoo focuses his analysis on the scope of the bank's liability in marketing activities for Insurance Products Linked to Investments (PAYDI)(Njoo, 2020, p. 130). The commonality among these three studies and this research lies in the overlap of their subject matter, namely customer data protection and the limits on the disclosure of bank secrecy within cross-sectoral collaborations in the financial industry. However, *a gap analysis* reveals a misalignment in legal focus; prior literature tends to be oriented toward resolving the impact of casuistic disputes in practice, fulfilling normative Sharia principles, or liability for the failure of commercial investment products. The novelty of this study lies in its doctrinal focus on testing the validity of *bundled consent* clauses in standard *pre-contractual* agreement forms, followed by a precise reformulation of the allocation of legal liability between banks and insurance companies under the integrated framework of the Personal Data Protection Act (PDP Act) and the Insurance Act (PPSK Act).

The urgency of this research is based on the existence of *an "incomplete* norm" in the Banking Law in conjunction with the PPSK Law, which does not explicitly regulate the form, limitations, and standards of customer consent when given in the form of bundled standard clauses. The absence of such clear regulations results in blurred lines of legal liability in the event of misuse or leakage of customer data. Consequently, legal uncertainty arises regarding whether full liability rests with the bank as the party collecting and transferring the data, or with the insurance company as the data processor. If left without clarity *under ius constituendum*, this situation not only causes massive financial losses for customers as data

subjects but also undermines the pillar of public trust that serves as the core of the national banking industry.

Based on this background, the legal issue at the center of this study is whether the use of *bundled consent* in the collaboration between banks and insurance companies can be justified as the basis for an exception to bank secrecy? Furthermore, how should the legal liability framework for the use of bundled consent as a basis for the bank secrecy exception in bank-insurance collaborations be reformulated to provide balanced legal protection for customers?

This study aims to critically and thoroughly analyze the validity of using bundled consent in *bancassurance* collaborations as a justification for the bank secrecy exception. Additionally, this study is directed toward identifying and formulating a precise and accountable reformulation of the legal liability framework among the parties to provide legal certainty and protection for depositors against the risk of misuse of personal data.

This study employs a normative legal research methodology (*Normative Legal Research*)(Rizkia & Fardiansyah, 2023, p. 120) to examine and analyze applicable positive legal norms regarding legal liability for the use of *bundled consent* as the basis for an exception to bank secrecy in collaborations between banks and insurance companies. The analysis focuses on provisions regarding bank secrecy obligations, exceptions based on customer consent, as well as regulations on customer data protection and consumer protection in the financial services sector to identify gaps in existing legal norms. The research approaches employed include *the statutory approach* to examine regulations related to these legal issues, the *conceptual approach* to understand the legal doctrines and concepts underpinning the research, and *the case approach* by analyzing various concrete cases that have occurred in practice(Nur Solikin, 2021, p. 59).

The legal sources used include primary legal materials derived from legislation, namely the Civil Code, Law No. 10 of 1998 on Banking, Law No. 8 of 1999 on Consumer Protection, Law No. 27 of 2022 on Personal Data Protection, Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, Financial Services Authority Regulation No. 44 of 2024 on Bank Secrecy, and *the General Data Protection Regulation* (GDPR). These primary legal sources are supported by secondary legal sources such as legal textbooks, scientific journals, and previous research findings, as well as tertiary legal sources in the form of legal dictionaries and encyclopedias collected through documentation and literature review techniques. The analysis of legal materials was conducted by grouping the collected legal materials, then analyzed qualitatively using the grammatical interpretation method, to

explain the literal meaning and scope of the norms, as well as systematic interpretation to understand the interrelationships between legal regulations in order to construct a comprehensive legal framework for the liability of the parties within the *bancassurance* scheme.

RESULTS AND DISCUSSION

The Validity of Using Bundled Consent as the Basis for Bank Secrecy Exceptions

An analysis of the doctrinal validity of *bundled* consent in *bancassurance* cooperation schemes requires a comprehensive understanding of the typology of circular legal relationships that exist between customers, banks, and insurance companies(Kosasih & Haykal, 2021, p. 21). Contractually, the initial relationship stems from the account opening agreement, which positions the customer as the creditor (depositor) and the bank as the debtor, based on *a fiduciary relationship*(Kothary & Negi, 2025). This relationship imposes an *implied* legal obligation on the bank to strictly uphold bank secrecy. However, the modern intermediary structure through *bancassurance* agreements expands the transmission of customer data for commercial purposes, such as risk *profiling* in the marketing of insurance products (Gultom, 2024, p. 208).

To map the conflicts in consent validity standards across the various legal regimes governing this hybrid practice, the following normative parameters provide a substantial comparison:

Table 1: Comparison of Parameters for the Validity of Customer Data Consent Based on Legal Regimes.

Legal Regime	Legal Basis	Key Characteristics of Consent	Implications for Bundled Consent
Banking Law	Article 44A(1) of the Banking Law	Written formality without rigid substantive restrictions	Deemed formally valid as long as it is set forth in a written document/standard clause.
Consumer Protection	Section 18 of the Consumer Protection Act (UUPK)	Prohibition of standard clauses that exacerbate an imbalance in bargaining power or shift liability.	Void ab initio if containing an exculpatory clause or disguised in a form that is difficult to understand.

Personal Data Protection	Article 20(2)(a) of the Personal Data Protection Act	Valid only if explicitly stated, limited, specific, transparent, and based on informed consent for a specific purpose.	Invalid if it does not provide the option of separate consent and the right to opt out.
Global Standards (GDPR)	Article 7 & Recitals 43 of the GDPR	Freely given, specific, informed, unambiguous, and must be easily withdrawable.	Deemed non-binding if the combination eliminates the freedom to choose independently.

Source: *Analyzed from primary sources.*

The misalignment between secular banking regulations and contemporary data protection stems from a paradigm shift from formal freedom *of contract* toward substantial contractual justice. Banks often use the principle of the binding nature of contracts (*pacta sunt servanda*) under Article 1338(1) of the Civil Code to legitimize *bundled consent*. Through the mass signing of account opening forms, consent to waive bank secrecy is claimed to have fulfilled the principle of consensualism.

However, doctrinally, this formal validity is substantively flawed due to the existence of abuse of circumstances (*misbruik van omstandigheden*) structured digitally(Kristiyani, 2020, p. 5). This imbalance is triggered by two main factors:

- Extreme Information Asymmetry: Banks have full control over the technological ecosystem, data distribution flows, and cross-sector commercial processing objectives. Conversely, customers are presented only with promotional information without explicit explanations regarding the risks of privacy breaches or the processing of their specific financial data by third parties.
- Structural Dependency: Digital banking services have evolved into a primary necessity for the public's daily financial and administrative activities. This situation forces customers into a "*take it or leave it*" position, where they are compelled to agree to commercial data disclosure clauses in order to gain access to core banking services(Alamsyah et al., 2025, p. 957).

This disparity justifies the strict intervention of Article 18(1)(a) and (2) of the Consumer Protection Law (UUPK), which prohibits the inclusion of standard clauses that shift the legal liability of business operators or are presented in a format that obscures consumer

understanding(Indonesia, Pemerintahan Pusat, 1999). The performance of a contract must be subject to the principle of objective good faith (Article 1338(3) of the Civil Code), which demands radical transparency(Syamsuddin, 2026, p. 1416).

When assessed against the parameters of Article 20 of the Personal Data Protection Act, the bank's role shifts to that of a Personal Data Controller, which is required to comply with the principle *of data minimization*. The disclosure of customers' telephone numbers or financial histories to insurance companies for the purpose *of* commercial marketing *profiling* is not part of the fulfillment of the primary banking contract. Consequently, bundling such consent without a standalone opt-out option effectively undermines the principle of contractual proportionality and reduces the data subject's right to autonomy. Article 23 of the Personal Data Protection Act (PDP Act) explicitly states that contractual clauses involving the processing of personal data without separate valid consent are null and void(Afrilia et al., 2026, p. 5644) .

The conceptualization of "conditional validity" in this study complements and corrects several analytical shortcomings in the prior legal literature to address whether the use of bundled consent can be justified as a basis for the bank secrecy exception. Nurhikma's (2025) study, which examines the activities of Islamic banks as *bancassurance* agents, relies on an analysis *of maqashid al-sharia* to emphasize that the sharing of customers' personal data without consent violates the principles of *hifz al-mal* (protection of wealth) and *hifz al-'ird* (protection of privacy/dignity). Although Nurhikma asserts that customer protection is guaranteed through the principles *of confidentiality*, *prudence, and trust*, the focus of her study lies at the macro-regulatory level following the PPSK Law and agency contracts based on the *Wakalah bil Ujroh* agreement. The study has not specifically examined the *pre-contractual* validity of the mechanism for combining consent in the standard clauses of account opening forms.

On the other hand, the research by Lindryani Sjofjan et al. (2022) limits its analysis to civil law aspects related to customer complaints arising from their phone numbers being provided to third parties for the insurance company's telemarketing purposes without explicit consent. The civil law solutions proposed by Sjofjan et al. are *case-specific and operational* in practice, namely by asking prospective customers for their consent during account opening or through coordination with *the bank's relationship manager*. This approach has not addressed the fundamental issue regarding the doctrinal validity of bundled consent clauses under the contemporary data protection legal regime. Meanwhile, the study by Cindy Indudewi Hutomo Njoo (2020) focuses separately on the realm of *the* bank's civil *liability* arising from

investment failure risks in the marketing of PAYDI (*unit-linked bancassurance*) products after the contract is concluded.

Unlike the three studies mentioned above, this research explicitly addresses the question: "Can the use of bundled consent in a collaboration between a bank and an insurance company be justified as a basis for the bank secrecy exception?" by demonstrating that the use of *bundled consent* in *bancassurance* collaborations cannot automatically be justified as a basis for the relative bank secrecy exception. The alignment between Article 44A of the Banking Law, which requires written formality, and Article 20(2)(a) of the Personal Data Protection Law, which demands explicit, specific, and transparent consent, leads to the conclusion that *bundled consent* in standard clauses contains a defect of consent due to the abuse of circumstances (*misbruik van omstandigheden*).

Therefore, its validity is conditional; *bundled consent* is null and void and cannot serve as a basis for the disclosure of bank secrecy unless the financial services provider cumulatively provides a separate clause (*separate consent*), is transparent regarding the data processor, and grants customers a genuine right to *opt* out without hindering access to core banking services.

Reformulation of Legal Liability for the Use of Bundled Consent in Bancassurance Cooperation

Bancassurance cooperation mechanisms that use *bundled consent* as the basis for an exception to bank secrecy have serious implications for the increased risk of customer data dissemination and misuse. To map how these violations occur in practice and how legal rules are currently applied in a repressive manner, the typology of data dispute cases in the national financial industry can be identified through the following operational instruments:

Table 2: Typology of Customer Data Misuse Cases and Patterns of Legal Violations

No	Dispute Case / Ruling	Patterns of Data Misuse	Violations of Contemporary Regulations	Impact / Customer Losses
1	BNI vs. BNI Life & Cigna Insurance (Bireuen District Court & Banda Aceh District Court)(Bahagia et al., 2019, p. 18).	Exploitation of customer data through telemarketing methods without explicit and separate confirmation.	Article 40(1) and Article 44A of the Banking Law; Article 4 of the Consumer Protection Law; Articles 16 and 20 of the Personal Data Protection Law.	Unwanted calls (unsolicited calls) and unilateral premium deductions via auto-debit.
2	Mr. Z v. Bank Mandiri & PT AXA	Institutional disclosure of phone	Defects in the pre-contractual	The customer's salary is

	Mandiri(Winda, 2017, p. 1528).	numbers; verbal manipulation of the word "yes" in telemarketing speed dials.	agreement (Article 1320 of the Civil Code); Breach of the bank's fiduciary duty.	automatically deducted by Rp500,000 each month without their full knowledge.
3	Samsuduri v. Bank Mandiri Wiyung Branch (Judgment No. 615/Pdt.G/2023/PN Sby)(Indonesia, 2023).	Leak of internal database by a bank employee; dissemination of a computer screenshot containing CIF and mother's maiden name to a public group.	Failure to protect the confidentiality and integrity of personal data (Article 46(1) of the Personal Data Protection Act).	Immaterial losses; extreme financial cyber threats (fraud) resulting from the leak of core security variables.

Source: Analyzed from primary sources.

Transactional relationships in *bancassurance* have fundamentally distorted the pillar *of the fiduciary relationship*, wherein the bank, as the party entrusted with full confidence (*fiduciary*), is obligated to prioritize the customer's interests over the corporate business interests. Through the *bundling consent* mechanism, there has been a shift in the normative function of Article 44A of the Banking Law. Written consent, which was essentially designed as *a protective tool* for deposit customers to prevent their data from being disclosed indiscriminately, has instead been manipulated by banks into *a legitimizing tool* to mass-distribute " " for the sake of pursuing *fee-based income*(Karwati et al., 2024, p. 102). This pattern reduces the legal status of customers from being *the served* party to merely a commodity or *a commercial data source* whose economic value is exploited without commensurate compensation.

When analyzed using the framework of the Personal Data Protection Act (PDP Act), the invalidity of this *bundled consent* rests on systematic violations of the four absolute requirements for explicit consent under Article 20, as well as the principle *of purpose limitation* under Article 16(c). Banks act as Data *Controllers* because they control the information from the outset and determine the direction of data-sharing policies(Indonesia, Pemerintah Pusat, 2022). Meanwhile, insurance companies occupy a hybrid position; they act as *Data Processors* when processing data at the bank's instruction for initial marketing, but immediately transition into *Joint Controllers* when executing external commercial strategies, managing policy portfolios, and debiting accounts independently(European Data Protection Board, n.d.).

The incorporation of commercial insurance consent into the core banking account opening administrative documents structurally undermines the principles *of fairness and transparency*(Rizki, 2022) . Data submitted by customers for the purpose of savings management is unlawfully diverted for third-party commercial purposes that customers never anticipated during *the pre-contract phase*. Because the documents are presented in *a "take it or leave it"* format without an opt-out clause (*opt-out by default*), this formal consent loses its moral and legal validity as it is obtained under the structural pressure of the public's need for financial access.

The reality of law enforcement in current banking data disputes reveals massive weaknesses stemming from reliance on traditional civil law based on *fault-based liability*. This weakness is paradoxically reflected in *Judgment No. 615/Pdt.G/2023/PN Sby*, where the panel of judges rejected the defendants' exceptions but simultaneously dismissed the plaintiff's civil claim in its entirety, even though the fact of a data breach involving sensitive information specifically CIF numbers and mothers' maiden names by an internal employee had been clearly proven in court(Wartapos, 2023). If the plaintiff seeks damages for an unlawful act (PMH) under Article 1365 of the Civil Code or for breach of contract under Article 1234 of the Civil Code, the burden of proving the element of fault rests on the customer. This is highly unfair given that customers structurally lack the technical capability to access digital evidence, encryption systems, or banking database audit logs.

This situation stems from *an "incomplete* norm" in Article 44A of the Banking Law, which merely requires "written consent" in *a formal, textual sense* without establishing standards for the validity of such consent, does not prohibit bundling practices, and does not provide a *rigid* right to revoke consent. Therefore, a radical reformulation of legal liability is required through the adoption of two contemporary legal doctrines:

- *Strict Liability* for Banks: The nature of liability must shift from fault-based to strict liability in order to provide optimal preventive protection. Banks, as data controllers who are most aware of how, when, and through which security systems the data is managed, must be directly liable for any failure to protect customers' personal data, without the need to prove the presence or absence of fault or negligence (*onrechtmatige daad*). A standard consent form that is flawed from the outset should no longer be used as *an* exoneration clause to release the bank from legal liability.

- Cross-Sector Joint *Liability*: To prevent the practice of shifting blame between banking institutions and their insurance partners, both entities must be positioned as legal entities jointly bearing joint and several liability for data processing compliance. Insurance companies are *active beneficiaries* of bank customers' commercial data; if they use databases obtained through flawed *consent* mechanisms, they bear absolute liability for any resulting financial or non-financial losses.

If the provisions of the Personal Data Protection Act (PDP Act) are consistently applied as a *lex specialis* overriding *the lex generalis* of traditional banking law, the sanctions imposed will no longer be limited to civil damages of fluctuating value. Pursuant to Article 67(2) in conjunction with Article 70 of the PDP Law, banks that allow internal database breaches or rely on illegal *consent bundling* should be subject to maximum administrative fines, including tiered fines for example, up to Rp40 billion as well as additional sanctions such as the suspension or revocation of their business licenses. This reformulation compels the financial services industry to strictly apply the principle of absolute consent separation (*unbundling consent*) from the pre-contract phase, thereby shifting the function of legal accountability from merely punishing after the fact (*repressive*) to an early prevention system (*preventive*) that guarantees the protection of privacy as a fundamental right of customers.

CONCLUSION

The use of bundled *consent* in *bancassurance* collaborations between banks and insurance companies cannot be automatically justified as a basis for the relative bank secrecy exception. Based on the synchronization and doctrinal validity testing under the integration of the Personal Data Protection Act (PDP Act), the Consumer Protection Act (UUPK), and the Civil Code (KUH Perdata), the validity *of bundled consent* in standard account opening clauses is deemed to be vitiated by a defect of consent due to the existence of abuse of circumstances (*misbruik van omstandigheden*), thereby rendering its legal force conditional. This consent bundling mechanism is declared null and void and loses its validity as an instrument exempting bank secrecy unless the financial services provider cumulatively provides separate consent clauses (*separate/granular consent*), transparency regarding the identity of the data processor, and a genuine right to *opt*-out without hindering the customer's access to core banking services. Due to the existence of *an "incomplete* norm" in pre-contractual provisions within traditional banking law that obscures lines of accountability, the reformulation of legal liability must be directed toward a paradigm shift toward the application of *strict liability* for

banks and *joint liability* between banks and insurance companies. As the primary *Data Controller*, the bank bears full responsibility for any failure in data protection or customer data breaches without the need to prove the elements of conventional civil tort (*onrechtmatige daad*). On the other hand, insurance companies, as *joint controllers* and active commercial *beneficiaries*, also bear strict civil liability as well as tiered administrative fines if they utilize customer databases derived from legally flawed consent mechanisms.

REFERENCE

1) Afrilia, E. T., Trijaya, M. W., Ariani, N. D., Septiana, D., & Mustika, D. (2026). Validitas Clickwrap Agreement dalam Transaksi E-Commerce Menurut KUHPerdata dan Undang-Undang Pelindungan Data Pribadi. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *4*(3), 5639–5645. https://doi.org/10.61104/alz.v4i3.6186

2) Alamsyah, G. N., Sudirman, Hamzah, I. F., & Umar, W. (2025). Analisis Hukum Terhadap Keabsahan Klausula Baku dalam Kontrak Financial Technology (Fintech). *Jurnal Ilmu Hukum, Humaniora Dan Politik*, *5*(2), 955–971. https://doi.org/10.38035/jihhp.v5i2.3239

3) Bahagia, B., Rahayu, S. W., & Mansur, T. M. (2019). Perlindungan Data Pribadi Nasabah Dalam Penawaran Transaksi Asuransi Oleh PT.Bank Negara Indonesia (Persero). *Syiah Kuala Law Journal*, *3*(1), 18–34. https://doi.org/10.24815/sklj.v3i1.12108

4) European Data Protection Board. (n.d.). *Data controller or data processor*. Retrieved May 26, 2026, from https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en

5) Gultom, E. (2024). Konteks Hubungan Hukum Dan Pelindungan Konsumen Dalam Pemasaran Produk Asuransi Melalui Bancassurance. *Jurnal Yuridis*, *11*(2), 199–215. https://doi.org/10.35586/jyur.v11i2.9088

6) Indonesia, M. A. R. (2023). *Putusan 615 PDT.G 2023 PN Sby 20260301162057*. Scribd. https://id.scribd.com/document/1005778651/putusan-615-pdt-g-2023-pn-sby-20260301162057

7) Indonesia, Pemerintah Pusat. (2022). *Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Database Peraturan | JDIH BPK. http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

8) Indonesia, Pemerintahan Pusat. (1999). *Undang-undang (UU) Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*. https://peraturan.bpk.go.id/Details/45288/uu-no-8-tahun-1999

9) Karwati, K., Hardyansah, R., & Saktiawan, P. (2024). Legal Analysis of Open Banking and Bank Customer Data Privacy Rights in Indonesia. *Journal of Social Science Studies*, *4*(1), 93–104. https://jos3journals.id/index.php/jos3/article/view/295

10) Kosasih, J. I., & Haykal, H. (2021). *Kasus Hukum Notaris di Bidang Kredit Perbankan*. Sinar Grafika. https://books.google.co.id/books?id=O-QhEAAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false

11) Kothary, M., & Negi, A. M. N. (2025). *Understanding the legal relationship between a banker and a customer in India: Challenges arising from the debtor and creditor relation*. (SSRN Scholarly Paper No. 5626790). Social Science Research Network. https://doi.org/10.2139/ssrn.5626790

12) Kristiyani, C. T. S. (2020). Consumer legal efforts due to abuse of circumstances (Misbruik Van Omstandigheden) in standardized agreements. *NOTARIIL Jurnal Kenotariatan*, *5*(1), 1–7. https://doi.org/10.22225/jn.5.1.1729.1-7

13) Njoo, C. I. H. (2020). *Tanggung Gugat Bank pada Aktivitas Bancassurance terhadap Pemasaran Produk Asuransi yang Dikaitkan dengan Investasi (PAYDI)* [Thesis, Universitras Airlangga]. http://www.lib.unair.ac.id

14) Nur Solikin. (2021). *Pengantar Metodologi Penelitian Hukum*. Qiara Media.

15) Nurhikma, N. (2025). *Pengaturan Rahasia Bank Dalam Aktivitas Bank Syariah Sebagai Agen Bancassurance* [4Doktoral, Universitas Andalas]. http://scholar.unand.ac.id/502603/

16) Rivaldo, A., & Syailendra, M. R. (2024). Tanggung Jawab Penyedia Layanan Perbankan Terhadap Penyalahgunaan Data Nasabah Berdasarkan Pasal 46 Ayat 1 UU PDP (Kasus Putusan 615/Pdt.G/2023/Pn surabaya). *UNES Law Review*, *6*(4), 10658–10665. https://doi.org/10.31933/unesrev.v6i4.2045

17) Rizki, M. J. (2022). *POJK 6/2022 Larang Telemarketing Produk Jasa Keuangan Tanpa Persetujuan Konsumen*. hukumonline.com. https://www.hukumonline.com/berita/a/pojk-6-2022-larang-telemarketing-produk-jasa-keuangan-tanpa-persetujuan-konsumen-lt6287737ca5230/

18) Rizkia, N. D., & Fardiansyah, H. (2023). *Metode Penelitian Hukum (Normatif Dan Empiris)*. Penerbit Widina. https://www.google.co.id/books/edition/METODE_PENELITIAN_HUKUM_NORMATIF_DAN_EMP/2X1JEQAAQBAJ?hl=id&gbpv=0

19) Silalahi, B. B. S., B, B., & Novita, Y. D. (2025). Aspek Hukum Dalam Penerapan Prinsip Know Your Customer (KYC) Pada Lembaga Perbankan. *Media Hukum Indonesia (MHI)*, *3*(2). https://doi.org/10.5281/zenodo.15552061

20) Siregar, A. N., & Putra, M. A. P. (2025). Kajian Hukum: Penegakan Perlindungan Data Pribadi Nasabah Bank Dalam Skema Bancassurance. *Jurnal Media Akademik (JMA)*, *3*(7). https://doi.org/10.62281/v3i7.2533

21) Sjofjan, L., Antoni, H., Ardianto, E., & Charina, D. A. (2022). Aspek Hukum Perdata Rahasia Bank Berkaitan Dengan Referensi Data Nasabah Bank Kepada Perusahaan Asuransi (Diteliti di Bank Muamalat Kantor Cabang Bengkulu Curup). *PALAR (Pakuan Law Review)*, *8*(4), 115. https://doi.org/10.33751/palar.v8i4.6621

22) Syamsuddin, A. F. (2026). Relationship Between Hospitals And Doctors Based On The Principle Of Justice. *JURNAL USM LAW REVIEW*, *9*(3), 1416–1437. https://doi.org/10.26623/julr.v9i3.14193

23) Wartapos. (2023). Bank Mandiri Mangkir di Sidang Gugatan Kebocoran Data Nasabah. *Wartapos*. https://www.wartapos.id/2023/07/25/bank-mandiri-mangkir-di-sidang-gugatan-kebocoran-data-nasabah/

24) Winda, N. (2017). Perlindungan Hukum Terhadap Nasabah Bank Dalam Sistem Bancassurance. *CALYPTRA*, *6*(1), 1528–1544. https://journal.ubaya.ac.id/index.php/jimus/article/view/3474