

REGULATING FINANCIAL DIGITAL INNOVATION: A STUDY DATA SHARING ON BANK AND FINTECH COLLABORATION

Valentino Gola Patria

PT Bank Mandiri, Indonesia,
tvalen223@gmail.com

Abstract

Banks are challenged to innovate in developing their products and services to retain their customers. One way for banks to improve their ability to develop digital financial products and services is by collaborating with fintech companies. The use of data is one of the important aspects in bank and fintech collaboration to improve digital products and services. Data sharing through Application Programming Interface (API) or known as Open Banking has been widely utilised by financial industry players, both banks and fintechs. This research aims to explore how data sharing arrangements between banks and fintechs in collaboration to develop their digital products and services. From the results of the research, currently the regulation of data sharing in the financial industry is carried out by Bank Indonesia in the payment system. In the regulation, Bank Indonesia involves SROs to create a standard known as Standard National Open API (SNAP), based on the research study, it is necessary to strengthen the regulation of several aspects including standard governing body, data governance aspects and IT risk management so that consumer protection and personal data protection can be further improved.

Keywords: *Open Banking; Open API Standard; Fintech Collaboration*

1. INTRODUCTION

The presence of information technology is increasingly widespread in its utilization in various activities of human life. Many countries in the world see this information technology as a strategic thing for the country, including Indonesia. The importance of information technology can be seen in the Okinawa declaration which states that countries, especially developed countries, that fail to keep up with the acceleration of information technology will eliminate the opportunity for these countries to participate in the information society and the world economic community. Changes due to advances in information technology bring greater challenges for the government. One of the impacts is the increasingly complex social changes, ranging from changes in mindsets to lifestyles that have an impact on how business actors in various sectors adjust their business models.¹

The government regulates the use of information technology and electronic transactions aimed at not only educating the nation's life as part of the world information society, but also in the development of trade and the national economy. Information technology is also intended to increase the effectiveness and efficiency of public services, including opening the widest possible opportunity for everyone to advance their thoughts and abilities in the field of the use and utilization of information technology as optimally as possible and

¹ Kemenkominfo Balitbang SDM, *Perkembangan Ekonomi Digital di Indonesia* (Jakarta: Puslitbang Aptika dan IKP, 2019), i.

responsibly as well as providing a sense of security, justice, and legal certainty for users and organizers of information technology.² The use of information technology has fostered economic activities that are often known as the digital economy. The digital economy is a business transaction activity carried out via the internet. Indonesia is one of the countries that has great potential and opportunity to play a role in the digital economy. The financial sector is one of the business sectors that play a role in the digital economy. Technological advances in the financial sector have encouraged community transactions to become more non-cash (cashless) and contributed to the efficiency of financial transactions for the community and the business world.

The impact of the development of information technology today, people are increasingly demanding financial services that can not only be accessed online but also with easier rules or requirements.³ In addition to banks, non-bank financial institutions are also starting to grow and provide digital financial services. The impact of the development of information technology today is people are increasingly demanding financial services that can not only be accessed online but also with easier rules or requirements. The development of technology used in the financial sector has given birth to many innovations accompanied by the proliferation of financial technology companies or financial technology (hereinafter referred to as fintech). Fintech is the result of a combination of financial services with technology that ultimately changes the business model from conventional to moderate, which initially in paying must be face-to-face and carry a number of cash, can now make remote transactions by making payments that can be made in a matter of seconds.⁴

The government continues to accelerate the digitalization of the national economy and finance, including efforts to accelerate the digitalization of the national economy and finance in the areas of fiscal policy, network infrastructure, and the readiness of the banking and national financial sectors.⁵ This is increasingly forcing banks to transform their digital services. According to Brett King, banks still have four options to respond to these changes, namely:⁶ (1) Do nothing, which will ultimately result in a decline in performance and will continue to be costly; (2) Partner with Fintech, which is the cheapest and fastest approach to technology adoption; (3) Acquire Fintech, where technology adoption can be faster, but still more expensive and potential culture barriers within the organization; and (4) Copy Fintech innovations, where this will be slow and very expensive.

Infosys, one of the world's leading banking technology companies, said that “the world of banking is being disrupted at a staggering pace”. Currently, banks are highly controlled by regulations, thus losing focus on technological innovation. With financial technology

² Article 4 Indonesian Electronic Information and Transaction Law Number 19 Year 2016 as amendment to Indonesian Electronic Information and Transaction Law Number 11 Year 2008.

³ Kemenkominfo Balitbang SDM, *Perkembangan Ekonomi Digital di Indonesia* (Jakarta: Puslitbang Aptika dan IKP, 2019), 21.

⁴ Bank Indonesia, “Mengenal Financial Technology, Departement Komunikasi,” *Bank Indonesia*, December 1, 2018, <https://www.bi.go.id/id/edukasi/Pages/mengenal-Financial-Teknologi.aspx>.

⁵ Jihaan Khoirunnisaa, “Ini Strategi Pemerintah Kembangkan Ekonomi Keuangan Digital,” *Detik*, April 5, 2021, <https://finance.detik.com/berita-ekonomi-bisnis/d-5520894/ini-strategi-pemerintah-kembangkan-ekonomi-keuangan-digital>.

⁶ Brett King, *Bank 4.0: Banking Anywhere, Never at a Bank* (Singapore: Marshall Cavendish Business, 2018), 319.

companies disrupting their markets, banks are trying to build new strategies to catch up.⁷ Various strategies and new business models have been developed by banks to provide digital services to their customers. The new business models come from existing banks as well as newly formed banks that only focus on digital services. For banks that already exist, one way that can be done is to adopt technology in improving digital banking services.

In developing products and services, information in the form of data is needed. Technological developments including the use of APIs (Application Programming Interface) have opened up more avenues for banks and fintech to collaborate. With the current development of information technology, providing data access can be done through open application programming interface API (Open API). Banks can open customer data to third parties (including fintech) through open API reciprocally, so that third parties can develop new products and services with ease of transactions.⁸ In digital finance, data is important for banks and fintechs in developing products and services. One manifestation of bank and fintech collaboration in digital finance is the utilization of data owned by banks and fintechs. The concept of data sharing between banks and third parties, in this case fintechs that use Open Application Programming Interface (Open API) in the payment system, is known as Open Banking, while Open Finance is an extension of Open Banking where data is also shared with parties outside the payment system. The purpose of Open Banking and/or Open Finance is to maintain a level playing field, prevent monopoly, and increase financial inclusion.⁹

There are three parties involved in API implementation, namely customers as data owners, banks, and fintech with a collaborative model. This model encourages the disclosure of bank and fintech financial information to third parties in a secure manner. The public is facilitated in making transactions and allowing interlink activities of two or more unaffiliated parties to increase the capabilities of each party. Bank and fintech collaboration in Indonesia is generally initiated by large banks with varied patterns, including investment through incubation programs. For banks, the presence of fintech can be utilized to sharpen consumer centric services or as a third party service provider to provide various services ranging from market support to supporting bank intermediation activities. Central Bank of Indonesia (Bank Indonesia) sees that the Payment Open API applied by various payment service players for payment transaction processing at the pre-transaction, initiation, and authorization stages has not been standardized. This has led to inefficiencies in the development and maintenance of the Payment API, not achieving interconnection, interoperability, and compatibility of the Payment Open API linkage.¹⁰

⁷ Infosys, "Banking as a Platform: A New Age Transformation," <https://www.infosys.com/iki/perspectives/new-age-transformation.html>.

⁸ Explanation of Regulation of the Members of the Board of Governors of Bank Indonesia Number 23/15/PADG/2021 on Implementation of the National Standard for Open Application Programming Interface for Payments.

⁹ Bank Indonesia, *Blueprint Sistem Pembayaran (BSPI) 2025* (Jakarta: Bank Indonesia, 2019).

¹⁰ *Ibid.*

However, the utilization of information technology definitely has both positive and negative impacts and it is natural to be aware of it.¹¹ The utilization of information technology in the financial sector, often known as financial technology (fintech), has made it easier for people to carry out financial transactions in their economic activities, but on the other hand it also creates the risk of cybercrime in the financial sector. There is a need for readiness from industry players and regulators in dealing with this impact. According to Tony, Acting Deputy Director of Financial Services Authority's Indonesian Banking Architecture, there are several risks that can arise from banking and fintech collaboration, namely: the protection and exchange of personal data; the risk of customer data leakage; cyber attacks; and outsourcing risks.¹²

If observed, the emergence of banking data sharing in Indonesia was initially implemented in a limited scope with certain contract schemes which were generally bilateral contracts through the use of open partner APIs. For example, Bank Central Asia (BCA) launched a website containing a list of APIs for developers to incorporate BCA services in their platforms or applications. In addition, Bank Mandiri has also opened an API for e-money products with the aim of allowing start-up companies to experiment with the service. In addition to these two banks, banks such as Bank Rakyat Indonesia (BRI), Bank Negara Indonesia (BNI), Permata, CIMB Niaga, Bukopin, Bank Tabungan Negara (BTN), and Bank Tabungan Pensiunan Nasional (BTPN) have started to open their API access to fintech companies for product and service collaboration.

In the bilateral cooperation scheme, it appears that a number of crucial elements in the cooperation contract are missing from the contract clause, especially aspects of consumer data protection (for example, customer consent), general consumer protection and risk management. The implementation is also constrained by a number of internal and external aspects. Internally, the implementation of data sharing using Open API is faced with high implementation costs, dependence on legacy systems, and limited talent. Externally, the constraints stem from limited regulatory support.

The development of data sharing in Indonesia can be said to have been born due to the need for innovation in product and service development, but this was done on a limited basis by banks and their cooperation partners, which was carried out in a fragmented manner so that Bank Indonesia took steps to standardize the API. So it can be said that the implementation of data sharing using Open API in Indonesia was initially market driven, but in its development it became Regulatory Driven.

Bank Indonesia sees that the Payment Open API applied by various payment service actors for payment transaction processing at the pre-transaction, initiation, and authorization stages has not been standardized. This causes inefficiencies in the development and maintenance of the Payment API, not achieving interconnection, interoperability, and compatibility of the Payment Open API linkage. Furthermore, the standardization of the Open API was included by Bank Indonesia as one of a series of policies in implementing the

¹¹ Djon S. Gazali and Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2016), 39.

¹² Dina Mirayanti Hutaeruk, "Ini Risiko yang Dihadapi dalam Kolaborasi Antara Bank dengan Fintech," *Kontan.co.id*, June 10, 2021, <https://keuangan.kontan.co.id/news/ini-risiko-yang-dihadapi-dalam-kolaborasi-antara-bankdenganfintech>.

vision of the payment system. The policy direction is in line with developments in other countries that have adopted the Open Banking concept. Standardization covers aspects that are also best practice in many countries to encourage a healthy digital ecosystem.

The inclusion of Bank Indonesia as the payment system authority that standardizes the Open API has provided an opportunity for parties to implement the Open API without fragmentation so as to increase healthy competition in making products and services that benefit customers. In addition to the interests related to market competition, innovation, and consumer empowerment as described above, regulation of data sharing is also very much needed given the emergence of new risks of misuse and data breaches that occur in the world today. This research discuss more on consumer and personal data protection implementation in Payment Systems SNAP API by analyzing several aspects, namely standard governing body, contract standards, consumer protection, and minimum requirements for third parties.

2. RESEARCH METHODS

The type of research used in this research is normative legal research. Normative legal research is an approach that is carried out based on the main raw material, examining theoretical matters concerning legal principles, legal conceptions, views and legal doctrines, regulations and legal systems using secondary data, including: principles, rules, norms and legal rules contained in laws and regulations and other regulations, by studying books, laws and regulations and other documents that are closely related to the legal issues studied.¹³

Based on its nature, this research uses qualitative research methods with descriptive analytical research on consumer and data protection implementation in Payment Systems SNAP API. Qualitative normative juridical research is research that refers to legal norms contained in laws and court decisions as well as norms that live and develop in society. Analytical descriptive research is a form of research aimed at describing existing phenomena, both natural and man-made phenomena.¹⁴ Analytical descriptive research is research that reveals laws and regulations related to legal theories that are the object of research.

3. ANALYSIS AND DISCUSSION

The development of data sharing in Indonesia can be said to have exist due to the need for innovation in product and service development, but this was done on a limited basis by banks and their cooperation partners, which was carried out in a fragmented manner so that Bank Indonesia took steps to standardize the API. So it can be said that the implementation of data sharing using Open API in Indonesia was initially market driven, but in its development it became Regulatory Driven. Currently, arrangements related to data sharing using Open API are more regulated in the payment system by Bank Indonesia, especially in arrangements related to the Standard National API (SNAP). However, in best practice, Open API governance is a unity of aspects between the standard governing body, contract

¹³ Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (Depok: Rajawali Pers, 2019), 13.

¹⁴ Zainuddin Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2010), 105.

standards, consumer protection, and minimum requirements for third parties in the cooperation of open API implementation.

3.1. Implementation of the Payment System Open API Governing Body Standards

Standard Governing body-Open API, among others, has a role to participate in compiling Open API standards and technical guidelines which become a reference for each Open API organizer that can support the creation of an open API ecosystem with integrity. As for the implementation of open banking in Indonesia as an implementation of Bank Indonesia's vision in the payment system, Bank Indonesia together with the Indonesian Payment System Association (*Asosiasi Sistem Pembayaran Indonesia*/ASPI) and representatives of the payment system industry (major players in the banking and fintech sectors who are members of ASPI, along with several related parties such as e-commerce and Payment Gateway players) formed a working group in the preparation of the National Standard for Payment Open Application Programming Interface (hereinafter SNAP).¹⁵

Since its launch on August 17, 2021, SNAP management has been carried out by Bank Indonesia for the first time. However, as of September 1, 2023, Bank Indonesia has transferred the management of the SNAP to ASPI. When viewed from the scope of SNAP management, what ASPI does is limited to the authority stipulated by Bank Indonesia, among others related to the management of the SNAP developer site system, evaluation and updating and SNAP Publication. ASPI as a Self Regulatory Organization has issued the SNAP Governance Guidelines, Data Standards and Technical Specifications, Technical and Security Standards. In accordance with PBI National Standard for Payment System, the standard guidelines issued by ASPI as Self Regulatory Organization (SRO) are approved by Bank Indonesia and established as National Standard, the ownership of the standard passes to Bank Indonesia when the standard is established as National Standard.¹⁶

The appointment of ASPI as a Standard Governing Body that prepares and/or manages Open API standards, in the opinion of researchers, is currently inadequate. With the growing need for data sharing not only for financial service institutions engaged in payment systems but also financial service institutions outside the payment system including fintech, a body that specifically handles the implementation and development of data standards and is responsible for its implementation is needed. With such a specialized entity, the governance and development of Open Banking can be better regulated. The Open Banking Implementation Entity (OBIE) in the UK is one example of a standard governing body that can be used as a reference. OBIE is known as Open Banking Limited (OBL), the Implementation Entity described in the CMA Order, is private limited. There is one task performed by OBL that does not fall within the scope of ASPI's duties, which is related to the management of redress mechanisms and dispute management systems. This is a crucial issue that may arise due to claims for

¹⁵ Asosiasi Sistem Pembayaran Indonesia, "Kick-Off Meeting Pembentukan WG Nasional Open API," *ASPI*, June 16, 2020, <https://www.aspi-indonesia.or.id/kick-off-meeting-pembentukan-wg-nasional-openapi/>.

¹⁶ Article 9 of Regulation of Bank Indonesia Number 23/PBI/2021 on National Payment System Standard.

damages in the event of disputes between the parties in the implementation of open banking.

3.2. Types of Data in Indonesian Law

Law Number 27 of 2022 of Personal Data Protection (hereinafter referred to as PDP Law) divides types of Personal Data into two types, which are general personal data and specific personal data.¹⁷ Specific personal data includes health data and information, biometric data, genetic data, crime record, child data, personal financial data¹⁸ and other data in accordance with the provisions of law and regulations. When examined closely, the list of Specific Data in the PDP Law resembles sensitive data which is “special categories of data” in the United Kingdom’s General Data Protection Regulation (UK GDPR) which requires a higher level of protection. Sensitive data requires greater protection and stricter processing, because in principle it is personal data that is prohibited from being processed because it will jeopardize the fundamental rights of people.¹⁹ The types of general data include full name, gender, citizenship, religion, marital status, and personal data combined to identify a person. So based on the Indonesian PDP Law, personal financial data is specific data. Specific Personal Data is Personal Data which, if processed, may result in a greater impact on the Personal Data Subject, including acts of discrimination and greater harm to the Personal Data Subject.²⁰

Inregards to Financial Data, Regulation of the Board Member of Central Bank Governors Number 23/15/PADG/2021 on the Implementation of the National Standard for Payment Open Application Programming Interface stipulates regarding the standard data categories, namely: registration, balance information, transaction history information, credit transactions, debit transfers and other categories applied by Bank Indonesia. In the SNAP Governance Guidelines, each of these categories is further elaborated as follows: (1) Registration, data required for consumers to be able to link their data in conducting payment transaction services or accessing their data; (2) Balance Information, data required for Consumers, Non-PJP Service Users, PJP Ains, and PJP PIAS to be able to access the latest balance information of their accounts in real time, in accordance with the services provided by PJP AIS;²¹ (3) Transaction History, data required so that Consumers, Non-PJP Service Users, or PJP PIAS can access transaction history information from their accounts in real time, in accordance with the services provided by PJP AIS; (4) Credit Transactions, which is used to transfer funds from one account to another account either in the same PJP AIS or different PJP AIS

¹⁷ Article 4 of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*.

¹⁸ Explanation of Article 4(2) of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*, what is meant by personal financial data includes but is not limited to data on the amount of deposits in banks including Savings, deposits and credit card data.

¹⁹ European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Austria: European Union Agency for Fundamental Rights, 2018), 96.

²⁰ Explanation of Article 4(1) of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*.

²¹ PJP (*Penyedia Jasa Pembayaran*) is Payment Service Provider; AInS is Account Information Services; PIAS is Payment Initiation and Acquiring Services; IAS is Account Issuance Services.

initiated by the sending party (debited party); (5) Debit Transactions, which is used to transfer funds from one account to another account both within the same PJP AIS and different PJP AIS initiated by the receiving party (credited party) and other types of information such as Response Status, which is information provided by the service provider to the service consumer in the response body, as an indication of the results of processing the received request. Response status consists of two components, namely the code (response code) and its description (response message). The processing and use of sensitive data, including financial data, requires the consent of the data owner who is subject to the PDP Law.

3.3. Implementation of Regulatory Sandbox for Fintech and Piloting Mechanism and Verification of National Standard Implementation

To ensure that fintech providers meet the set criteria, both Bank Indonesia and the Financial Services Authority (*Otoritas Jasa Keuangan/OJK*) have organized a Regulatory Sandbox and piloting and verification process. Regulatory sandbox is one of the stages in smart regulation,²² which is used in regulating the development of fast-changing innovations. There are four stages in Smart Regulation, namely: (i) Testing and Piloting Environment; (ii) Regulatory Sandbox; (iii) Restricted Licencing/Special Charter Scheme; (iv) Full License. Bank Indonesia regulates that Fintech providers who will participate in the regulatory sandbox must be registered with Bank Indonesia, this is slightly different from the requirements of OJK which requires that they must also be registered with the organizing association.²³ According to the author, it is necessary to synchronize and standardize the registration requirements for the regulatory sandbox, this is to also optimize the role of the Association as an SRO. According to the author, the implementation of this regulatory sandbox is a new way of regulating based on prudential principles from Bank Indonesia and OJK in the face of developments and changes in products and technology in the fintech industry, regulatory sandboxes in various countries are a learning arena including for regulators, so that the direction of licensing given is expected to be not wrong and not high risk.²⁴

Regulatory sandbox is expected to answer challenges such as the lack of capacity of regulators and the development of existing financial market infrastructure for fintech providers as well as the difficulty of balancing aspects of financial inclusiveness with financial market security principles such as stability, integrity, consumer protection and fair competition,²⁵ as well as minimizing the potential losses suffered by consumers and the financial system with disruptive innovations that are not accompanied by proper studies because the sandbox becomes a laboratory for these ideas before being released

²² Dirk A. Zetzche, Ross P. Buckley, Janos N. Barberis, and Douglas W. Arner, "Regulating a Revolution: From Regulatory Sandbox to Smart Regulation," *Fordham Journal of Corporate & Financial Law* 23, no. 1 (2017): 31–103, <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1450&context=jcfl>.

²³ Article 8 of *Regulation of Financial Services Authority Number 13/POJK.02/2018 on Digital Finance Innovation in the Financial Services Sector*.

²⁴ Dea Chadiza Syafina, "Mengenal Regulatory Sandbox, Rahim dari Kelahiran Para Fintech," *Tirto.id*, April 26, 2018, <https://tirto.id/mengenal-regulatory-sandbox-rahim-dari-kelahiran-para-fintech-cJpW>.

²⁵ Ivo Jenik and Kate Lauer, *Regulatory Sandboxes and Financial Inclusion* (Washington D.C.: CGAP, 2017), 2.

to the market.²⁶ Piloting and verification of National Standard Implementation is conducted through the Payment System Open API Testing Application on the SNAP Developer site. The SNAP-based Payment Open API pilot is online within the scope of SNAP's technical security standards, data standards and technical specifications. The Open API trial through the Application at the Developer Site aims to test the conformity of the Payment Open API development with technical and security standards, data standards, and SNAP technical specifications. The purpose of verification is to ensure that service providers and service users who develop open APIs are in accordance with technical and security standards, data standards, and SNAP technical specifications and have passed functionality testing.

3.4. Application of Agreement Standards and Consumer Consent in Data Sharing Cooperation using Open APIs

The parties' agreement in sharing data using the Open API, in this case the cooperation carried out by the Bank and Fintech, both as service providers and users of the Payment Open API service, is based on the existence of a standard contract. The object of the contract is related to customer data.

3.4.1. Open API Contract Standard

The Open API contract standard is part of open API governance which aims to regulate the minimum clauses that must be included in the Open API Cooperation contract including the rights and obligations of the parties and compliance with laws and regulations. The Cooperation Contract is a manifestation of the freedom of contract stipulated in the Civil Code. This freedom of contract is the basis for filling the void in the field of open contract law, with the intention that the law can meet the needs of society in accordance with the dynamics of economic development and can be a tool of social engineering. The Payment Open API Governance contains general principles and minimum clauses that are standardized in the Payment Open API service contract.

General Principles of the Payment Open API Contract include: (1) The contract can be made in the form of an agreement or in the form of general terms and principles; (2) The contract contains the minimum clauses stipulated by Bank Indonesia and can be added with other clauses deemed necessary by the Service Provider and/or Service User PJP; (3) The preparation of the contract takes into account the laws and regulations, including in terms of the implementation of Open API Payment services; (4) Contains things that must be done and things that are prohibited; (5) The language used in the agreement is Indonesian and can be paired with English or other foreign languages. However, in the event of a dispute or inconsistency, the agreement clause in Indonesian shall prevail.

²⁶ *Ibid.*, 3.

The minimum clauses included in the Open API service contract between service providers and service users include at least the following: (1) Parties. The contract is made by the parties authorized to represent the Service Provider and/or PJP Service User, either based on their own authority or based on a power of attorney; (2) Definitions. This section includes important terms used in the Payment Open API service that is the scope of the Cooperation; (3) Scope. This section describes the scope or limitations of the Payment Open API service provided by the Service Provider to the PJP Service User; (4) Cooperation Period. Termination of Cooperation, and Temporary Termination; (5) Data Confidentiality Service Providers and PJP Service Users include the obligation to maintain data confidentiality which at least contains the obligation of Service Providers and PJP Service Users to maintain data confidentiality including but not limited to confidential information of a technical or commercial nature in accordance with laws and regulations; (6) Handling of Consumer Complaints Service Providers and PJP Service Users establish a mechanism for handling consumer complaints which can be further regulated in a separate document, which is an integral part of the contract; (7) Dispute Resolution. In the dispute resolution mechanism at least contains: The parties prioritize the settlement of disputes by deliberation to reach consensus if there is a dispute between the Service Provider and PJP Service User. In the event that deliberation to reach consensus is not reached, it is necessary to regulate settlement through a judicial institution or outside the judicial institution. Dispute resolution is carried out in accordance with the legal domicile agreed by the parties.

In addition to the general principles and minimum clauses, the Open API service contract can add additional clauses including: (i) Transaction SLA; (ii) Service Fees and Taxes; (iii) Data Reconciliation; (iv) Promotion and Socialization. In the event that the Service Provider cooperates with Non PJP Service Users and other parties in the implementation of Open API Payment services, the Service Provider ensures that these parties apply contract standards as stipulated in the SNAP governance guidelines and include these matters in the contract.

The regulation of standard contracts in SNAP aims to ensure the rights and obligations of the parties regarding the use of data as well as ensuring consumer protection and protection of consumer personal data are carried out by each party. Thus, the Bank and Fintech cooperation agreement in data sharing is a consensual, obligatory and real agreement, meaning that it contains an agreement regarding the rights and obligations of each party followed by the delivery of the agreed object and is reciprocal.

3.4.2. Consumer Consent

One important aspect in data sharing is related to consumer consent. The regulation on consumer consent is contained in the PDP Law where in processing personal data, the personal data controller must obtain explicit legal consent from the Personal Data Subject for one or several specific purposes that have been conveyed by the Personal Data Controller to the Personal Data Subject.²⁷

The implementation of the PDP Law related to Consumer consent is further regulated in Bank Indonesia Regulation Number 03 of 2023 on Bank Indonesia Consumer Protection which regulates the obligation to obtain customer consent before sharing data to other parties.²⁸ As for this consent, OJK also regulates this in Financial Services Authority Regulation Number 22 of 2023 on Consumer Protection in the Community in the Financial Services Sector, where the exchange of data and/or information on consumers in the financial sector as long as they get written consent from consumers.²⁹ Both Bank Indonesia Regulation and Financial Services Authority Regulation still regulate general matters related to consent, for this reason, in the author's opinion, because consent must be explicit, so that details such as the purpose of using data, what information, and the rights of data subjects, as well as mechanisms for submitting consent, canceling and so on need to be regulated completely in a clear format.

Arrangements related to consumer consent in SNAP are regulated in Chapter II of Governance Guidelines related to Consumer Protection and Chapter III of Governance Guidelines related to Data Protection. In Chapter II related to Consumer Protection, it is stated that Service Providers and PJP Service Users in the implementation of the Payment Open API obtain consumer consent for the use of consumer data.

When examined, there are several things in the PDP Law that have not been regulated in the SNAP Governance Guidelines related to information that must be conveyed to consumers in providing consent related to personal data processing, including the type and relevance of Personal data to be processed, the retention period of documents containing Personal data, the period of data processing, details about the information collected, and the rights of the Personal Data Subject. According to the author, Bank Indonesia and the SROs must regulate matters related to information to consumers who own this data in detail in the SNAP Governance Guidelines so that there is no ambiguity in the application of matters related to Consumer Consent which can cause obstacles in the implementation of obtaining consumer consent in the field and reduce the legal certainty of the parties involved in sharing data through the Open API.

3.5. Consumer Protection and Personal Data Protection in Payment System Open APIs

Service providers and PJP service users in implementing consumer data protection refer to the provisions of Bank Indonesia and laws and regulations. With the issuance

²⁷ Article 20(2) of Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection.

of the PDP Law, the regulation of consumer data protection in the implementation of Open API should also refer to this Law. Important matters in the PDP Law include types of personal data, rights of personal data subjects, processing of personal data, transfer of personal data, dispute resolution, should be further regulated in the rules below including the implementation related to the Open API Payment both issued by Bank Indonesia and by the Payment System SRO.

3.5.1. Personal Data Subject Rights in SNAP API

Based on the review of the regulation of data subject rights regulated by Bank Indonesia and payment system SROs in the SNAP governance guidelines and data subject rights regulated in the PDP Law. There are several data subject rights that have been regulated in the SNAP Governance Guidelines, but there are several data subject rights that have not been regulated or need further explanation so as not to conflict with the PDP Law. Matters that have not been explicitly regulated or need further clarity relate to first, the right to obtain a copy of personal data about him/her. This has not been regulated in the SNAP API governance guidelines. Secondly, the right to object to decision-making actions based solely on automated processing, including profiling, that give rise to legal consequences or have a significant impact on the personal data subject. Further provisions on this matter will be regulated in a Government Regulation. This too has not been regulated in the SNAP API Governance Guidelines.

Third, the right to suspend or restrict processing of personal data in proportion to the purposes for which the personal data is processed. This has not been explicitly regulated in the SNAP Governance Guidelines. Fourth, the right to sue and receive compensation for the violation of the processing of personal data about him/her in accordance with the provisions of laws and regulations. Provisions related to violations of personal data processing and procedures for the imposition of compensation have not been regulated in the SNAP Governance Guidelines. Finally, fifth, the right to obtain and/or use personal data about him/her from the controller of personal data in a form that is in accordance with the structure and/or format commonly used or readable by electronic systems. Personal data subjects have the right to use and transmit personal data about themselves to other personal data controllers, as long as the systems used can communicate with each other securely in accordance with the Principles of personal data protection. Provisions related to the right to use and transmit personal data are not yet regulated in the SNAP Governance Guidelines.

According to the author, the rights of the subject of personal data need to be regulated completely and explicitly in the SNAP Governance Guidelines issued by ASPI which is a standard reference related to the implementation of Open APIs

²⁸ Article 35 of *Regulation of Bank Indonesia Number 03/2023 on Bank Indonesia's Consumer Protection*.

²⁹ Article 20 of *Regulation of Financial Services Authority Number 22 of 2023 on Consumer and Community Protection in the Financial Services Sector*.

used in Bank and Fintech collaboration so as to reduce the potential for violations of the Law related to Personal Data Protection.

3.5.2. Personal Data Transfer and Data Portability

In the PDP Law, it is possible for the Controller of personal data to transfer or receive the transfer of personal data to another Controller of personal data within the jurisdiction of Indonesia as long as it fulfills the provisions of personal data protection in the Indonesian PDP Law.³⁰ The PDP Law regulates matters related to data portability currently, as follows:

- a. The personal data subject has the right to obtain and/or use Personal Data about him/her from the Personal Data Controller in a form that is in accordance with the structure and/or format commonly used or readable by electronic systems.³¹
- b. The personal data subject has the right to use and send Personal Data about him/her to other Personal Data Controllers, as long as the systems used can communicate with each other securely in accordance with the principles of personal data protection under the PDP Law.³²

In the author's opinion, the enactment of these two articles will make it difficult to implement data portability in the field. The clarity of the form and structure or format in this article must be clarified, because the structure and format of the data owned by the data controller will depend on the system used. Currently, the standardization of the form and structure or format of data has been regulated in the SNAP Payment system, but for data standards in the use of Open API outside the Payment system has not been regulated. According to the author, standardization is needed in this regard.

3.6. Implementation of the Precautionary Principle and Risk Management in Data Sharing using the Open API

The Open API Governance Guidelines regulate the precautionary requirements for service providers and service users in the implementation of Open API services in order to mitigate the risks that can occur. The application of the precautionary principle includes, among others:

1. Principles of good governance and prudence for Service Providers and PJP Service Users;
2. Monitoring the fulfillment of PJP Service User requirements by Service Providers;
3. Periodic monitoring by Service Providers and PJP Service Users; and
4. Preparation of Open API Payment Service Cooperation.

Security standards are part of the National Payment Open API Standard which aims to ensure data confidentiality, data and system integrity, and service availability,

³⁰ Article 55 of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*.

³¹ Article 13(1) of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*.

³² Article 13(2) of *Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection*.

regulating standards for authentication, authorization, encryption to ensure data integrity and confidentiality, the existence of a business continuity plan, as well as the implementation of a fraud detection system to mitigate potential fraud. Although SNAP has set strict Technical and Security Standards to protect sensitive data. However, in my opinion, there are still some security risks that must be considered, namely: attacks on Banks and Fintech companies, which have different security measures, that have access to the Open Banking API; and attacks on Open Banking site developers themselves. AFPI as the SNAP Manager including the Developer Site must be able to safeguard against possible cyber-attacks. This security by AFPI is only generally regulated in the PBI National Standard which regulates the obligation of SROs as Standard Managers to ensure the security and reliability of information systems used in the preparation and/or management of National Standards.³³

In the author's opinion, the obligations of ASPI as standard governing body need to be regulated further because it has not been regulated in the SNAP governance standard which is more related to Service Providers and Service Users. Matters that need to be regulated include AFPI Governance in IT Security, considering that AFPI is an Association which is certainly different from the risk management practices of Bank and Fintech technology that have been regulated by OJK and Bank Indonesia. Regarding the implementation of prudential principles and risk management that must be carried out by Service Providers and PJP Service Users in the form of implementing Good Governance and applying prudential principles, monitoring the fulfillment of requirements and periodic monitoring by Service Providers of Service Users, in my opinion it will be quite troublesome for Service Providers, To facilitate this, according to the author, it is necessary to involve third parties, for example parties who can audit IT risk management governance standards according to existing best practices including security standards regulated in SNAP. This is also in accordance with the provisions of Certification Fulfillment and/or Information System Security and Reliability Standards in SNAP. Examples of current International Best Practice are related to ISO 27001 and ISO 27002.³⁴

The use of independent third parties in conducting audits is also to fulfill the provisions of SNAP related to periodic audits by Service Providers and Service Users related to SNAP implementation. It is expected that the use of Standard Best Practice in IT Security both in the Open Banking Platform and in Banks and Fintech, can improve customer data security, which in turn can have an impact on public trust and create growth in the Digital Finance Industry.

³³ Article 10 of *Regulation of Bank Indonesia Number 23/PBI/2021 on National Payment System Standard*.

³⁴ ISO 27001 is an international standard that governs Information Security Management Systems (ISMS). The standard was released by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 provides a framework and guidelines for managing information security risks in an organization. ISO 27002 is an information security reference designed to assist companies in selecting, implementing, and maintaining an Information Security Management System (ISMS). This standard is used as a complementary standard to the ISO 27000 series, especially to the main ISO 27001 series. ISO 27002 is used as a more specific guide than the ISO 27001 framework for selecting appropriate security controls in implementing an effective ISMS.

4. CONCLUSION

The findings of this research indicate that both the Central Bank of Indonesia and the Indonesian Financial Services Authority (OJK) use various policy combination to regulate and oversee digital financial activities, including data sharing in banking collaboration with third parties including fintech such as implementing principle based regulation, implementing regulatory sandbox and piloting mechanism and verification of National Standard Implementation and optimizing the role SROs to detailing regulation in form national standards. It is necessary to strengthen the institutional structure especially related to Standard Governing Body in the governance aspect related to IT Risk, strengthening and synchronizing regulation related to Data Portability, Data Subject Rights, and Customer Consent.

REFERENCES

- Ali, Zainuddin. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2010.
- Asosiasi Sistem Pembayaran Indonesia. “Kick-Off Meeting Pembentukan WG Nasional Open API.” *ASPI*, June 16, 2020. <https://www.aspi-indonesia.or.id/kick-off-meeting-pembentukan-wg-nasional-openapi/>.
- Bank Indonesia. “Mengenal Financial Technology, Departement Komunikasi.” *Bank Indonesia*, December 1, 2018. <https://www.bi.go.id/id/edukasi/Pages/mengenal-Financial-Teknologi.aspx>.
- Bank Indonesia. *Blueprint Sistem Pembayaran (BSPI) 2025*. Jakarta: Bank Indonesia, 2019.
- European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European Data Protection Law*. Austria: European Union Agency for Fundamental Rights, 2018.
- Gazali, Djoni S., and Rachmadi Usman. *Hukum Perbankan*. Jakarta: Sinar Grafika, 2016.
- Hutauruk, Dina Mirayanti. “Ini Risiko yang Dihadapi dalam Kolaborasi Antara Bank dengan Fintech.” *Kontan.co.id*, June 10, 2021. <https://keuangan.kontan.co.id/news/ini-risiko-yang-dihadapi-dalam-kolaborasi-antara-bankdenganfintech>.
- Infosys. “Banking as a Platform: A New Age Transformation.” <https://www.infosys.com/iki/perspectives/new-age-transformation.html>.
- Jenik, Ivo, and Kate Lauer. *Regulatory Sandboxes and Financial Inclusion*. Washington D.C.: CGAP, 2017.
- Kemenkominfo Balitbang SDM. *Perkembangan Ekonomi Digital di Indonesia*. Jakarta: Puslitbang Aptika dan IKP, 2019.
- Khoirunnisaa, Jihaan. “Ini Strategi Pemerintah Kembangkan Ekonomi Keuangan Digital.” *Detik*, April 5, 2021. <https://finance.detik.com/berita-ekonomi-bisnis/d-5520894/ini-strategi-pemerintah-kembangkanekonomi-keuangan-digital>.
- King, Brett. *Bank 4.0: Banking Anywhere, Never at a Bank*. Singapore: Marshall Cavendish Business, 2018.
- Regulation of Bank Indonesia Number 03/2023 on Bank Indonesia’s Consumer Protection.*
- Regulation of Bank Indonesia Number 23/PBI/2021 on National Payment System Standard.*

- Regulation of Financial Services Authority Number 13/POJK.02/2018 on Digital Finance Innovation in the Financial Services Sector.*
- Regulation of Financial Services Authority Number 22 of 2023 on Consumer and Community Protection in the Financial Services Sector.*
- Regulation of the Members of the Board of Governors of Bank Indonesia Number 23/15/PADG/2021 on Implementation of the National Standard for Open Application Programming Interface for Payments.*
- Republic of Indonesia Law Number 11 of 2008 on Electronic Information and Transaction.*
- Republic of Indonesia Law Number 19 of 2016 on Amendment of Republic of Indonesia Law Number 11 of 2008 on Electronic Information and Transaction.*
- Republic of Indonesia Law Number 27 of 2022 on Personal Data Protection.*
- Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Depok: Rajawali Pers, 2019.
- Syafina, Dea Chadiza. “Mengenal Regulatory Sandbox, Rahim dari Kelahiran Para Fintech.” *Tirto.id*, April 26, 2018. <https://tirto.id/mengenal-regulatory-sandbox-rahim-dari-kelahiran-para-fintech-cJpW>.
- Zetzche, Dirk A., Ross P. Buckley, Janos N. Barberis, and Douglas W. Arner. “Regulating a Revolution: From Regulatory Sandbox to Smart Regulation.” *Fordham Journal of Corporate & Financial Law* 23, no. 1 (2017): 31–103. <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1450&context=jcfl>.