https://doi.org/10.56861/nalarnagara.v1i3
e-ISSN: 0000-0000

International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy
Nalarnagara Journal
Vol. 1, No. 3, July 2026 pp. 1311-1322
Journal Page is available at https://internationaljournal.lppmunsaka.ac.id/index.php/nalarnagara

Personal Data Protection as A Limit to State Authority in The Supervision of the Banking Sector in Indonesia

Andrew Garibaldi Davinci[1], Annisa Fitria[2], Henry Arianto[3]
[1,2,3]Universitas Esa Unggul
Email: andrew.garibaldi@student.esaunggul.ac.id, annisa.fitria@esaunggul.ac.id, henry.arianto@esaunggul.ac.id

ABSTRACT

This study analyzes personal data protection as a legal limit to the exercise of state authority in the supervision of the banking sector in Indonesia. The issue arises because banking supervision may create a need to obtain customer information, while such information is closely related to the right to privacy, bank secrecy, and the trust-based relationship between banks and customers. This study focuses on two issues: how personal data protection limits state authority in banking supervision, and whether the regulatory framework and its implementation are consistent with the principle of the rule of law and the protection of customers' privacy rights. This study uses normative legal research with statutory and conceptual approaches. The findings show that state authority to supervise banks is legitimate, but it cannot be exercised without limits. Access to customer data must have a legal basis, be directed toward a lawful purpose, be limited to the necessary information, and be accompanied by the principles of proportionality, security, and accountability. Indonesian law has provided a normative basis through regulations on personal data protection, bank secrecy, financial services supervision, and electronic system security. However, implementation still requires clearer operational limits, stronger institutional coordination, and a strengthened role for personal data protection officers or officials. Therefore, personal data protection is not an obstacle to banking supervision, but a legal instrument that ensures state supervision remains within lawful and accountable limits.

Keywords: *privacy rights; state authority; personal data protection; banking supervision; bank secrecy.*

INTRODUCTION

The development of information technology has changed the pattern of the relationship between banks and customers. Services that previously depended on direct interaction at branch offices are now increasingly carried out through digital channels, such as mobile banking, internet banking, electronic account opening, online identity verification, and integrated payment systems. This change has made personal data an inseparable part of the provision of banking services. Data is not only used for administrative purposes, but also to process transactions, identify customers, assess risks, and connect banking services with the digital financial ecosystem. This condition provides benefits for service efficiency, but at the same time creates new risks to the security and use of customer data (Ichsandi and Silalahi 1). These risks become broader in open banking practices because customer data may be transferred or used by other parties through digital data exchange mechanisms (Rohmah and Ribawati 1-2).

In the banking sector, customer data has a higher protection value than general information. Such data may include identity, account number, balance, transaction history, credit data, source of income, and other information that may indicate a person's economic

condition. This information is personal because it can describe financial habits, economic capacity, legal relationships, and even the customer's transaction activities. If such data is used unlawfully, customers may suffer financial loss, reputational harm, and loss of security in using banking services. Therefore, the relationship between banks and customers is not only based on financial services, but also on the trust that the information submitted to banks will be kept confidential (Ichsandi and Silalahi 4).

The urgency of protecting customer data is increasing because digital banking services are highly dependent on electronic systems. Every process of authentication, transaction, data storage, account activity monitoring, and financial service integration requires a secure and reliable system. If the system is disrupted, the impact is not only felt by the bank as the service provider, but also by customers as the owners of personal data. The ransomware attack against Bank Syariah Indonesia in 2023 showed that cybersecurity disruptions may be directly related to personal data protection in the banking sector (Kholis 275-77). This incident shows that customer data issues cannot be separated from system security, risk governance, and public trust in digital banking services (Rohmah and Ribawati 2).

From the legal perspective, Indonesia has regulated personal data protection through Law Number 27 of 2022 concerning Personal Data Protection. The existence of this law shows that personal data is no longer viewed merely as administrative information, but as part of the right to personal protection that must be guaranteed by law (Budhijanto 3-4). In the banking sector, this protection does not stand alone because it is also related to bank secrecy rules, the authority of the Financial Services Authority, electronic system security, and financial sector strengthening. Therefore, customers' personal data exists at the intersection of personal data protection law, banking law, information technology law, and financial services supervision law.

These various regulations show that customer data exists within a complex legal sphere. Customer data is not only related to the interests of banks as service providers, but also to the state's obligation to maintain financial sector stability, protect consumers, and ensure compliance by financial service institutions. In this context, the Financial Services Authority has an important position as the institution that carries out regulatory and supervisory functions over the banking sector. This supervisory function is needed so that banks conduct their business soundly, comply with legal provisions, and continue to protect customers' interests (Johan 24-25). However, in practice, the exercise of supervisory authority may create a need to obtain or examine certain information controlled by banks.

State authority to supervise banks is basically legitimate and necessary. Without supervision, banking activities may create risks to financial system stability, consumer interests, and public trust. The Financial Services Authority was established so that activities in the financial services sector are conducted in an orderly, fair, transparent, accountable, stable manner and are capable of protecting the interests of consumers and the public (Diyanatalia et al. 547). However, such authority must still be placed within the framework of the rule of law. This means that supervision cannot be based merely on institutional needs, but must also observe legal limits when it touches customers' personal data.

The legal issue arises when state supervision is directly related to customers' privacy rights. The state may have a lawful reason to obtain certain data from banks, but that reason cannot be interpreted as authority to open customer data broadly. Every action involving customer data must be explainable in terms of its legal basis, purpose of use, scope of data, reason for necessity, and security mechanism. Therefore, personal data protection needs to be positioned as a benchmark to assess whether the exercise of supervisory authority remains within reasonable limits or has exceeded interests justified by law.

This study does not only discuss personal data protection from the perspective of data breaches or electronic system security. The main focus of this study is to view personal data

protection as a legal limit to state authority in the supervision of the banking sector. This is important because national regulations have provided a basis for protection, but their implementation still faces problems in supervision, institutional capacity, cross-institutional coordination, and accountability mechanisms (Kholis 275-76). Therefore, it is necessary to examine the extent to which personal data protection can limit state action when banking supervision requires access to customer data.

Based on this background, this study examines two research questions. First, how does personal data protection function as a legal limit to state authority in the supervision of the banking sector in Indonesia? Second, have the regulation and exercise of state authority in the supervision of the banking sector been consistent with the principle of the rule of law and the protection of customers' privacy rights?

This study aims to explain the function of personal data protection as a legal limit to state authority in the supervision of the banking sector. In addition, this study aims to assess the consistency between regulation, the implementation of supervision, and the protection of customers' privacy rights within the framework of the rule of law.

METHOD

This study uses normative legal research because the issue examined relates to the assessment of legal norms that limit state authority in accessing customer data in the banking sector. This research does not rely on field data, but on the examination of legal materials to understand the relationship between personal data protection, bank secrecy, supervisory authority, and customers' privacy rights.

The approaches used consist of the statutory approach and the conceptual approach. The statutory approach is conducted by examining legal provisions governing personal data protection, banking, the Financial Services Authority, electronic information and transactions, financial sector strengthening, and bank secrecy. The conceptual approach is used to explain the concepts of privacy rights, customer personal data, confidentiality of banking information, supervisory authority, and legal limits on state action.

The legal materials in this study were obtained through library research on laws and regulations, books, scholarly journals, legal articles, and other supporting sources relevant to the subject matter. These legal materials were then organized according to the issues analyzed and examined qualitatively. The analysis was conducted by connecting legal norms and legal concepts to explain the function of personal data protection as a limit to state authority and to assess its consistency with the rule of law and the protection of customers' privacy rights.

RESULT AND DISCUSSION

CUSTOMER PRIVACY RIGHTS AND PERSONAL DATA AS OBJECTS OF LEGAL PROTECTION

The analysis of the limitation of state authority in banking supervision must begin by placing customer data as part of the right to privacy. Privacy rights in this context are not only understood as the right to be free from interference, but also as a person's right to control information attached to them. In banking relationships, such information may include identity, account number, transaction history, credit data, source of income, balance, and other information that describes the customer's personal and economic condition. Therefore, personal data protection becomes an important instrument to ensure that information relating to a person is not used freely without a legal basis and lawful purpose (Budhijanto 3-4).

Customer data has a special character because it does not merely function as a bank's administrative data. Through account and transaction data, a person's consumption patterns, financial capacity, transaction relationships, source of funds, and economic activities can be

identified. This character gives customer data a sensitive value, both from the perspective of private interests and legal interests. If the data is used without authority, the impact is not only economic loss, but may also disturb the customer's reputation, sense of security, and trust in banking institutions. Thus, customer data needs to be understood as an object of legal protection that is directly related to the right to privacy.

The Personal Data Protection Law provides that personal data is data concerning an individual who can be identified directly or through combination with other information. This definition is relevant to the banking sector because customer data often does not stand alone. Names, account numbers, identity numbers, transaction histories, credit data, and other financial information may be connected to form a customer's personal profile. In fact, personal financial data falls within the category of specific personal data. Therefore, the processing of customer data must be carried out carefully because such data has a higher level of risk than general data.

In addition to being protected under the personal data protection regime, customer information is also related to the principle of bank secrecy. Under banking law, banks are obliged to keep confidential information concerning depositors and their deposits, except in circumstances expressly justified by law. The principle of bank secrecy shows that the relationship between banks and customers is built on trust. Customers provide information and place funds in banks with the expectation that banks will not disclose such information to other parties without a lawful reason. Therefore, the obligation to maintain bank secrecy is part of the protection of trust, information security, and customers' privacy rights (Ichsandi and Silalahi 4).

In modern banking practice, the scope of customer data processing has expanded because banking services have shifted to electronic systems. Mobile banking, internet banking, electronic account opening, digital identity verification, and application-based payment services cause customer data to be processed quickly, repeatedly, and through interconnected systems. This condition makes personal data protection inseparable from electronic system security. If a bank's system experiences disruption, leakage, or a cyberattack, customer data may be affected. The ransomware attack against Bank Syariah Indonesia in 2023 is an example showing that cybersecurity risks in banking may be directly related to the security of customers' personal data (Kholis 275-77).

Based on the above discussion, customers' personal data must be positioned as an object of legal protection with several dimensions. First, the data forms part of privacy rights because it relates to a person's identity and personal condition. Second, the data is protected by the principle of bank secrecy because it arises from the trust-based relationship between banks and customers. Third, the data is high-risk because it can describe a person's financial condition and economic activities. Fourth, in digital banking services, such data also depends on electronic system security. Therefore, every use, disclosure, or granting of access to customer data must be placed within clear legal limits.

PERSONAL DATA PROTECTION AS A LEGAL LIMIT TO STATE AUTHORITY

After customer data is understood as part of the right to privacy and as an object of legal protection, the discussion moves to the function of personal data protection as a limit on state action. In the supervision of the banking sector, the state through the competent authority may require certain information from banks. However, this need cannot be interpreted as authority to disclose, use, or process customer data without clear legal standards. In a rule-of-law state, every action affecting citizens' rights must be explainable in terms of the basis of authority, the purpose of use, the scope of the action, and its accountability.

The Personal Data Protection Law provides a framework that every activity involving personal data constitutes data processing. Such processing includes various actions, from

obtaining, collecting, storing, analyzing, using, disclosing, transferring, to deleting or destroying personal data. Therefore, when the state requests or obtains customer data from a bank, such action cannot be separated from the personal data protection regime. State access to customer data must be viewed as data processing that must comply with the principles of lawfulness, purpose limitation, security, and accountability.

The first measure in assessing whether state access to customer data is lawful is the existence of a legal basis. The state cannot simply state that access is needed for supervision. There must be a provision of law granting authority to a certain institution or official to request, receive, or disclose customer data. Article 20 of the Personal Data Protection Law emphasizes that personal data processing requires a processing basis. In the banking context, such basis may be a legal obligation or the exercise of authority granted by law. Without a clear legal basis, a data request may become an act exceeding authority.

In addition to a legal basis, access to customer data must also be directed toward a lawful purpose. Such purposes may include banking supervision, compliance examination, consumer protection, prevention of financial crimes, taxation, judicial proceedings, or other purposes determined by laws and regulations. Article 15 of the Personal Data Protection Law recognizes exceptions to the rights of personal data subjects, including for the purpose of supervision in the financial services sector, monetary affairs, the payment system, and financial system stability. However, such exceptions must not be read as a general permission to disclose all customer data. Exceptions must still be used in a limited manner and in accordance with procedure.

The next limit concerns the correspondence between the data requested and the purpose to be achieved. Customer data may only be accessed if it has a direct relationship with the interest of supervision or an ongoing legal process. In addition, the type of data requested must be limited to data that is truly necessary. This principle is important because customer data may contain very broad information, including balance, account mutations, credit data, source of funds, and transaction patterns. If the supervisory purpose only requires certain data, full disclosure of data cannot be justified because it may violate customers' privacy rights.

The application of this principle can be seen in money laundering cases. In money laundering cases, account data, transaction data, and information concerning assets may be needed to trace the source of funds, movement of funds, relationship between transactions, or use of accounts to disguise the proceeds of crime. In such circumstances, the disclosure of customer data may be justified as long as it is based on legal authority, relates to a case being handled, and is limited to data relevant to the alleged criminal offense. This means that personal data protection does not prevent data disclosure for law enforcement, but ensures that such disclosure is not carried out excessively.

Procedurally, the disclosure of customer data can be carried out through a general mechanism or a special mechanism. The general mechanism applies when the disclosure of bank secrecy still requires permission or coordination with the Financial Services Authority. Under this mechanism, the authorized party must submit a written request explaining the legal basis, purpose of the request, identity of the party whose data is requested, and the scope of the data required. The request is then assessed before the bank can provide data within the specified limits. This procedure is important to ensure that data disclosure is not carried out merely on the basis of verbal or general requests.

The special mechanism applies when a specific law grants direct authority to certain officials or institutions to request data or information. In money laundering cases, Law Number 8 of 2010 grants investigators, public prosecutors, and judges the authority to request written information from Reporting Parties, including banks as financial service providers, regarding the assets of parties related to the case. In such circumstances, bank secrecy and

financial transaction confidentiality provisions do not apply. However, the request must still be made in writing and must contain the identity of the requesting official, the identity of the party whose information is requested, a brief description of the criminal offense, and the location of the assets.

Authority in money laundering cases also depends on the stage of case handling. At the investigation stage, the request may be made by investigators. At the prosecution stage, the authority lies with public prosecutors. At the trial stage, the request may be made by judges. These differences show that the disclosure of customer data does not always have to wait for a court decision, but it must still be connected to the authority of the official at the relevant stage of the case. Therefore, the main limit is not only who requests the data, but also whether the request is consistent with the stage, purpose, and scope of the case.

If the flow of funds is suspected to involve another party, that party's data may be requested as long as there is a relationship that can be explained in connection with the case. Such relationship may include receipt of funds, transfer of funds, placement of funds, use of an account, or another transactional connection with the alleged criminal offense. However, the data of another party must not be disclosed merely because of an unfocused suspicion. The request must still state the identity of the party whose data is requested, the party's relationship with the case, the type of data needed, the period of the data, and the reason why the data is relevant. In this way, the disclosure of another party's data remains within legal limits and does not become a broad search for data without an adequate basis.

Limits on data access are also related to the principles of proportionality and accountability. The broader the data requested, the greater the obligation to ensure that the request is truly necessary, secure, and accountable. The state must maintain a balance between the interests of supervision or law enforcement and customers' privacy rights. In administrative law, supervision of governmental action is needed so that the use of authority remains consistent with legal purposes and does not develop into arbitrary action (Paramitha et al. 167-69).

Limits on state authority are also strengthened by bank secrecy regulation. The Banking Law and Financial Services Authority Regulation Number 44 of 2024 concerning Bank Secrecy affirm that customer information must in principle be kept confidential. Exceptions are indeed possible, for example for judicial purposes, taxation, mutual assistance in criminal matters, the performance of duties by Bank Indonesia and the Deposit Insurance Corporation, or the interests of other institutions based on their authority. However, such exceptions must be understood as limited access. Exceptions to bank secrecy do not mean that all customer data may be disclosed without limits.

In addition to a legal basis and lawful purpose, the disclosure of customer data must also be traceable. Banks need to have internal mechanisms to record requests, the basis for providing data, the types of data provided, the parties receiving the data, and the reasons for disclosing the information. In certain circumstances, data disclosure also requires permission or coordination with the Financial Services Authority. Such documentation is important to ensure that every data disclosure can be reviewed if misuse, procedural violation, or information leakage occurs.

Therefore, personal data protection functions as a legal limit to state authority because every access to customer data must be placed within a legal framework. The state may continue to carry out supervision and law enforcement functions, but their implementation must be based on lawful authority, clear purposes, a relevant relationship between the data and the case or supervision, actual necessity, written procedures, data security, and accountability mechanisms. These limits ensure that state authority does not become overly broad access to customers' personal data.

BANKING PRACTICES THAT INTERSECT WITH CUSTOMERS' PERSONAL DATA

After the limits of state authority in banking supervision have been explained, it is necessary to examine how customers' personal data is used in banking practice. This is important because customer data is not merely a legal concept, but is present in almost every stage of the relationship between banks and customers. The data is used from the formation of the legal relationship, transaction monitoring, provision of digital services, reporting to authorities, to the disclosure of bank secrecy in certain circumstances. Thus, banking practice shows that customer data processing is an ongoing activity and carries legal risks if it is not accompanied by clear limits.

At the initial stage of the relationship between a bank and a customer, personal data is used for account opening and identity verification. Banks generally request information concerning identity, address, contact number, occupation, source of income, and other data needed to identify prospective customers. Such data collection is necessary so that banks can fulfill administrative obligations, apply the prudential principle, and comply with know-your-customer principles. However, from this initial stage, customer data already falls within the scope of legal protection because banks obtain information related directly to customers' identity and personal circumstances. Therefore, the use of data at the initial stage of the banking relationship must still be based on a clear purpose and must not be used outside lawful interests.

Customer data is also used in transaction monitoring and banking compliance. Through transaction data, banks can assess whether a customer's financial activities are consistent with the customer's profile and the purpose of using the account. The data may also be used to prevent account misuse, detect unusual transactions, apply anti-money laundering principles, prevent terrorism financing, and fulfill reporting obligations in the financial services sector. In this context, the use of customer data has a justifiable basis as long as it is carried out for compliance purposes and is limited to relevant data. Conversely, if the data is used for other purposes unrelated to the banking relationship or legal obligations, such use may create problems for customers' privacy rights.

In digital banking services, the scope of customer data processing becomes broader. Mobile banking, internet banking, electronic account opening, digital identity verification, and application-based payment services cause customer data to be processed continuously through electronic systems. This condition makes system security an important part of personal data protection, because every disruption to an electronic system may directly affect customer data. Article 15 of the Electronic Information and Transactions Law requires electronic system providers to operate systems reliably, securely, and responsibly. This provision is relevant to digital banking services because customer trust greatly depends on the bank's ability to protect data processed through electronic systems. The development of digital services also increases the risk of data misuse if it is not accompanied by adequate safeguards and supervision (Ichsandi and Silalahi 1).

Another practice that expands the use of customer data is open banking and the integration of digital financial services. In this ecosystem, customer data may be connected to third parties through digital data exchange. Such integration can support service convenience, transaction efficiency, and financial innovation, but it also expands the range of parties that may potentially access or process customer data. Therefore, data exchange in the open banking ecosystem must be based on a legal basis, specific purposes, limits on use, system security, and clear accountability. Without such limits, the interconnection between banks and third parties may increase risks to customers' digital privacy (Rohmah and Ribawati 1-2).

Customer data may also intersect with state authorities through reporting, examination, and supervision. In certain circumstances, banks may be requested to provide information to authorized institutions for the purposes of supervision, examination, consumer protection, taxation, judicial proceedings, or other legal interests determined by laws and regulations. Financial Services Authority Regulation Number 44 of 2024 concerning Bank Secrecy shows that the disclosure of bank secrecy is possible, but only in certain circumstances and as an exception limited by law. Thus, the provision of customer data to the state or certain institutions must be specific, follow procedure, and be accountable.

Legal risks arise if customer data is used, requested, accessed, processed, or exchanged without adequate limits. The state or supervisory authority may indeed need certain data for supervisory purposes, but such need cannot be used as a reason to disclose all customer information. The data used must have a direct relationship with the purpose to be achieved, be relevant, and be truly necessary. The ransomware attack against Bank Syariah Indonesia in 2023 showed that disruption to electronic banking systems may affect the security of customers' personal data (Kholis 275-77). This incident shows that customer data protection depends not only on legal rules, but also on system readiness, access limitation, and effective accountability mechanisms.

Based on the above discussion, banking practice shows that customers' personal data is used in various activities, from account opening, identity verification, transaction monitoring, digital services, integration with third parties, reporting to authorities, to the disclosure of bank secrecy in certain circumstances. These practices prove that customer data may indeed be processed for lawful purposes, but not without limits. Every action involving customer data must have a legal basis, a clear purpose, traceable procedures, and be limited to relevant and necessary data. Thus, banking practice strengthens the importance of personal data protection as a legal limit to state authority in the supervision of the banking sector.

THE CONSISTENCY OF THE REGULATION AND EXERCISE OF STATE AUTHORITY WITH THE PROTECTION OF CUSTOMERS' PRIVACY RIGHTS

After personal data protection, bank secrecy, state supervisory authority, and the practice of customer data processing have been explained, this section assesses whether the regulation and exercise of state authority in the banking sector are consistent with the rule of law and the protection of customers' privacy rights. This assessment is important because banking supervision does not only concern the compliance of financial institutions, but may also create room for the state to request, access, use, process, or exchange customer data. Therefore, the measure of consistency is not merely whether authority exists, but also how that authority is limited, supervised, and held accountable.

Normatively, the Personal Data Protection Law provides a basis that personal data is an object that must be protected in every processing activity. In the banking sector, customer data has an important position because it can identify a person and describe the person's financial condition through account numbers, transaction histories, balances, credit data, and other financial information. In fact, personal financial data falls within the category of specific personal data. Therefore, every state action involving customer data, whether in the form of requesting, using, disclosing, or exchanging data, must remain within the framework of lawful, limited, secure, and accountable personal data processing.

In addition to general protection under the Personal Data Protection Law, the banking sector has special regulation through the principle of bank secrecy. The Banking Law and Financial Services Authority Regulation Number 44 of 2024 concerning Bank Secrecy show that customer information must basically be kept confidential, although in certain circumstances it may be disclosed based on legal provisions. This means that the disclosure of customer data is not absolutely prohibited, but it is also not authority that may be exercised

freely. Exceptions to bank secrecy must be understood as limited and procedural authority that may only be exercised for interests determined by laws and regulations.

From the supervisory perspective, the Financial Services Authority Law provides the basis for the state to regulate and supervise financial services activities, including banking. This authority is needed to maintain financial system stability, bank compliance, consumer protection, and the integrity of the banking sector. However, the authority of the Financial Services Authority remains limited by the obligation to maintain information confidentiality. This shows that in a rule-of-law state, supervisory institutions are not only granted authority to obtain information, but are also burdened with the obligation to use such information in a limited manner and in accordance with the legal purpose underlying it. In the context of digital banking services, this obligation must also be linked to electronic system security as regulated under the Electronic Information and Transactions Law.

If the relationship among these regulations is read systematically, Indonesian law has actually built a fairly complete protection framework. The Personal Data Protection Law provides basic principles of data processing, the Banking Law and the Financial Services Authority Regulation on Bank Secrecy provide sectoral protection, the Financial Services Authority Law provides the basis for supervisory authority, and the Electronic Information and Transactions Law affirms the importance of electronic system security. Therefore, state authority in banking sector supervision does not stand alone, but must be exercised together with obligations to protect personal data, bank secrecy, information security, and accountability in data use.

As a normative comparison, Singapore shows that customer data protection requires a combination of general rules and sectoral rules. The Personal Data Protection Act 2012 regulates personal data protection in general, while the Banking Act 1970 regulates the confidentiality of customer information in the banking sector. In addition, the existence of the Personal Data Protection Commission shows the importance of an institution that plays a role in the implementation and supervision of personal data protection. This comparison is relevant for Indonesia because the Personal Data Protection Law also mandates the establishment of an implementing institution for personal data protection. The existence of such an institution is important so that personal data protection does not stop as a norm, but can be implemented through effective supervision, coordination, enforcement, and accountability mechanisms (Yunanda et al. 15-18).

Although Indonesia's normative framework has moved toward the protection of customers' privacy rights, the main challenge still lies in implementation. In practice, requests for and use of customer data must truly be limited to data that has a direct relationship with the purpose of supervision. The state or supervisory authority must not use supervision as a reason to disclose data broadly without limits. This risk becomes greater in the open banking ecosystem because data exchange with third parties can expand the scope of access to customer data if it is not accompanied by clear limits on use and accountability (Rohmah and Ribawati 1-2). In addition, the development of digital financial services may also create overlapping authority among regulators if supervisory boundaries are not formulated clearly (Soeharlim et al. 854-858).

Therefore, the regulation and exercise of state authority in the supervision of the banking sector in Indonesia can be said to have a basis consistent with the principle of the rule of law and the protection of customers' privacy rights. However, such consistency still needs to be strengthened at the operational level, especially through limitations on the state's scope of access to customer data, inter-institutional coordination, electronic system security, the establishment of an effective personal data protection institution, and accountability mechanisms for the use of data. Accordingly, state authority in banking supervision must continue to be tested through legal basis, lawful purpose, data necessity, proportionality,

security, and accountability so that it does not become excessive authority over customers' personal data.

CONCLUSION

Personal data protection in the supervision of the banking sector functions as a legal limit to state authority when such authority intersects with customer data. The state may request, access, use, process, or exchange customer data for lawful supervisory purposes, but such actions must not be carried out freely. Every access to customer data must have a clear basis of authority, be directed toward a purpose justified by law, be limited to data that is truly necessary, and be implemented through secure and accountable procedures. Thus, personal data protection does not eliminate the state's supervisory function, but places that authority within measurable limits so that it does not become absolute authority.

Indonesian law has basically provided a foundation for the protection of customers' privacy rights in the supervision of the banking sector. This can be seen from the existence of the Personal Data Protection Law as the basis for personal data protection, the Banking Law and the Financial Services Authority Regulation on Bank Secrecy as special protection for the confidentiality of customer data, the Financial Services Authority Law as the basis for supervision of the financial services sector, and the Electronic Information and Transactions Law as the basis for electronic system security. However, the exercise of such authority still requires strengthening in operational limits, inter-institutional coordination, system security, personal data protection institutions, and accountability for the use of customer data. The comparison with Singapore shows that customer data protection will be more effective if it is built through the integration of general personal data protection rules, sectoral banking rules, and supervisory mechanisms capable of ensuring accountability.

RECOMMENDATIONS

The government and lawmakers need to strengthen the implementation of Articles 53 and 54 of the Personal Data Protection Law in the banking sector, particularly regarding officials or officers responsible for the personal data protection function. This strengthening is important because banks manage personal data on a large scale and process specific personal financial data. Therefore, the existence of officials or officers responsible for the personal data protection function must not be understood merely as an administrative obligation, but as an internal supervisory instrument to ensure that every processing of customer data is carried out lawfully, in a limited manner, securely, and accountably.

The Financial Services Authority and related institutions need to encourage the involvement of officials or officers responsible for the personal data protection function in policies and procedures relating to requests for, disclosure, use, and exchange of customer data. Such involvement is necessary so that every action involving customer data can be assessed from the outset in terms of legal basis, purpose, data necessity, scope of request, and risks to customers' privacy rights. In this way, data disclosure for supervisory, examination, or law enforcement purposes can still be carried out without disregarding the principle of personal data protection.

Banks as personal data controllers need to provide adequate position and authority to officials or officers responsible for the personal data protection function. Such officials or officers should play a role in providing compliance advice, monitoring the implementation of personal data protection, assessing data processing risks, documenting requests for the disclosure of customer data, and serving as a liaison among banks, authorities, and personal data subjects. By strengthening this role, the protection of customers' personal data can

operate as a real accountability mechanism, not merely as formal compliance with statutory provisions.

REFERENCES

Budhijanto, Danrivanto. Personal Data Protection Law in Indonesia: Cyberlaw & Cybersecurity. Refika Aditama, 2024.

Diyanatalia, Joan Lyne, Lu Sudirman, and Hari Sutra Disemadi. "Supervision by the Financial Services Authority and Its Impact on the Effectiveness of Consumer Data Protection at Rural Banks in Batam." Jurnal Hukum to-ra: Law to Regulate and Protect Society, vol. 11, no. 3, 2025, pp. 546-571. doi:10.55809/tora. v11i3.592.

Government of Singapore. Banking Act 1970. 1970.

Government of Singapore. Personal Data Protection Act 2012. 2012.

Ichsandi, Muhammad Wildan, and Wilma Silalahi. "The Urgency of Personal Data Protection in the Banking Sector in the Digital Era." Rewang Rencang: Journal of Lex Generalis Law, vol. 5, no. 12, 2024.

Johan, Erik Syaputra. "The Role of the Financial Services Authority in Protecting the Security and Confidentiality of Customers' Personal Data in Banking Products in the Digital Era." Mahalini: Journal of Business Law, vol. 2, no. 1, 2025, pp. 24-38.

Kholis, Ilman Maulana. "Personal Data Protection and Cybersecurity in the Banking Sector: A Critical Study of the Implementation of the Personal Data Protection Law and the Electronic Information and Transactions Law in Indonesia." Staatsrecht: Journal of Constitutional Law and Islamic Politics, vol. 4, no. 2, 2024, pp. 275-299. doi:10.14421/t5sfe747.

Nasution, Rafi Aulia, et al. "Legal Protection of Customers' Personal Data in Banking Services after the Enactment of Financial Services Authority Regulation Number 6/2022." Journal of Education, Humaniora and Social Sciences, vol. 7, no. 1, 2024, pp. 71-78. doi:10.34007/jehss. v7i1.2292.

Financial Services Authority. Financial Services Authority Regulation Number 44 of 2024 concerning Bank Secrecy. 2024.

Paramitha, Amelia Ayu, et al. State Administrative Law. Edited by Anik Iftitah, Sada Kurnia Pustaka, 2023.

Prayogo, P., R. S. M. Korah, and M. H. Soepeno. "An Analysis of the Legal Protection of Customers' Personal Data in Digital Transactions." Journal of Banking Law, vol. 9, no. 1, 2024, pp. 39-54.

Putri, N., et al. "A Juridical Analysis of Bank Customer Protection in the Crime of Data Theft through the Electronic Information and Transactions Law and the Banking Law." Journal of Criminal Law and Banking, vol. 2, no. 4, 2024, pp. 926-934.

Republic of Indonesia. Law Number 7 of 1992 concerning Banking. 1992.

Republic of Indonesia. Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking. 1998.

Republic of Indonesia. Law Number 11 of 2008 concerning Electronic Information and Transactions. 2008.

Republic of Indonesia. Law Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering. 2010.

Republic of Indonesia. Law Number 21 of 2011 concerning the Financial Services Authority. 2011.

Republic of Indonesia. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. 2016.

Republic of Indonesia. Law Number 27 of 2022 concerning Personal Data Protection. 2022.

Republic of Indonesia. Law Number 4 of 2023 concerning Financial Sector Development and Strengthening. 2023.

Republic of Indonesia. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. 2024.

Rohmah, Latifah Nur, and Eko Ribawati. "The State's Obligation to Protect the Digital Privacy Rights of Islamic Bank Customers in the Open Banking Era." Scientific Journal of Economics and Management, vol. 3, no. 12, 2025, pp. 1-13. doi:10.61722/jiem. v3i12.7270.

Santoso, Joko Tri, and Agus Wibowo. Cyber Law and Information Security. 2024.

Sirait, Lisa Novita. "Authority for Banking Regulation and Supervision in Accessing Financial Information for Taxation Purposes by the Directorate General of Taxes." Journal of Social and Science, vol. 1, no. 11, 2021, pp. 1533-1541. doi:10.59188/jurnalsosains. v1i11.291.

Soeharlim, Irwan, et al. "The Dynamics of the Boundaries of Supervisory Authority between the Financial Services Authority and Bank Indonesia over Fintech Activities in the Banking Sector." Berajah Journal, vol. 6, no. 3, 2026, pp. 854-858. doi:10.47353/bj. v6i3.522.

Wibowo, Kurniawan Tri, et al. Digital Law and Data Privacy. Edited by Muhammad Syaukani, CV Al-Haramain Lombok, 2025.

Yakovleva, Svetlana. Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law. Hart Publishing, 2023.

Yunanda, Veris, et al. "The Urgency of Establishing LPPDP as an Effort to Strengthen Personal Data Protection: A Comparison between Indonesia, Hong Kong and Singapore." Scientific Journal of Law and Human Rights, vol. 4, no. 1, 2024, pp. 11-25. doi:10.35912/jihham. v4i1.2962.