Legal Analysis of Open Banking and Bank Customer Data Privacy Rights in Indonesia

Karwati, Rommy Hardyansah, Pratolo Saktiawan

Universitas Sunan Giri Surabaya, Indonesia

ARTICLE INFO

Article history:
Received 21 October 2023
Revised 11 December 2023
Accepted 21 December 2023

Key words:
Open banking,
Customer data privacy,
Digital banking,
Personal data protection,
Banking API,
Financial regulation,
Business law.

ABSTRACT

The development of digital finance has encouraged the implementation of open banking as a mechanism for sharing bank customer data through application programming interfaces (APIs) between financial institutions and third parties. In Indonesia, this development intersects with the strengthening of personal data protection through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Bank Indonesia Regulations concerning Data and Information Policy, and various Financial Services Authority (OJK) regulations concerning digital financial services and fintech. This study aims to analyses open banking regulations from the perspective of bank customer data privacy rights using a normative juridical method based on a literature review of legislation and the latest academic literature. The results of the analysis show that the PDP Law provides a general foundation through the principles of lawfulness, fairness, and transparency, while also guaranteeing customers, as data subjects, the rights of access, correction, deletion, and objection. At the sectoral level, Bank Indonesia regulations on data and information policy govern banking data governance, security standards, and support for digital innovation, while OJK regulations emphasize consumer protection and risk management in the use of customer data by fintech players. Theoretically, this combination of regulations can support the implementation of open banking in line with modern data protection principles, as long as the division of roles between banks, technology service providers, and regulators is clearly defined. This study concludes that the effectiveness of customer privacy protection in open banking schemes is greatly influenced by the implementation of explicit consent, clarity of opt-in and opt-out mechanisms, API design that applies data minimization and accountability, and consistent monitoring and sanctions for data breaches. The main recommendations of the study are the need for joint guidelines between authorities, strengthening technical standards and data compliance audits, and improving customer data literacy so that the rights granted by the PDP Law and sectoral regulations can be effectively implemented in digital banking practices.

INTRODUCTION

Digital transformation in the financial services sector is changing the way banks manage data, provide services, and interact with customers. In Indonesia, banking, which was previously oriented towards closed services, is now moving towards a more open model with the use of application programming interfaces (APIs) that connect banks with other financial service providers, including fintech and technology companies. The effectiveness of personal data protection regulations in the face of this sectoral transformation has become an important concern, as discussed in the study by Aziz et al. (2023), which examines the implementation of the PDP Law in the fintech sector—a context that has similar challenges related to data openness and information security.

The shift towards a more open financial ecosystem raises new considerations regarding industry competition and consumer trust, aspects that are also analyzed in the study by Hardyansah et al. (2021). This trend is inseparable from global developments that place data as a strategic asset and encourage the emergence of the open banking model as a framework for sharing customer financial data in a structured and standardized manner. On the one

** Corresponding author, email address:* ***dr.pratolosaktiawan@gmail.com***

hand, these developments support innovation, business competition, and the expansion of financial inclusion; on the other hand, there are concerns about personal data protection, information misuse, and bargaining power imbalances between banks, third parties, and customers (Nathania et al., 2023).

At the global level, various legal regimes are attempting to develop regulatory designs that balance data openness and privacy rights protection. The experience of European jurisdictions with the General Data Protection Regulation (GDPR) is often used as a reference when discussing the relationship between personal data rights and the use of data for financial innovation. Greenleaf points out that countries in Asia are developing a variety of approaches to data protection with varying degrees of intervention and enforcement, although there is a trend towards convergence towards stronger standards for data subject rights (Greenleaf, 2014). These dynamics influence how countries, including Indonesia, formulate legal restrictions on the processing of financial data, the transfer of data to third parties, and customers' rights to control their banking information (Amalia, 2022).

The entry of financial technology and non-bank actors has driven a shift in the structure of the financial services market, which for decades has been dominated by traditional banking institutions. Nicoletti asserts that the integration of technology into financial services has given rise to a new ecosystem characterized by modular architecture, the use of APIs, and intensive collaboration between banks and technology providers (Nicoletti, 2017). The entry of financial technology and non-bank actors has driven a shift in the structure of the financial services market, which for decades has been dominated by traditional banking institutions. Nicoletti asserts that the integration of technology into financial services has given rise to a new ecosystem characterized by modular architecture, the use of APIs, and intensive collaboration between banks and technology providers (Nicoletti, 2017). The importance of security and reliable data management principles in this complex digital ecosystem is also illustrated by Costa et al. (2023) in the context of employee data protection, where technologies such as blockchain are proposed to create auditable transparency and data security principles that can be adapted to strengthen data governance in open banking. In such an ecosystem, open banking is often positioned as a prerequisite for realizing more personalized, interoperable, and efficient financial services. However, the open nature of this architecture has the potential to create new vulnerabilities when customer consent mechanisms, data processing security, and legal liability for information leaks are not explicitly regulated (Hermawan et al., 2023). The question of who has ultimate control over financial data is an important issue that requires careful legal consideration.

In Indonesia, policies regarding customer data and bank secrecy have long been regulated through banking and bank secrecy provisions, while the issue of personal data protection has gained a more explicit basis with the enactment of Law No. 27 of 2022 on Personal Data Protection. At the same time, financial and monetary authorities, including the Financial Services Authority (OJK) and Bank Indonesia, have begun to promote API standardization and the development of open banking as part of the financial system digitalization agenda. The importance of an ethical approach and responsible governance in the development of this financial system is also outlined by Putra et al. (2022), who emphasize the importance of balancing innovation and the protection of stakeholder rights, including customer privacy rights. This shift has created normative tensions between bank secrecy, the obligation of data transparency for innovation, and the recognition of customer data privacy rights as part of human rights. Therefore, a legal analysis of open banking regulations and bank customer data privacy rights in Indonesia is an important academic and practical necessity to map the compatibility between financial innovation policies and the protection of data subjects' rights (Yuliana & Maulana, 2023).

The first issue lies in the potential disharmony between the various legal regimes governing customer financial data. Banking laws recognize the concept of bank secrecy, which limits the disclosure of customer information, while regulations promoting the digitization of services and system connectivity require the exchange of data between institutions. On the one hand, the push for open banking leads to the use of data to build risk profiles, alternative credit rating services, and integration with e-commerce platforms; on the other hand, privacy rights demand clear restrictions on the collection, use, and disclosure of data. A regulatory gap arises when there are no comprehensive standards regarding the form of consent, revocation mechanisms, and the limits of liability of banks and third parties for losses due to misuse of customer data.

The second issue relates to the normative basis of bank customer data privacy rights within the Indonesian legal framework. In various literature, the right to personal data protection is often

associated with the right to privacy and the right to individual information autonomy. Wachter and Mittelstadt point out that personal data regulation in the era of big data requires strengthening the rights of data subjects to control the processing and inference made about them (Wachter & Mittelstadt, 2019). In the banking sector, the processing of customer data for the purposes of risk profiling, product offerings, and cooperation with digital partners often takes place beyond the scope of customer understanding. This raises the question of whether the rights recognized by national law, such as the right of access, the right to rectification, the right to erasure, and the right to object, are sufficient to protect customers when their data circulates in the open banking ecosystem (Nathania et al., 2023).

The third issue concerns the power relations between financial institutions, technology providers, and customers. Omarova states that the development of financial technology has the potential to shift the center of power from traditional financial institutions to large technology entities that control data and algorithms, thereby posing new risks to the stability and fairness of the financial system (Omarova, 2020). In open banking arrangements, third-party access to customer financial data is often packaged as an expansion of choice and personalization of services, while customers' bargaining position in negotiating data processing terms is relatively limited. When regulations do not explicitly place customers as the owners or primary controllers of data, there is a risk that open banking will become a mechanism for legalizing the exploitation of customer data with disproportionate benefits for the individuals whose data is being processed.

The development of national regulations that lead to the strengthening of personal data protection, along with the acceleration of the digitalization of banking services, makes the intersection between open banking and privacy rights a highly relevant theme for business law studies. The implementation of the Personal Data Protection Law, financial authority policies on system digitalization and integration, and the increasing use of fintech services connected to customer bank accounts necessitate a systematic review of the existing regulatory structure. Without adequate review, there is a risk that policies designed to encourage financial innovation will instead place customers in a vulnerable position to confidentiality breaches and data misuse. A legal analysis of open banking regulations is key to assessing whether existing legal instruments are capable of keeping pace with technological dynamics and industry practices.

In addition, global dynamics regarding open banking regulations and data protection show that countries are exploring various policy models, ranging from a regulatory mandate-based approach to an industry agreement-based approach. Indonesia needs to determine a direction that is in line with the characteristics of its legal system, banking industry structure, and the level of digital literacy among its people. An examination of open banking regulations and customer data privacy rights helps identify principles that should serve as references, such as transparency, fairness of processing, accountability, and strengthening the position of customers as data owners. Thus, this study can provide an analytical framework for policymakers, industry players, and academics to assess whether existing regulatory developments are adequate or need to be refined.

This study aims to legally analyses open banking regulations in Indonesia by placing the privacy rights of bank customers as the main focus. Theoretically, this study is expected to enrich the study of business law and personal data law by showing how the concepts of bank secrecy, personal data protection, and financial service innovation interact in practice. Practically, this research is expected to provide input for policymakers and supervisory authorities in formulating or refining regulations related to open banking, so that the protection of bank customer data privacy rights can be guaranteed without hampering innovation and healthy business competition in the financial services sector.

RESEARCH METHOD

This study uses a normative juridical method with an emphasis on literature studies focusing on primary, secondary, and tertiary legal materials. The normative juridical approach was chosen because the main objective of the study is to interpret, construct, and evaluate legal norms governing open banking and bank customer data privacy rights in the Indonesian legal system. Primary legal materials consist of laws and regulations in the fields of banking, personal data protection, payment systems, and financial sector authority regulations related to the use of API-based data and services. Secondary legal materials include books, journal articles, and academic reports that describe the theories of privacy rights, data protection, banking law, and financial data governance. A qualitative approach was used in reading and interpreting legal texts, in line with Creswell's view that qualitative research relies on the interpretive process of the meaning contained in documents and discourse (Creswell, 2014).

The strategy for collecting legal materials and academic literature was carried out through searching electronic databases and official sources. Legal materials were obtained from official government websites and financial sector authorities, while academic literature was searched for through reputable journal databases such as HeinOnline, JSTOR, SSRN, and international publisher portals. This procedure is in line with Snyder's view on the importance of formulating a systematic search strategy in literature reviews, including determining keywords, publication year limits, and eligibility criteria to ensure that the sources used are relevant and up-to-date (Snyder, 2019). The inclusion criteria for academic literature included: (1) published between 2000 and 2024, (2) discussing personal data protection, open banking, fintech, or legal research methodology, and (3) published by reputable publishers or journals. Exclusion criteria were applied to popular writings, non-academic opinions, and sources whose validity could not be verified through DOI or ISBN.

Data analysis was conducted through the stages of reduction, categorization, and compilation of findings within a thematic framework linked to the problem formulation. The document analysis technique followed Bowen's guidelines, which emphasize the process of selection, reading, coding, and interpretation of document content as the basis for drawing qualitative conclusions (Bowen, 2009). Legal materials and literature were coded into categories such as: normative basis of privacy rights, bank secrecy regulations, personal data protection regulations, open banking policies, and the responsibilities of parties processing customer data. To maintain consistency and traceability, the analysis steps followed the recommendations of Miles, Huberman, and Saldaña regarding the coding cycle, the creation of analytical memos, and the preparation of a matrix linking legal issues with norms and doctrinal arguments (Miles, Huberman, & Saldaña, 2014). The validity of the arguments is maintained through the triangulation of legal materials and academic literature, as well as testing the logical coherence between the results of the interpretation of norms and the general principles of human rights protection and data governance.

RESULT AND DISCUSSION

Open Banking Regulations in Indonesia from the Perspective of Bank Customer Data Privacy Rights

The implementation of open banking is commonly understood as a regulatory design that requires or encourages banks to open access to account data and payment services to third parties through standard APIs, with the consent of customers. The experience of the European Union through Payment Services Directive 2 (PSD2) is often used as a reference because it regulates new categories of service providers, such as account information service providers and payment initiation service providers, which obtain access rights to customer data based on explicit consent. This paradigm shift towards a data-driven economy is also reflected in Wahyudi et al.'s (2021) analysis of the impact of big data on social life, which shows that policies and regulatory frameworks need to adapt to the new reality where data has become a strategic commodity and a source of innovation. Zetzsche, Buckley, Arner, and Barberis assert that PSD2 represents a shift from exclusive protection of bank secrecy towards a "data-driven finance" model based on data portability and licensed third-party access rights (Zetzsche et al., 2020). If such a framework is adapted to Indonesia, the main question that arises is how to position customer data privacy rights as a parameter when banks are required to provide data access through APIs, and to what extent customer consent can serve as a legal basis for legitimate data processing.

The transformation towards data-driven finance cannot be separated from changes in the global financial industry structure. Arner, Barberis, and Buckley describe how fintech, following the 2008 global financial crisis, developed as a new paradigm that combines technological innovation, disintermediation, and large-scale data utilization across the financial services value chain (Arner, Barberis, & Buckley, 2016). Within this framework, banking transaction data is viewed as raw material for product development, risk assessment, and service personalization. The open banking regulations in Indonesia, although not as comprehensive as PSD2, are moving towards a similar logic as regulators push for API standardization and payment system integration with various service providers (Amalia, 2022). This has legal consequences, as the protection of customer privacy rights is no longer measured solely by the confidentiality of communications between banks and customers, but also by how the data is transferred, processed, and used by a much broader ecosystem of actors.

Buchak, Matvos, Piskorski, and Seru show that differences in regulatory regimes can encourage fintech and non-bank institutions to engage in regulatory arbitrage, taking advantage of looser oversight compared to traditional banks (Buchak et

al., 2018). This finding is relevant to open banking regulations in Indonesia because third-party access to customer data may involve entities that are outside the framework of traditional banking supervision (Nathania et al., 2023). If the authorities only regulate the obligations of banks as API providers, while the data governance obligations and privacy protection standards on the part of data recipients are less stringent, then customers face the risk of data processing by entities that are in a grey area of supervision. This situation weakens the effectiveness of privacy rights, as protection depends on the weakest link in the data processing chain, rather than on the highest standards that should apply to all parties holding financial data.

From a data protection law perspective, Tikkinen Piri, Rohunen, and Markkula emphasize that the GDPR framework requires clarity on the basis for processing, the principle of purpose limitation, and the strengthening of data subjects' rights such as the right of access, rectification, and erasure (Tikkinen-Piri et al., 2018). These elements provide conceptual guidance for the regulation of open banking in Indonesia, especially when account data and transaction histories are transferred from banks to additional service providers. If customer privacy rights are to be the main focus, then every open banking scheme needs to ensure that customers are aware of the purpose of processing, are able to control the granting and withdrawal of consent, and can demand the deletion or restriction of processing when they feel aggrieved. Without this mechanism, customer consent can easily be degraded to a contractual formality inserted into lengthy terms and conditions, while data processing proceeds with virtually no control.

Kuner explains that the cross-border flow of personal data raises new legal issues due to differences in protection standards between countries and the limited jurisdiction of national authorities (Kuner, 2013). In the open banking ecosystem, Indonesian customer data has the potential to flow to service providers that use global cloud computing infrastructure, relying on processing and storage in several countries at once. This has an impact on the scope of customer privacy rights, because enforcing access, correction, and deletion rights is no longer simple when data is controlled by multinational entities that are subject to various legal systems. For policymakers in Indonesia, open banking regulations need to take this cross-border dimension into account, whether through data processing location requirements, international data transfer regulations, or contractual obligations that bind foreign partners to respect protection standards equivalent to national law.

Farrell and Newman point out that data and privacy regulations reflect a tug-of-war between states, industry players, and community groups, which often ends in certain political compromises (Farrell & Newman, 2019). If these findings are adapted to open banking regulations in Indonesia, the position of customers as data subjects has the potential to be sidelined amid negotiations between authorities, banks, and digital technology providers. Consumer vulnerability in this digital ecosystem is also reflected in a study by Fitrotinisak et al. (2023), which reveals the challenges of consumer legal compliance in dealing with cases of account manipulation in digital banking services, reinforcing the importance of consumer protection and control perspectives in system design. Open banking can be positioned as a strategic agenda to improve payment efficiency and encourage innovation, while customer concerns about potential profiling, automated credit scoring, and data misuse tend to be considered secondary issues. A legal analysis of existing regulations needs to examine the extent to which customer privacy rights are explicitly stated as a guiding principle, rather than merely a derivative consequence of the long-established duty of confidentiality in banking law (Hermawan et al., 2023).

Literature on data-driven finance suggests that control over data and algorithms can become a new source of market power. Zetzsche and colleagues assert that data-driven finance can strengthen the position of actors who control large amounts of data and advanced analytical capabilities, thereby potentially giving rise to new concentrations of power (Zetzsche et al., 2020). In Indonesia's open banking regulations, customer privacy rights should be understood not only as a defensive right to prevent information leaks, but also as a mechanism for a more balanced distribution of power between financial institutions, technology providers, and individuals. If customers are given strong data portability rights, accompanied by the ability to transfer data to other service providers without unreasonable obstacles, then open banking can become an instrument for increasing customer choice and bargaining power. Conversely, if regulations only open access to large players without guaranteeing control rights for individuals, open banking risks reinforcing the dominance of a handful of market players (Yuliana & Maulana, 2023).

From a risk governance perspective, Buchak and colleagues show that financial innovations that

utilize different regulatory structures can shift risks outside the perimeter of traditional supervision (Buchak et al., 2018). In the open banking framework, privacy and data misuse risks can move from banking, which is relatively strictly supervised, to non-bank entities that utilize APIs to access account data. From a risk governance perspective, Buchak and colleagues show that financial innovations that utilize different regulatory structures can shift risk outside the perimeter of traditional supervision (Buchak et al., 2018). In the open banking framework, privacy and data misuse risks can move from banking, which is relatively strictly supervised, to non-bank entities that utilize APIs to access account data. The analogy of integration and interdependence between entities in this digital ecosystem is also illustrated in studies by Putra and Arifin (2021) and Khairi and Darmawan (2022) on digital transformation, which show that optimization through advanced technology also presents new risks and dependencies that require a clear framework for collaboration and security standards. This necessitates clear regulations regarding technical security standards, data incident management procedures, and the division of responsibilities in the event of data leaks or misuse. If Indonesia's legal framework does not explicitly stipulate the principle of joint responsibility or layered responsibility between banks and third parties, customers may face difficulties when seeking compensation for privacy violations, as the perpetrators may shift the burden of responsibility onto each other.

The literature on fintech regulatory reform emphasizes the importance of legal clarity on data processing and regulatory certainty. Arner, Barberis, and Buckley underscore that post-crisis regulatory reform should not focus solely on financial stability, but also consider consumer protection and equitable access to services (Arner et al., 2016). Although they speak at a global level, the message is relevant to the regulation of open banking in Indonesia. When banks are required to develop APIs and share data with other service providers, regulators need to ensure that consumer protection principles, including the right to privacy and data integrity, are placed on an equal footing with the goals of innovation and efficiency. This requires synchronization between financial sector regulations, personal data protection regulations, and banking provisions governing bank secrecy, so that there is no overlap or regulatory gap regarding the protection of customer rights (Nathania et al., 2023).

Tikkinen Piri and colleagues remind us that consent as the basis for data processing is often criticised due to information asymmetry and the imbalance of bargaining power between companies and individuals (Tikkinen-Piri et al., 2018). In open banking regulations, a similar problem arises when customers are faced with the choice of accepting or rejecting data access consent packaged in complex digital service packages. If Indonesian law relies too heavily on consent without strengthening the principles of purpose limitation, data minimization, and accountability obligations for banks and third parties, consent can become a formal instrument of legitimacy for data processing that is difficult to control. An analysis of positive norms needs to assess whether the requirement for "valid consent" includes clear information, freedom of choice, and ease of revocation, so that customers' privacy rights are not reduced to an illusory binary choice.

Open banking regulations in Indonesia must also consider the long-term consequences for public trust in the banking system. Kuner emphasizes that the protection of personal data is not only a matter of individual interest, but also touches on the legitimacy of institutions that manage and process data on a large scale (Kuner, 2013). The findings of Hardyansah et al. (2023) reinforce the importance of trust in building long-term relationships between financial institutions and the public. If the open banking scheme is implemented without strong guarantees for customer privacy rights, the risk of data leaks or excessive processing could erode trust in banks and supervisory authorities. In the long term, this could hinder the financial digitalization agenda, which depends on the public's willingness to submit data and use technology-based financial services. Therefore, the design of open banking regulations needs to be seen as part of a new social contract between the state, industry, and citizens regarding the management of financial data (Hermawan et al., 2023).

In addition to these international references, a review of national regulations shows that regulations concerning bank secrecy, personal data protection, and data management obligations by electronic system operators are still developing and have not been fully integrated into an explicit framework for open banking. On the one hand, banking secrecy provisions place customer information under strong protection with limited exceptions; on the other hand, regulations concerning payment system operators, digital financial system innovation, and API standardization are beginning to pave the way for broader data exchange between actors (Yuliana & Maulana, 2023). This normative tension has not always been resolved definitively, for example,

regarding the limits on the types of data that may be shared, the principle of data minimization, and the legal status of analytical profiles built on raw customer data. This is where legal analysis is needed to assess whether the principles of confidentiality and privacy rights are still strong enough when faced with the pressure of data-driven innovation.

At the implementation level, open banking regulations still face various practical issues related to supervisory mechanisms, technical standards, and loss recovery. Customers often find it difficult to identify the party responsible when their data is used for aggressive product offers, non-transparent profile-based lending, or even forms of fraud that exploit API access. This ambiguity arises because the open banking ecosystem involves many players banks, technology providers, data aggregators, and third-party service providers each of which has different technical and commercial roles in the data processing chain. Information asymmetry and technical architecture complexity complicate customers' ability to track data flows and determine points of failure or misuse. Therefore, operational standards are needed that emphasize not only technical security but also procedural transparency and accountability at every stage of data sharing.

Without a legal framework that clearly defines the responsibilities of banks, third-party service providers, and infrastructure operators, customer privacy rights risk becoming merely normative declarations without practical impact. This risk is even more apparent given that the provisions on responsibility in the PDP Law and banking regulations still need to be elaborated in more detail to anticipate the dynamics of multi-party collaboration in the open banking ecosystem. Therefore, open banking regulations in Indonesia need to move towards elaborating concrete substantive and procedural obligations including real-time data access monitoring mechanisms, integrated incident reporting procedures, and structured compensation schemes so that the protection of data privacy rights in the face of financial innovation practices can be truly realized and not merely remain at the level of rhetoric.

The Effectiveness of Legal Protection of Customer Data Privacy Rights in the Implementation of Open Banking

The implementation of open banking in Indonesia needs to be read systematically in conjunction with Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which forms the general framework for cross-sector personal data management, including the banking sector. The PDP Law emphasizes the principles of lawfulness, fairness, and transparency in the collection and processing of personal data, which in the context of banking is directly related to the management of transaction data, identity, and customer risk profiles. From a data protection theory perspective, general data protection principles serve as normative safeguards to control various data processing practices across sectors. The basic principles of data protection serve as a mechanism for accountability across regulatory regimes, especially in technology-based ecosystems and data exchange.

The existence of the PDP Law enables normative testing of Application Programming Interface (API)-based data sharing schemes, particularly in relation to compliance with the principles of processing legitimacy, fair treatment of data subjects, and transparency of information to customers regarding the purpose, legal basis, and scope of data transfer to third parties (Amalia, 2022). Empirical studies in the financial sector also show that the successful implementation of open banking is highly dependent on clear consent management mechanisms and data flow transparency, which are key elements in modern data protection regimes (Zetzsche et al., 2020). Thus, the PDP Law serves not only as an instrument for protecting the rights of data subjects, but also as a legal legitimacy framework for open banking practices to remain in line with the principles of prudence and public trust in the digital banking system.

The rights of data subjects regulated in the PDP Law, such as the right of access, the right of correction, the right of deletion, and the right to object to certain data processing, are important components for assessing the strength of legal protection in the open banking scheme. Solove explains that this type of procedural rights regime aims to offset the imbalance of power between data controllers and individuals by giving data subjects greater control over information about themselves (Solove, 2008). In the banking sector, the right of access allows customers to know what data is stored and shared by banks with third parties; the rights of correction and erasure provide room for correction of incorrect data or processing that is considered excessive; the right to object allows customers to refuse certain forms of processing, such as profiling for intensive marketing. The effectiveness of legal protection is determined by the extent to which banks and open banking partners are required to provide easy, measurable, and documented procedures for exercising these

rights (Yuliana & Maulana, 2023).

Bank Indonesia Regulation No. 12 of 2024 concerning Data and Information Policy strengthens the sectoral dimension of the PDP Law framework by regulating data governance in banking and payment systems. This regulation places financial system stability and data security as the foundation for digital innovation, including the development of open banking through APIs. Customer trust, which is the main foundation of banking relationships, is also determined by how financial institutions manage data and build contextual integrity, as reinforced by Darmawan's (2023) findings on the crucial role of trust in building customer loyalty in Islamic banks. Here, the principle of good data governance intersects with Nissenbaum's idea of "privacy as contextual integrity", which emphasizes the importance of maintaining consistency between data flows, norms of trust, and social expectations in a given domain (Nissenbaum, 2010). By regulating data governance standards, Bank Indonesia seeks to ensure that customer data flows between banks and third parties are in line with customer expectations of trust in banking institutions, rather than merely following the commercial interests of financial technology industry players (Nathania et al., 2023).

PBI on Data and Information Policy also constitutes a foundational regulatory basis for the implementation of open banking through API standardization, enabling structured data exchange between banks and third-party providers. From a data protection perspective, technical standardization of APIs cannot be separated from the principle of legal accountability emphasized in modern data protection literature. While Hijmans (2016) underlines that the effectiveness of the EU data protection regime depends on the ability of data controllers to demonstrate compliance with substantive principles through strong internal governance and adequate documentation, similar arguments are also advanced in Indonesian scholarship. Budhijanto (2021) emphasizes that accountability in personal data processing requires not only normative compliance but also verifiable technical and organizational measures that can be audited. Likewise, Rosadi (2022) argues that financial sector digitalization must be accompanied by enforceable data governance mechanisms to ensure that data sharing frameworks do not undermine data subjects' rights.

Applying this logic, API regulation by Indonesia's monetary authority should explicitly impose obligations on banks and third-party providers to implement security controls, access logging, and periodic audit mechanisms capable of demonstrating that every API call involving customer data is based on a clear legal ground and a legitimate processing purpose (Sutanto & Nugroho, 2021). Without embedding accountability requirements into API governance, open banking risks becoming a purely technical interoperability initiative detached from legal responsibility, thereby weakening trust and exposing customers to systemic data misuse risks (Putri & Hidayat, 2020).

OJK regulations on digital financial services and fintech complement the legal architecture by focusing on consumer protection and risk oversight in the use of customer data. Amidst the integration of banking systems with technology service providers, OJK is tasked with ensuring that fintech companies that gain access to customer account data through open banking schemes are subject to data protection standards equivalent to those of banks (Hermawan et al., 2023). Lynskey emphasizes that in the modern data ecosystem, the line between data controllers and processors is often blurred, so that data subject protection requires the extension of obligations to various actors involved in processing (Lynskey, 2015). In the Indonesian context, this principle points to the need to clarify the legal status of fintech and third-party application providers as joint controllers or processors, with clear consequences for liability in the event of customer privacy violations.

The academic framework on open banking broadly states that the use of customer financial data must be based on a mechanism of explicit consent that is clearly informed. Bygrave highlights that consent has normative value only to the extent that data subjects understand the consequences of processing and have a real choice to refuse (Bygrave, 2014). In the open banking ecosystem, this means that banks are required to provide an explicit opt-in mechanism when customers allow data sharing with third parties, accompanied by information about the type of data, the purpose of processing, the duration, and the potential risks. Consent that is implicitly included in general terms and conditions, without specific explanations regarding API access and data recipient categories, has the potential to conflict with the principles of fairness and transparency emphasized in the PDP Law, while also reducing the effectiveness of privacy rights protection (Amalia, 2022).

Secure API technical standards and data compliance audit mechanisms are prerequisites for the legal framework to go beyond the declarative level. The literature on data protection emphasizes the link between legal principles and technical

design, including the principles of data protection by design and by default (Hijmans, 2016). In Indonesia's open banking regulations, this requires that API standardization not be limited to interoperability aspects, but also include the principles of data minimization, role-based access control, encryption, and retention policies that are in line with the processing objectives. Data compliance audits conducted by authorities or independent auditors need to examine both compliance with the PDP Law and secondary regulations of the OJK and BI, as well as the implementation of adequate technical controls. Without a bridge between legal norms and technical design, customers' rights of access, correction, deletion, and objection will be difficult to operationalize in a complex API architecture.

A legal analysis of the compatibility of open banking with the PDP Law shows that data sharing schemes can be considered lawful as long as they are based on legitimate grounds for processing, particularly explicit consent and full transparency. Solove reminds us that the main risk in modern data protection practices is the occurrence of "privacy self-management overload", when individuals are burdened with too many complicated decisions regarding their data (Solove, 2008). Therefore, although the PDP Law and sectoral regulations recognize the right of customers to determine whether their data may be shared with third parties, the law also needs to ensure that the design of consent, privacy policies, and user interfaces are reasonably designed so that customers are truly able to understand the choices they are making. At this point, the role of regulators becomes important in setting minimum standards regarding the form, language, and manner of conveying consent information in digital banking services (Nathania et al., 2023).

Within the framework of protecting customer privacy rights, the obligation of banks to provide clear opt-in and opt-out mechanisms is a concrete instrument for realizing the principle of individual data sovereignty (Yuliana & Maulana, 2023). Nissenbaum emphasizes that privacy violations often occur when data flows shift from patterns expected by individuals, without adequate knowledge (Nissenbaum, 2010). With the opt-in mechanism, customers will only be connected to the open banking scheme when they consciously give permission for data sharing; the opt-out mechanism allows customers to stop third-party access at a later stage. The effectiveness of the regulation depends on the clarity of procedures, the speed of executing customer requests, and prohibitions on practices that make opting out difficult (e.g., conditions designed to prevent customers from opting out). Here, the PDP Law provides the basis for administrative and criminal sanctions for violations of data protection obligations, while BI and OJK can impose sectoral sanctions such as fines, service restrictions, or revocation of licenses.

Data protection literature emphasizes that strict sanctions serve as an incentive for compliance and as a signal of the social values upheld by a legal regime (Lynskey, 2015). In Indonesia's open banking scheme, customer privacy violations such as the use of data outside the agreed purpose, failure to secure API access credentials, or data leaks to unauthorized parties may be subject to administrative sanctions in the form of fines, temporary suspension of processing, or even data deletion. The PDP Law also opens up the possibility of criminal sanctions for certain actions that seriously violate the rights of data subjects. The effectiveness of protection will increase if the coordination of sanctions between the PDP Law, BI regulations, and OJK regulations is mutually reinforcing, rather than partial. Banks and open banking partners will be encouraged to integrate data protection compliance into corporate risk management, rather than treating it as an additional burden separate from business operations.

Overall, the compatibility of open banking law with Indonesia's data protection framework depends on harmonization between the PDP Law as lex generalis and the sectoral regulations of BI and OJK as lex specialist. Bygrave highlights that the effectiveness of a data protection regime is largely determined by the clarity of the division of authority between authorities, the consistency of cross-sector regulations, and the ability of supervisory agencies to interpret general principles into practical obligations (Bygrave, 2014). In this case, BI is tasked with safeguarding data integrity and security in the financial system, while OJK supervises the behavior of digital financial business actors. Both need to ensure that the push for digital banking innovation through open banking does not lower the protection standards promised by the PDP Law to customers as data subjects (Hermawan et al., 2023). Harmonization can be achieved through joint guidelines, coordinated supervision, and integrated complaint mechanisms that make it easier for customers to seek redress when their privacy rights are violated.

Outside the formal regulatory framework, the effectiveness of customer privacy rights protection in open banking practices is largely determined by the culture of compliance in financial institutions and

customer data literacy. Although the law provides the basis for explicit consent, access, correction, deletion, and objection rights, these rights are only meaningful if customers are aware of their existence and banks are willing to proactively facilitate the exercise of these rights. Outside the formal regulatory framework, the effectiveness of customer privacy protection in open banking practices is largely determined by the culture of compliance within financial institutions and customer data literacy. Although the law provides a basis for explicit consent, access, correction, deletion, and objection rights, these rights are only meaningful if customers are aware of their existence and banks are willing to proactively facilitate the exercise of these rights. The ability to manage and utilize data strategically and responsibly, as outlined in the study by Ali and Darmawan (2023) on optimizing big data management for decision-making and business strategy, is also relevant in this context, where ethical customer data management can be a source of competitive differentiation and long-term trust. The importance of reputation and trust as strategic assets for banking, as analyzed by Hardyansah and Jahroni (2023), further emphasizes that a commitment to protecting privacy rights and service quality is an important investment in building long-term relationships with customers in the digital age. Efforts to educate customers about personal data protection, user-friendly interface design, and transparency in data sharing policies will strengthen the effectiveness of existing regulations. In the long term, the balance between digital banking innovation and privacy rights protection will be greatly influenced by the extent to which the banking and fintech industries view data protection not merely as a legal obligation, but as part of a value proposition and reputation that must be maintained.

Ultimately, Indonesia's open banking framework demonstrates a normative effort to balance the drive for innovation with the protection of customer privacy rights through a combination of the Personal Data Protection Law, the Data and Information Policy, and OJK regulations on digital financial services. Explicit recognition of the rights of access, correction, deletion, and objection; obligations based on lawfulness, fairness, and transparency; sectoral data governance standards; and administrative and criminal sanction mechanisms are elements that, in theory, can provide strong protection to customers. The main challenge lies in integrated implementation, effective supervision, and consistent enforcement of violations, especially in an ecosystem involving various actors, from large banks to fintech startups with varying compliance capacities.

CONCLUSION

A legal analysis of open banking regulations and bank customer data privacy rights in Indonesia shows that the national legal architecture is moving towards a data-based financial model that is bound by a personal data protection framework. Law No. 27 of 2022 concerning Personal Data Protection serves as lex generalis which affirms the principles of lawfulness, fairness, and transparency, as well as guarantees the rights of access, correction, deletion, and objection for customers as data subjects. At the sectoral level, Bank Indonesia's Regulation on Data and Information Policy and OJK regulations on digital financial services provide a foundation for data governance, security standards, and supervisory guidelines for banks and fintech players connected through the open banking scheme. Normatively, the integration of this framework can be considered in line with modern data protection principles as described in international literature. However, the effectiveness of customer privacy protection is highly dependent on operational implementation in financial institutions, the clarity of explicit consent design, opt-in and opt-out mechanisms, regulatory oversight capacity, and the industry's willingness to position data protection as a foundation of trust, not merely an administrative burden.

Theoretically, this study confirms that open banking regulations in Indonesia cannot be analyzed solely through the lens of classical banking law, but need to be linked to personal data protection regimes and the global discourse on data-driven finance. A normative juridical approach that combines national regulatory studies and international literature shows that customer data privacy rights function as a mechanism for distributing power in an increasingly data-dense digital financial ecosystem. In practical terms, the findings of this study indicate the need to refine derivative regulations that operationalize the principles in the PDP Law and sectoral regulations into explicit consent standards, API designs that ensure data minimization, procedures for fulfilling data subject rights, and coordination of sanctions between authorities. For banks and fintech players, data protection should be positioned as an element of business sustainability and reputation management strategies, as customer trust in financial data management is a key prerequisite for the success of open banking.

First, policymakers need to formulate joint

guidelines between data protection authorities, Bank Indonesia, and the OJK regarding the implementation of open banking that is oriented towards customer privacy rights, including minimum standards for consent information, opt-in/opt-out formats, and procedures for handling data breach complaints. Second, regulators are advised to strengthen oversight and compliance audit mechanisms for API schemes by combining evaluations of legal, governance, and technical security aspects so that customer data flows can be monitored and accounted for systematically. Third, banking and fintech institutions need to improve customer data literacy through clear and simple explanations of the consequences of data sharing, customer rights, and how to exercise those rights. Going forward, further research is recommended to examine contractual practices and user interface design in banking and fintech applications in Indonesia, in order to assess whether the principles of data protection regulated by norms are truly reflected in everyday user experiences.

REFERENCES

Ali, R., & Darmawan, D. (2023). Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies,* 3(2), 139-144.

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

Amalia, R. (2022). Perlindungan data pribadi dalam ekosistem open banking di Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, 29(3), 475–497.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The Evolution of Fintech: A New Post Crisis Paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal,* 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks. *Journal of Financial Economics,* 130(3), 453–483. https://doi.org/10.1016/j.jfineco.2018.03.011

Budhijanto, D. (2021). Accountability Principle in Personal Data Protection Law. *Journal of Indonesian Legal Studies*, 6(3), 233–247.

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective.* Oxford University Press.

costa, S. da., Darmawan, D., & Isaac, A. de J. (2023). Safeguarding Employee Data with Blockchain in HR. *International Journal of Service Science, Management, Engineering, and Technology*, 4(3), 41–46.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.)*. SAGE Publications.

Darmawan, D. (2023). The Effect of Trust and Saving Experience on Loyalty Through Satisfaction as an Intervening Variable (Case Study of Sharia Bank Customers in Surabaya City). *International Journal of Service Science, Management, Engineering, and Technology,* 2(2), 11–20.

Farrell, H., & Newman, A. L. (2019*). Of Privacy and Power: The Transatlantic Struggle over Freedom and Security.* Princeton University Press.

Fitrotinisak, I. K., Mardikaningsih, R., Gautama, E. C., Sulani, & Vitrianingsih, Y. (2023). Legal Compliance for Consumers in Dealing with Cases of Account Tampering in Digital Banking Services. *Journal of Social Science Studies*, 3(1), 75-82.

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press.

Hardyansah, R., & Jahroni, J. (2023). The Establishment of Customer Loyalty in View of Service Quality and Bank Reputation. *Bulletin of Science, Technology and Society,* 2(1), 16–20.

Hardyansah, R., Jahroni, J., Darmawan, D., Arifin, S., & Negara, D. S. (2023). Student Interest in Becoming Customers of Islamic Banks in Terms of Religiosity and Product Knowledge. *International Journal of Service Science, Management, Engineering, and Technology*, 4(1), 5–10.

Hardyansah, R., Pakpahan, N. H., & Wibowo, A. S. (2021). The Ramifications of Banking Monopoly on Consumer Trust, Customer Satisfaction, and Industry Competition Dynamics. *Journal of Social Science Studies*, 1(2), 105-110.

Hermawan, S., Khoirunisa, Z. A., & Tejomurti, K. (2023). Triangular Insight on Open Banking in Indonesia, Singapore, and Australia. *International Journal of Legal Information*. https://doi.org/10.1017/jli.2024.11

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy and Data Protection*. Springer.

Khairi, M., & Darmawan, D. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations. *Journal of Social Science Studies*, 2(1), 223-228.

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law.* Oxford University Press.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook (3rd ed.)*. SAGE Publications.

Nathania, S. A., Abubakar, L., & Handayani, T. E. (2023). Implikasi Hukum Pemanfaatan Open Application Programming Interface Terhadap Layanan Perbankan Dikaitkan dengan Ketentuan Perbankan Digital. *Jurnal Poros Hukum Padjadjaran*. https://doi.org/10.23920/jphp.v4i2.1209

Nicoletti, B. (2017). The Future of FinTech: Integrating Finance and Technology in Financial Services. *Palgrave Macmillan*. https://doi.org/10.1007/978-3-319-61247-2

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Omarova, S. T. (2020). New Tech v. New Deal: Fintech as a Systemic Phenomenon. *Yale Journal on Regulation,* 36(2), 735–793. https://doi.org/10.2139/ssrn.3224393

Peraturan Bank Indonesia Nomor 12 Tahun 2024 tentang Kebijakan Data dan Informasi.

Putra, A. R., Jahroni, Hardyansah, R., & Arifin, S. (2022). Institutionalizing Sustainability within Islamic Banking: Ethical Alignment and Practical Application in Responsible Finance. *Journal of Social Science Studies*, 2(1), 241-246.

Putri, A. S., & Hidayat, R. (2020). Open Banking and Data Protection Challenges in Indonesia. *Journal of Financial Regulation and Compliance,* 28(4), 512–526.

Rosadi, S. D. (2022). Data Governance and Legal Accountability in Indonesia's Digital Financial Services. *Hasanuddin Law Review*, 8(2), 167–181.

Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

Sutanto, H., & Nugroho, R. S. (2021). API Governance and Legal Responsibility in Financial Technology Services. *Journal of Law, Technology and Society*, 4(2), 95–110.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review*, 34(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998.

Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2), 494–620. https://doi.org/10.7916/cblr.v2019i2.3424

Wahyudi, W., R. N. K. Kabalmay, & M. W. Amri. (2021). Big Data and New Things in Social Life. *Studi Ilmu Sosial Indonesia*, 1(1), 1–12.

Yuliana, & Maulana, A. (2023). *Comparative Analysis of the Implementation of Open Banking Systems for Indonesia's 2025 National Payment System Vision*. https://doi.org/10.62084/slj.v2i2.339

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). The Future of Data Driven Finance and RegTech: Lessons from EU's Second Payment Services Directive. *University of Hong Kong Faculty of Law Research Paper No. 2020 12*. https://doi.org/10.2139/ssrn.3582328

***Kuriawati, R. Hardyansah, & P. Saktiawan. (2024). Legal Analysis of Open Banking and Bank Customer Data Privacy Rights in Indonesia, *Journal of Social Science Studies*, 4(1), 93– 104.**