Journal of Central Banking Law and Institutions, Vol. 1 No. 2, 2022, pp. 323 - 352
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
https://doi.org/10.21098/jcli.v1i2.19

LEGAL ISSUES OF PERSONAL DATA PROTECTION AND CONSUMER PROTECTION IN OPEN API PAYMENTS

Camila Amalia, Esha Gianne Poetry, Mochamad Kemal Kono, Dadang Arief K., Alex Kurniawan

Legal Department, Bank Indonesia, Indonesia
e-mail: camila@bi.go.id (correspondent author), esha_gp@bi.go.id, mochamad_kk@bi.go.id, dadang_arief@bi.go.id, alex_k@bi.go.id

Submitted: 29 March 2022 – Last Revised: 10 May 2022 – Accepted: 18 May 2022

Abstract

Digital financial innovation in Indonesia demands equal disclosure of data and information among banks and financial technology (fintech) companies through the Open Application Program Interface ("Open API"). The Bank of Indonesia has the authority to regulate the standardisation of Open API payments to create data disclosure integrity, as well as improve personal data protection and consumer protection in open banking. This paper examines several legal aspects that have emerged and assesses whether current provisions have addressed these nascent legal issues. This paper uses a normative juridical approach with a descriptive analysis specification, using laws and regulations as the primary sources. Based on the research, existing regulations cover the essential egal aspects of Open API payments. However, to strengthen consumer rights surrounding Open API payments, it is still necessary to amend the Indonesian Consumer Law that to become more favorable toward the interests of consumers. Also, the effectiveness of personal data protection in Open API payments requires coordination among relevant regulatory authorities.

Keywords: *Bank Indonesia, open API, consumer protection, personal data protection, payment system.*

I. INTRODUCTION

The Bank of Indonesia (BI) as the authority regulating payment systems in Indonesia is mandated to create a payment system that is fast, easy, cheap, safe, and reliable amidst the current massive digital innovation in the financial sector. On the one hand, BI is expected to be able to support innovation in payment system, while also mitigating risk. To deal with this, BI has launched the Indonesia Payment System Blueprint 2025 (BSPI 2025).[1] BSPI 2025 focuses

[1] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025 BI: Menavigasi Sistem Pembayaran Nasional di Era Digital* (Jakarta: Bank Indonesia, 2019), 24.

specifically on the pillars of open banking to enable banks to disclose their customer's financial data and information to third parties (fintech or other parties) or vice versa, so that there is a level playing field between commercial banks and fintech, reducing the risk of monopoly and widening inclusivity opportunities from obtaining wider granular data.[2]

Through the BSPI 2025 vision, BI encourages industries in the payment sector to cooperate in providing services to the public. The implementation of an Application Programming Interface (API) between banks and fintech endures compliance with standards set by BI to create integrity in data in the context of open banking.[3]

To optimise Open API payment implementation and to mitigate the above risks, Open API payment arrangements must include consumer protection and personal data protection. This concern has been triggered by many cases regarding leaks of consumer data that were experienced by Tokopedia.[4] In addition, there are also practices of buying and selling consumers' personal data, which has the potential to harm them. As happened in 2018, the practice of buying and selling bank customer data through the *temanmarketing.com* site,[5] set off an alarm, underscoring the urgency of strengthening the personal data protection framework.[6]

In this regard, BI has issued a set of regulations in the payment system sector, starting with PBI No. 22/23/PBI/2020 concerning Payment Systems (PBI SP) as an umbrella law that regulates the implementation of payment systems based on an activity- and risk-based approach. This was followed by PBI No. 23/6/PBI/2021 concerning Payment Service Providers (PBI PJP). Also, in August 2021, BI issued PBI No. 23/11/PBI/2021 concerning National Payment System Standards (PBI Standards), PADG 23/15/PADG/2021 concerning National Open Application Programming Interface Payments Standards (PADG SNAP), along with guidelines for SNAP and Developer Site governance (Technical and Security Standards, Data Standards, and Technical Specifications).

---

[2] *Ibid.*

[3] Bank Indonesia, *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran* (Jakarta: Bank Indonesia, 2020), 1.

[4] CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual," CNN Indonesia, accessed May 3, 2021, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

[5] Sherly Puspita, "Polisi Bongkar Jual Beli Data Nasabah Bank via Situs Web," Kompas.com, accessed November 20, 2021, https://megapolitan.kompas.com/read/2018/04/16/21312031/polisi-bongkar-praktik-jual-beli-data-nasabah-bank-via-situs-web?page=all.

[6] Bank Indonesia, *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran, 11.*

The question arises whether the current regulatory framework is sufficient to address the legal aspects of Open API Payments, particularly related to personal data protection and consumer protection? The legal aspects of this unique transactional tool include the importance of customer consent, procedures for accessing consumer data, handling cyber security risks, and resolving disputes. Several legal aspects that arise are analysed and assessed for whether they have been addressed in the current laws, included the existing BI provisions.

This paper describes various aspects of personal data and consumer protection in Indonesia, especially in relation to the implementation of Open API payments, which have never been fully discussed. Accordingly, research on the subject is important in Indonesia, especially related to cyber law and consumer protection. In addition, this paper can be considered by stakeholders in preparing the PDP law and strengthening consumer protection. Finally, this paper can be a reference for consumers to understand their rights regarding their personal data in making payment transactions.

Indonesia does not currently have a law that specifically regulates personal data protection. Provisions for privacy and use of personal data are still scattered about various provisions and are not regulated in specific provisions. This is where BI's role as the regulatory authority over payment systems compels the implementation of personal data protection and consumer protection, specifically applied to the Open API payments enterprises. Absent specific action by BI, this legal vacuum may lead to uncertainty in enforcing personal data protection and consumer protection in the payment systems arena. Therefore, it is incumbent on BI to issue a series of payment system provisions to fill the gaps in protection of consumer data in the payment sector by requiring Open API enterprise to apply the governance and standards set by BI, including the information security and privacy aspects. At the same time, it is important to strengthen the laws codifying the rights of consumers.

According to Zeller and Dahdal in their working paper entitled *Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection*. based on the application of open banking in Australia and around the world, the core areas of regulation in an open banking framework should include open API protocols and technical standard settings identification of the basic elements in data sharing, identification of requirements and parameters used by third parties to obtain data access, and consumer approval mechanisms.[7] The result of their study indicates that regardless of the regulatory area, open

[7] Bruno Zeller and Andrew Dahdal, "Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection," *Qatar University College of Law, Working Paper Series, Working Paper No. 2021/001*, 2021, 5, https://doi.org/http://dx.doi.org/10.2139/ssrn.3766076.

banking around the world basically revolves around the same core principles, but the arrangements can differ depending on the interests of stakeholders in a particular country's financial system.[8] It is relevant to this paper BI's need to regulate in detail the open API payment in Indonesia to drive the economic growth while still protecting consumers' rights. This initiative is a form of BI's progressive response to digital financial innovation as well as to mitigate the risks that arise, especially those related to data protection and consumer protection.

Leong in his working paper entitled *Open Banking: The Changing Nature of Regulating Banking Data - A Case Study of Australia and Singapore*, provides a comparison of the framework for regulating customer data in open banking in Singapore and Australia. The role of the relevant authorities is becoming more important in regulating and supervising the market more so than the data.[9] Based on the research, data ownership regulation becomes important in implementing open banking in Australia and Singapore. With the recognition of market conduct, market participants in open banking will ensure the integrity and governance of personal data. The conclusion is relevant to this paper that the role of BI is very important in regulating the payments market, as well as sharing and ownership of data for API providers and API users. Cooperation among relevant authorities is also the key to effective enforcement of laws on personal data protection and consumer protection.

This paper employs a normative juridical research approach with analytical descriptive specifications, through library research of primary materials (laws and regulations in Indonesia (including BI provisions) and in several countries (e.g., EU General Data Protection, Payment System Directive), secondary materials (books, legal journals, consultative papers, and reports); and tertiary material (online news articles). In this paper, a literature review includes several countries' laws and regulations relevant to the problems studied, including the EU, Australia, and Singapore. The regulatory framework used by several countries are analysed to ascertain various aspects of personal data protection and consumer protection in Open API payments. Furthermore, the analysis covers how those legal aspects have been accommodated in the current laws, including BI regulations.

The scope of this paper includes: First, the introduction, which contains an explanation of the existing situations of digital transformation in the payments sector held by banks and fintech, the risks that have and can arise, as well as BI's response as a regulator to address massive digital innovation while

[8] *Ibid.,* 23.

[9] Emma Leong, "Open Banking: The Changing Nature of Regulating Banking Data – A Case Study of Australia and Singapore," *Banking & Finance Law Review* 35, no. 3 (2020): 443–69, 469.

still upholding consumer interests; Second, a brief description of Open API payments and parties involved, as well as the importance of supervision in the implementation of Open API payments; Third, mapping existing regulations in Indonesia related to aspects of personal data protection and consumer protection in Open API payments; **Fourth**, an analysis of the legal aspects of personal data protection and consumer protection in the current regulations that support the effectiveness of Open API payments proliferation. In this section, these various legal aspects are examined to determine whether the current provisions address this issue; and Fifth, conclusions, articulating that BI provisions in Open API payments are sufficiently managed facing such legal issues in Open API payments. However, it is further argued that it is necessary to amend consumer protection law to strengthen consumer protection in the financial sector.

II. OPEN API PAYMENTS AND THE REGULATORY FRAMWORK FOR OPEN API PAYMENTS IN INDONESIA

II.A. Open API at a Glance

The "BI Consultative Paper: Open API Standard and Interlink Banks with Fintech" defines an API as a set of protocols and instructions that enable interconnection between applications and easy access and exchange of data/information.[10] An API enables communication among software applications where one application requests and/or passes data to another application or takes advantage of each involved application's features. An API makes it easy for application developers to develop their applications without worrying about adding application features. Therefore, an API must be open source, referred to as Open API. Open API is the open use of API technology, providing access to API users who are partners in Open API cooperation with a system owned by an API provider to access and/or use consumer data, ostensibly with the consent of the consumer, for the purposes or services approved by consumers.[11] One example of this efficiency is the GoJek application. If the developer of this ridesharing/hailing application was not connected to the Google Maps Open API, it would be prohibitively expensive for the application to develop an independent proprietary location mapping application to map all locations in Indonesia.

[10] Bank Indonesia, *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran, 7*.

[11] *Ibid*., 7.

In general, an Open API ecosystem consists of three parties:[12]

1. API providers (data attribute providers) store consumer data and/or provide a service and provide API so that third parties can access and/or use consumer data and/or use their services through an API based on consumer approval;
2. API users (third party providers – TPP) access and/or use consumer data stored by API providers and/or use services from API providers based on consumer approval; and
3. Consumers.

In addition, based on the services provided, API can be grouped into four categories:[13]

1. Product and/or service information API;
2. Product and/or service registration API;
3. Account information API; and
4. Payment transaction API.

In this study, the analysis is carried out for the Open API for payment transactions (hereinafter in this study is called the Open API Payments), which is an Open API that allows API users to access payment services provided by API providers based on the consent of the consumer.

II.B. The Regulatory Model of Open API Payment in Indonesia

Globally, there are three regulatory models of Open API. First, is the regulator-driven model, where regulators impose the implementation of an Open API standard allowing banks to be more efficient and innovative, which can lead to lower costs for consumers. In this model, there are regulators who mandate Open API legal frameworks for market players. Jurisdictions that follow this model include the European Union, UK, Hong Kong, Australia, and Mexico.[14]

Second, is the market-driven model, where the market itself dictates that banks adapt to be more competitive in terms of digital financial innovation. Industries that create Open API standards and use them are market driven and standardised, as for example in New Zealand.[15] There is also the application

[12] *Ibid*., 7.

[13] *Ibid*., 8.

[14] Spire and Whitesight, "Open Banking: A Game Changer for The Financial Eco-System," 2022, 9, https://aqmen365.com/uploads/Open-Banking-Report---Part-1---V1.3-b32abcb8adfd7d589baff6322302758f.pdf.

[15] Westpac New Zealand, "Open for Business: A Guide to Open Banking in NZ," accessed August 7, 2021, 5, https://www.westpac.co.nz/assets/Business/institutional/documents/Thought-Leadership-Articles/Guide-to-Open-Banking-Westpac-NZ.pdf.

of Open API that is market driven, but not standardised (market driven non-standardised),[16] including the regulatory frameworks of the US and Canada.[17]

Third, is the government encouraged model, where there are no special arrangements regarding Open API set by regulators. Regulators merely encourage the formation of a balanced market so that the industry moves to create its own standards according to the needs of the community. Singapore and India take this approach.[18]

BI follows a regulator driven model, where an Open API standard is mandatory for Open API Payment participants and implemented in stages to anticipate the infrastructure readiness of Open API participants. BI has released the "PBI Standard" which regulates the obligations of Payment Service Providers (PJP) and Payment Infrastructure Providers (PIP), Support Providers and/or parties collaborating with PJP and/or PIP, to provide governance, risk management, information system security standards, interconnection and interoperability standards, and other technical standards. Furthermore, BI has also issued PADG SNAP, its regulation implementing the "PBI Standard." In addition, BI governs the National Open API Standard (SNAP) which includes technical and security standards, data standards, and SNAP technical specifications published on a developer site page, as well as governance guidelines in the implementation of Open API Payment connectivity. The developer site page (https://apidevportal.bi.go.id/snap/) publishes the arrangements made by BI in the Open API Payment, set out in the form of detailed guidelines and standards (regulated and standardised).[19] These guidelines and developer site pages can be reevaluated according to evolving needs. Also, BI may assign a Self-Regulatory Organization (SRO) to formulate and issue regulations in the payment systems sector, including technical and micro provisions, and to prepare and manage the standards set by BI.[20]

In this Open API Payment arrangement, the ultimate focus of the arrangement is PJPs, both API providers and API users. Other regulatory provisions are focused on non-PJP parties as users of Open API services, as well as developers of systems, applications, and/or devices in the Open API Payment ecosystem. The standardisation of Open API Payment systems is the

---

[16] Ismail Chaib, "Regulating Open Banking - How Regulators around the World are Shaping the Future of Financial Services" (Berlin, 2018),11, https://www.openbankproject.com/reports/regulatingopenbanking/.

[17] Spire and Whitesight, "Open Banking: A Game Changer for the Financial Eco-System", 9.

[18] *Ibid.*, 10.

[19] Bank Indonesia, "Standar Nasional Open API Pembayaran," accessed March 29, 2022, https://apidevportal.bi.go.id/snap/docs/standar-data-spesifikasi-teknis.

[20] Indonesia, Bank of Indonesia Regulation No. 22/23/PBI/2020 on Payment System, Art. 10.

control by the relevant authorities to ensure that Open API Payments mitigate the risk of fragmentation and security risks (personal data, user consent, and verification).[21] This set of regulations governed by BI is expected to support interoperability between API providers and API users and achieve integrity in the Open API Payment ecosystem.

III. MAPPING OF REGULATIONS ON PERSONAL DATA PROTECTION AND CONSUMER PROTECTION IN INDONESIA

III.A. Mapping of Personal Data Protection Regulations in Indonesia

Work by the Organization for Economic Co-operation and Development (OECD) between 1998 and 2007 elevated the importance of information security and privacy to the continued growth of the information society.[22] Hence, there are two areas of concern in personal data protection for Open API Payments: 1) policies for information security and privacy. Privacy policies include the principles or procedures of the provider in processing personal data; and 2) information security policies including the obligation to mitigate and resolve the risk associated with information systems, among others from various means of unauthorised access, data theft, and other risks. Essentially, regulations in Indonesia have covered those two areas. The constitution of the Republic of Indonesia and Banking Laws address privacy concern. Various agencies regulate the substance of information security and privacy concerns.

The basis for regulations related to data protection in Indonesia can be found in Article 28 letter G of the 1945 Constitution of the Republic of Indonesia, which states "...that everyone has the right to protect themselves, their families, their respect, dignity, and property under their control; and security and protection from the threat of fear to do, or not to do, something that is a human right." In addition, Law No. 7 of 1992 concerning Banking as amended by Law No. 10 of 1998 (Banking Law), regulates, among other things, the confidentiality of personal data regarding depositors and their deposits.

Law No.11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016 (The EIT Law) regulates the protection of personal data is. Article 26 regulates a person's personal data, the use of which must be carried out with the consent of the person concerned. Violation of this obligation is considered a breach of a civil rather than criminal violation, governed by the contractual relationships among the parties.

---

[21] Bank Indonesia, *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran,* 3.

[22] Organisation for Economic Co-Operation and Development, "OECD Policies for Information Security & Privacy," accessed January 10, 2022, https://www.oecd.org/sti/ieconomy/49338232.pdf.

Furthermore, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (GR 71/2019) implementing the EIT Law also regulates the protection of personal data in electronic systems.[23] GR 71/2019 emphasise that personal data processing must comply with the principle of providing data protection to data owners, including: 1) that personal data collection is carried out in a limited and specific manner with the consent of the data owner (consent); 2) that data processing shall be in accordance with its purpose (purpose limitation); 3) the rights of the data owner are guaranteed (vital interest); 4) it is carried out accurately, completely, not misleadingly, up-to-date and taking into account the purpose of processing personal data (data minimisation); 5) data processing is undertaken by protecting the security of personal data from loss, misuse, unauthorised access, and alteration/destruction (security concern); 6) the provider shall notify the purpose of data collection (notification); and 7) a mechanism to destroy and/or delete the data unless it is still in the retention period (data erasure). These principles are adopted from the EU-General Data Protection Regulation (GDPR), which is also the reference for personal data protection settings by many countries around the world.

To further regulate personal data protection in electronic systems, the Ministry of Communication and Informatics (Ministry of CIT) has issued the Regulation of Minister of Communication and Information Technology No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (The MCIT 20/2016). This regulation expressly prescribes that the acquisition and collection of personal data must be conditioned on approval from a data owner or based on statutory provisions.[24] This law also requires electronic systems operators to meet certain requirements to accommodate the acquisition and collection of personal data, including having interoperability and compatibility capabilities and legal compliance software. Also, MCIT 20/2016 regulates dispute resolution in the context of protecting personal data owners, namely by the Minister of CIT who coordinates with Sector Supervisory and Regulatory Agencies to follow up complaints from personal data owners.[25]

MCIT 20/2016 controls in detail how service providers in electronic systems must develop the infrastructure and procedures to mitigate cyber risks in accordance with the government's requirements. The IET Law and GR 71/2019 act as a reference for BI in regulating personal data protection in

[23] Indonesia, Government Regulation No. 71 of 2019 on The Implementation of Electronic Systems and Transactions, Art. 26 (1), Art. 39 (3), and Art. 40 (1.d).

[24] Indonesia, Minister of Communication, and Informatics Regulation No. 20 of 2016 on Protection of Personal Data in Electronic System, Art. 9 (1).

[25] Minister of Communication and Informatics Regulation No. 20 of 2016, Art. 29 (4).

the payment systems business. PBI SP regulates the management of data and other information related to the payment systems. In processing data and other information related to the payment Systems, PJP, and parties collaborating with PJP and requires, among other things, application of the principles of personal data protection including compliance with aspects of consumer approval for the use of personal data.[26] Furthermore, under PBI PJP, PJP have the obligation to implement a data and/or information processing mechanism related to the payment system which includes access and processing procedures, data standardisation, technical standardisation, security standardisation, and governance standardisation. This obligation also applies to third parties who cooperate with PJP if data processing is carried out through a third party's infrastructure. Further arrangements regarding the protection of consumers' data are contained in the Open API Payment Standard Guidelines (SNAP). This Guideline dictates that API providers and API users have the mechanism to protect data, mechanisms for approval, revocation, and deletion or destruction of data, as well as the mechanism and/or procedures for handling data leaks. SNAP has bridged the regulatory gap for personal data protection in the payment sector that is not specifically regulated in GR 71/2019 and MCIT 20/2016. The EIT Law and its implementing regulations as well as BI provisions require Open API parties to apply the governance and standards as set by BI, including the information security and privacy concerns.

III.B. Mapping Consumer Protection Regulations in Indonesia

Law No. 8 of 1999 concerning Consumer Protection (the Consumer Law) regulates among other things the rights and obligations of consumers and businesses, prohibited actions by businesses, responsibilities of businesses, and dispute resolution. The Consumer Law creates the National Consumer Protection Agency,[27] which provides advice and considerations to the government to develop consumer protection in Indonesia.[28] In addition, this Law regulates consumer dispute resolution, which can be pursued through formal court proceedings or alternative forms of dispute resolution through the Consumer Dispute Settlement Agency.[29]

The Consumer Law does not, however, prohibit the inclusion of standard clauses in the agreements between service providers and consumers, except those conditions enumerated in Article 18. This law sets out a better regulatory framework for consumer protection in terms of protection from abuse. According to Article 18 of the Consumer Law, businesses are prohibited from

[26] Bank of Indonesia Regulation No. 22/23/PBI/2020, Art. 107 (1.a).
[27] Indonesia, Law No. 8 of 1999 on Consumer Protection, Art. 31.
[28] *Ibid.,* Art. 33.
[29] *Ibid.,* Art. 49(1).

contracts of adhesion, taking advantage of their superior bargaining power to weaken consumer protections. This Law is intended to prevent abuse of circumstances by businesses who have a stronger position, which in the end harms consumers.[30]

However, the current Consumer Law needs to be amended to explicitly protect the rights of consumers relating to the confidentiality and security of personal data.[31] Furthermore, this Law may lead businesses to limit their liability if they can prove that they have not done anything wrong or if there is negligence on the part of the consumer.[32] This is the reason why there needs to be a significant regulatory reform of the Consumer Law, where businesses face strict liability for violating protections on data confidentiality and security rather than relying on the "fault" element on the consumer side.

Concerning the operation of payment systems, BI issued PBI No. 22/20/PBI/2020 concerning BI Consumer Protection (PBI CP). Consumer protection regulated under the PBI CP includes protection for consumers who utilise the products and/or services from providers that are regulated and supervised by BI. PBI CP mandates the providers' obligation to provide protection for consumer data and/or information and prohibits the provider from providing consumer data and/or information to other parties, unless there is written consent from the consumer, and/or instructed by the provisions of the legislation.[33]

Based on the regulatory map, Indonesia does not have a Personal Data Protection Law (PDP Law). Provisions regarding personal data protection and consumer protection are instead scattered across several laws and regulations including the IET Law and the Consumer Law as well as their implementing regulations, including those promulgated by BI. However, the absence of such a PDP Law will likely not disrupt the implementation of the Open API Payment standards set by BI. If BI regulations provide clear rules regarding the obligations and relationships of the parties in implementing Open API Payments in contracts, and BI and other relevant authorities conduct effective oversight of the industry involved in Open API Payments. The vision is creation of market integrity in payment systems that encourages more consumer confidence. Also, the success of the Open API Payment system requires collaboration among supervisory agencies in the financial sector and cyber industry to create legal certainty in the division of authority of the

---

[30] Ahmadi Miru and Sutarman Yodo, *Hukum Perlindungan Konsumen* (Jakarta: Rajawali Pers, 2017), 126-127.

[31] Law No. 8 of 1999 on Consumer Protection, Art. 4.

[32] *Ibid.,* Art. 27, point d.

[33] Indonesia, Bank of Indonesia Regulation No. 22/20/PBI/2020 on Bank Indonesia's Consumer Protection, Art. 33(1-2).

supervisory agencies in protecting personal data. The key to success is finding consensus among the authorities to ensure effective and efficient supervision with respect to areas where the respective tasks of all stakeholders converge.

As an example of a successful supervisory regime, *De Nederlandsche Bank* (DNB), the Central Bank of the Netherlands, has the authority to supervise Open API Payment implementation. However, when Open API Payment implementation relates to personal data protection, an institution outside DNB, namely *Autoriteit Persoonsgegevens* (AP) has the relevant authority. Both DNB and AP agreed to conduct supervision of PSD2 by signing a cooperation protocol on 21 February 2019.[34] A similar cooperation is applied in Australia, where the Reserve Bank of Australia (RBA) and Australian Competition Consumer Commission (ACCC) have an MoU as the basis for policy coordination for competition and access in payment systems, information sharing, coordination meeting and liaising among stakeholders.[35]

IV. THE LEGAL ASPECTS OF PERSONAL DATA PROTECTION AND CONSUMER PROTECTION IN OPEN API PAYMENTS

The effectiveness of Open API Payment regulations is determined, among other things, by the comprehensiveness of regulatory coverage of various legal and technical aspects of Open API Payment. Below, this paper describes various legal implications that have emerged related to data protection and consumer protection, as well as how current regulations have addressed these various legal issues.

IV.A. Scope of Consumers' Personal Data

One of the legal aspects that is important to discuss preliminarily is the scope of consumers' personal data in the Open API Payment, whether it only covers individual data or also includes data owned by companies or other legal entities. GR 71/2019 defines personal data as data about a person either identified and/or can be identified separately or in combination with other information either directly or indirectly through electronic and/or non-electronic System.[36] It is not clear whether the scope of personal data includes legal entities.

---

[34] Eric Goosen, "The Influence of Law & Regulations on The Process of Digital Transformation at Banks in The Netherlands" (Leiden University, 2020), 25.

[35] Australian Competition & Consumer Commission and Reserve Bank of Australia, "MoU the ACCC and RBA" (2018), accessed May 8, 2022, https://www.rba.gov.au/payments-and-infrastructure/payments-system-regulation/mou/accc-and-the-rba/.

[36] Government Regulation No. 71 of 2019 on The Implementation of Electronic Systems and Transactions, Art. 1 point 29.

Meanwhile, PBI CP and SNAP use the term "consumer data and/or information," instead of "personal data." PBI CP and SNAP establish a definition of consumer that includes individuals or entities, whether in the form of legal entities or not legal entities that utilise the products and/or services of service providers.[37] This definition aligns with the Circular Letter of the Financial Service Authority (the OJK) No.14/SEOJK.07/2014 concerning Confidentiality of Consumers' Personal Data and/or Information stipulates that consumer personal data and/or information is data and/or information which includes individuals and corporations.

However, the GDPR does not govern data owned by companies or any other legal entities. However, legal entities' data related to the identity of a person within the company, such as the employee telephone numbers, constitutes personal data.[38] This GDPR definition is adopted in the MCIT 20/2016, which defines personal data as certain personal data that is stored, maintained, and kept true and confidential.[39] The latest draft of PDP Bill also defines personal data owner as an individual.[40]

Based on the explanation above, there are differing definitions of the term "consumer personal data" in the laws and regulations in Indonesia. To reconcile the various definitions of consumer personal data in the laws and regulations, BI has the authority to regulate the scope of consumer personal data in the payments sector, as governed by OJK in SE No. 14/SEOJK.07/2014. This has been covered in the PBI CP that the subject of personal data in BI provisions includes consumer data of both individuals and legal entities.

IV.B. Types of Personal Data in Open API Payments

The success of Open API depends on the extent to which consumers are confident their data is protected during payment processing of banks, fintech, or third parties. Thus, an Open API regime must clearly regulate the type of consumer personal data in Open API, including the requirement to obtain consumers' approval of any data disclosure. It is important to provide an understanding to the industry regarding which types of data require consumers' consent.

---

[37] Bank of Indonesia Regulation No. 22/20/PBI/2020 on Bank Indonesia's Consumer Protection, Art. 1 point 1.

[38] European Commission, "Do the Data Protection Rules Apply to Data about a Company?," accessed June 14, 2021, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en.

[39] Minister of Communication and Informatics, Protection of Personal Data in Electronic System, Article 1 point 1.

[40] The House of Representative, "The Draft of Personal Data Protection Bill" (January 2020), https://www.hukumonline.com/pusatdata/detail/lt561f74edf3260/ruu-pelindungan-data-pribadi-tahun-2020/document, Article 1 point 6.

In fact, however, the amount of data and information collected without consumers' awareness (without explicit consent) continues to increase due to technological developments through data analytics by providers. This is because data analytics aggregates seemingly non-personal data with identifiable information or identifiable individuals, thereby blurring the line between non-personal and personal data.[41]

Under SNAP, the scope of data in the Open API payment has been set, including:

1. transaction data, including data set forth in the SNAP technical standards and specifications; and
2. other data, including but not limited to profile data of parties related to an Open API Payment and underlying payment data in an Open API Payment.

Although the SNAP framework does not specifically regulate the scope of consumer personal data, SNAP has provided a general definition of consumer data, namely profile data and other data attached to identified consumers and/or identifiable separately or in combination with other information either directly or indirectly through electronic and/or non-electronic means.[42]

The scope of data in Open API Payment and the definition of consumer-owned data in SNAP has clearly mandated that API providers and API users to implement personal data protection. Thus, API providers and API users as well as collaborating third parties must treat consumer-owned data as personal data which must be protected.

As a comparison, the Consumer Data Rights Rules 2020 (CDR) in Australia does not govern types of personal data regulated in open banking, but rather identifies four categories of data in open banking based on the Farrell Report, which are:

1. Data provided by consumers, such as information provided directly by customers to their banks, for example, customer addresses/contact details provided when opening accounts or applying for loans. This includes information that has been provided for payment purposes.
2. Transaction data is the data generated from transactions of consumer accounts, including records of deposits, withdrawals, transfers, and other transactions carried out by customers (such as direct transactions with

[41] Organisation for Economic Co-Operation and Development, "Personal Data Use in Financial Services and The Role Of Financial Education: A Consumer-Centric Analysis," OECD, 2020, 9, https://www.oecd.org/finance/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf.

[42] Indonesian Payment System Association (ASPI), *SNAP - Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)*, Ver. 1.0 (Jakarta: Bank Indonesia, 2021), 3, https://www.bi.go.id/id/layanan/Standar/SNAP/Documents/SNAP_Pedoman_Tata_Kelola.pdf.

merchants), account balances, interest earned or charged, and other fees charged to customers.

3. Value-added consumer data is the data generated by a data holder's efforts to dig deeper into consumer information, for example, income/asset checking data, customer verification data, credit report data, credit scores, individual customer data collected from customer accounts and have been standardised, cleaned, or reformatted to be more efficient.
4. Collected data that is created when a bank uses different customer data to generate de-identifying, collective, or average data from groups of customers, for example, data on average account balances grouped by postal code or data on the average size of small business overdrafts grouped by industry.

Meanwhile, the provisions of the EU payments system, as set forth in the Payment System Directive 2 (PSD2), do not set rigid limits on the types of personal data in the payment sector. PSD2 requires that data can be shared with consumer consent when consumers use payment services which including payment initiation or account information services.[43]

According to the OECD, the sharing of personal data in the financial sector from a consumer perspective, can be classified into:[44]

Table 1.
The Grouping of Personal Data in the Financial Sector from a Consumer Perspective (OECD)

Personal Data	Data collection channels
consumer is aware	1. Data submitted during the KYC process (name, ID, telephone number, NPWP (Taxpayer Identification Number), and monthly salary data). 2. Data provided to support product purchases (such as payment transaction data). 3. Data provided for specific services (such as data aggregation tools: information on sources of funds). 4. Data collected when consumers use payment services (sources of funds, balance information, account balance fluxuating, and transfers.).
consumer is unaware	1. Data collected during consumer interactions. 2. Data available from social media, including consumer behavior patterns. 3. Data shared by the provider from third parties

[43] Data that is outside the payment initiation service and account information, such as data of credit, savings, investments, do not fall into the scope of data in payment system according to PSD 2; they are subject to data governed by GDPR. it is called "interregulation" where there is an umbrella law which underlies the general personal data protection, and at the same time there is a specific regulation issued by sector agency that shall not contradict each other. Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, https://mafr.fr/media/assets/ouvrages/edpb_guidelines_202006_interplaypsd2andgdpr.pdf

[44] Organisation for Economic Co-Operation and Development, "Personal Data Use in Financial Services and The Role of Financial Education: A Consumer-Centric Analysis,"9.

According to the simulated transaction above, the processing of personal data shared without consumer awareness should also be a concern for consumer. For example, the combination of aggregate transaction data with various consumer behaviour patterns on social media that results in a special category of personal data is categorised as personal data in payment systems because the data can be combined to identify an individual.

The type of data in Open API Payments is similar to the Australian model which does not specifically regulate the type of private data. Identifying personal data in the payment systems sector is not easy because the same personal data can be used for various purposes across several sectors (outside of payment systems). For this reason, BI simply regulates the definition of consumer data in general and coverage data in Open API Payments. The regulation is sufficient to guide the industry to identify consumer's personal data so that its processing is carried out to ensure the consent of the consumer. Thus, consumer data that is further processed so that it has added value through automatic processing should also be categorised as personal data because it meets the elements of the personal data definition set forth in SNAP. For example, consumer data that is combined with consumer behavior and then analysed using artificial intelligence to produce new information that is useful for product development for API providers and API users must be processed only with consumers' approval.

IV.C. Access to Consumers' Personal Data

PBI CP mandates that service providers that cooperate with other parties to manage consumer data and/or information, must ensure that other parties protect the confidentiality and security of the Consumer data and/or information. This obligation is also reinforced in Article 257 paragraph (1) of PBI PJP that in processing data and/information related to payment systems, PJP and/or cooperating parties are required to apply the principles of personal data protection including fulfilling the aspects of user approval for any use of their personal data. In that API providers and API users are both PJP, they will comply with BI's provisions because PJP is an entity that is directly under BI regulation and supervision. However, if the API user is a non-PJP, there must be measures to ensure that the Open API requirements are met by non-PJP parties. For this reason, the scope of the subject of the Open API Payments regulation must also cover non-PJP parties to create a level playing field between PJP and non-PJP parties who enter into cooperation in the Open API Payments business as an effort to achieve the integrity of the Open API Payments ecosystem.

In the European Union, the regulation of personal data protection in payment systems were promulgated through PSD 2, which stipulates that

consumers who intend to use the new services cannot be prevented by their banks. In such a case, a bank must provide access to a consumer's account information to other parties if the consumer instructs to do so. This regulation gives complete power to banking consumers in the European Union to provide access to data transfers from banks to services provided by other parties. This regulation is mandated by Article 20 paragraph (1) of the GDPR regarding one of the rights of data subjects, namely the right to data portability.

The problem is a potential situation where PJPs (bank/fintech company) and non-PJP third parties do not have a contractual relationship. Although the provision of personal data is carried out according to consumer consent, this should not be enough for a PJP to transfer personal data to other parties because a PJP must believe that the non-PJP party also applies personal data protection to its consumers. In addition to consumer consent, it is necessary to: 1) perform due diligence to ensure the third party is eligible to process personal data; and 2) ensure the enforceability underlying contract between PJP and the non-PJP cooperating parties in the Open API payment.

For this reason, Article 14 of PADG SNAP stipulates the obligation of PJPs to ensure that non-PJP API users apply the Open API Payment standards and comply with all requirements set by BI. PJPs are also required to make contracts with non-PJPs who cooperate according to contract standards set by BI, including ensuring that non-PJP API users have a mechanism for ensuring consumer approval. Thus, data portability rights need to be balanced with the prudential principle by PJPs before access to personal data is given to non-PJP API users as well as periodic audits during the cooperation period.

IV.D. Due Diligence

In some jurisdictions such as Australia and the European Union, non-PJP parties as API users must be accredited entities. These two jurisdictions have the authority to accredit third parties so that when there is a request for data disclosure by a third party, PJPs must immediately provide the consumer data based on the third party's accreditation. This accreditation concept makes the industry more efficient, where third party due diligence standards are set by the authorities so that the authorities will also later carry out due diligence and have the right to audit non-PJP parties as API users who cooperate with PJP as API providers.

Meanwhile in Hong Kong, PJPs are required to conduct due diligence before providing access to personal data to non-PJP parties.[45] This concept

[45] Consultative Group to Assist The Poor and Hogan Lovells, *CGAP Guidance Note: Key Considerations When Developing Legal Terms and Conditions for Financial Services APIs* (Washington DC: CGAP, 2020), 12-3, https://www.findevgateway.org/sites/default/files/publications/files/cgap-guidance-note-key-considerations-when-developing-legal-terms-and-conditions-for-financial-services-apis-january-2020.pdf.

is based on the logic that PJPs are the parties who must be liable if non-PJP cooperating parties violate the use of personal data because PJPs do not apply the cautionary principle. Failure of compliance by non-PJP parties as API users has the potential to affect PJPs' reputations as API providers, and in turn will harm consumers and is subject to sanction imposed by BI. Also, PJP is an institution that obtains a license from BI, while non-PJP parties are not entities that are directly under the control of BI as supervisory authority over payment systems. Control of performance by non-PJP API users is mandated through obligations contractually imposed on PJPs so that authorities can force non-PJP API users to comply with Open API provisions.

In Indonesia, due diligence requirements for both PJP providers and API Users, as well as non-PJP API users is carried out by the SRO. SRO is an Indonesian legal entity that represents industry and is designated by BI to support the implementation of payment systems including Open API Payments. However, in terms of an API user as a non-PJP party, the PJP has to ensure that the non-PJPs implement all the procedures and mechanisms in SNAP. Article 16 of PADG SNAP stipulates that PJPs as API Providers are required to ensure non-PJP API users perform testing on the SNAP-based Open API Payment test applications on the SNAP Developer Site, perform functionality testing, have procedures and documents for development of changes, and system maintenance, submit verification requests to SRO, and comply with relevant laws and regulations. Furthermore, the implementation of verification and providing recommendations related to the implementation of SNAP is carried out by the SRO with reference to the policy settings set by BI.

From BI's perspective as a regulator, supervision of non-PJP parties as API users is within its purview. In this regard, Article 29 of SNAP stipulates that BI may request transaction data and other data related to Open API to non-PJP API users. If BI finds a violation by non-PJP API user, BI can coordinate with the relevant authorities for the imposition of sanctions.

IV.E. Necessity of Contract between API Provider and API User

Since API providers and API users have passed verification through due diligence, standardised contractual cooperation is required, especially to protect the rights and obligations of the parties to the Open API payment and encourage the parties' compliance, including the provisions on personal data protection and consumer protection.

Setting and providing access to personal data by API providers and API users is a critical issue. Besides being a legal obligation for API providers based on BI's provisions, API providers and API users also must have contracts

to regulate, among other things, the mechanism for accessing personal data, level of disclosure of personal data, and allocation of liability among the parties, costs, and indemnification, with the minimum clause regulated by BI's provisions.

In comparison to other jurisdictions, in the EU, provisions for access to personal data of payment system providers are regulated as a legal obligation based on PSD2, meaning that without a contract between the API providers and API users, providing access to personal data is mandatory for the party managing personal data. PSD2 requires that PJPs that cooperates with other parties must meet certain requirements, including the extent to which the other party has access to consumer data, and the obligations of the parties. Even though those other parties are not under the supervision of the EU payment systems authority, they are still subject to the GDPR, where the penalties for breaches of personal data are very high.

However, in Indonesia, without contractual obligations between PJPs and other non-PJP parties, PJPs will find it difficult to allocate liability for breaches of personal data protections according to the needs of the parties. Therefore, contracts between API providers and API users, including non-PJP API users or other parties who cooperate with PJP, are necessary. Such contracts are a coercive tool for non-PJP API users and parties who cooperate with PJPs to fulfill the principles of personal data protection and consumer protection. Moreover, the implementation of risk management of parties outside the PJP is not as strong as a bank or PJP, both of whom are familiar with detailed policies, procedures, internal controls, and external controls.

Based on Article 89, point b, of the PBI SP, third parties are subject to supervision of the PBI so that normatively they must comply with the principles of personal data protection and consumer protection stipulated in this PBI. However, implementation is not that facile because BI cannot impose sanctions if parties outside the PJP commit violations; in contrast to PJPs which are regulated entities. For this reason, it is necessary to enter into contracts so that non-PJP API users' access to personal data is still controlled by the API provider.

Additionally, after a contract has been executed, PJPs still must evaluate the performance of non-PJP parties during the contract period. If there is any inconsistency by non-PJP parties against the requirements set by BI, the PJPs may suspend or terminate the contract. For this reason, contracts must also explicitly set forth provisions for terminating cooperation between PJP and non-PJP API users.

To protect the interests of consumers' personal data, in Chapter V of SNAP, a standard contract has been published which contains general principles

and standard clauses that must be included in the contract between the API provider and the API user, including between PJPs and parties collaborating with PJPs, as well as the rights and obligations of the parties to cooperate in Open API Payments. Also, Chapter V of SNAP includes the need to obtain consumer approval before a transaction is processed, prohibition of data disclosure except with the consent of consumers and service providers and/or PJP service users, deletion of consumer data at the request of consumers, by adhering to the applicable regulations, and establishing a consumer complaint mechanism.

IV.F. Data Portability Rights

Open API implementation can accelerate financial inclusion because individuals can request to transfer data from one provider to another to access credit sources. For example, data such as online shopping transactions can be used as supporting material for credit analysis to replace one's existing financial data, which so far have only been based on salary slips.

This right to data portability provides a guarantee to individuals as data owners for access the data from the electronic system operators and transfer it according to the consumers' instructions. If consumers intend to take advantage of their data portability rights involving providers' Intellectual Property Rights (IPR) and provider charge a fee (since there is a cost for investing technology to process consumer data). This fee must be reasonable, and therefore, BI has the authority to determine the pricing scheme that arises in the use of this Open API Payments, as regulated in Article 14 paragraph (2) of the PBI standards.

However, considering that the data portability rights are not regulated in current Consumer Law, BI through the PBI CP stipulates that a provider must grant consumers the right to access their personal data and/or information managed by the provider (Article 32). In addition, this right is further governed under SNAP,[46] where consumers can access data and/or information managed by their providers. Through PBI CP and SNAP, BI has affirmed the consumer right to data portability as also applied to international best practices (GDPR).

The regulation of data portability rights should be included in any amendment to the Consumer Law because it is a basic right of consumers. The regulation of portability rights needs to consider certain prerequisites, as applied in Singapore, among others, that requests for data portability comply with applicable regulations, and the party that manages the data must have a

[46] Indonesian Payment System Association (ASPI), *SNAP - Standar Nasional Open API Pembayaran (Pedoman Tata Kelola),* ver. 1.0, 5.

legal relationship with the person who request its personal data, and the data receiver must meet the requirements in managing personal data.

Usually, the regulation of data portability rights is accompanied by regulation of right to restrictions on processing and right to rectify. In Europe, those rights are regulated in GDPR. Based on Article 18 GDPR, the right to restriction of processing can be exercised when:

- The accuracy of the data in question is contested;
- The data owner does not want the data to be erased;
- The data is no longer needed for the original purposes but may not be deleted yet because of legal grounds; and/or
- The decision on your objection to processing is pending.[47]

Meanwhile in Indonesia, based on article 21 of the MCIT 20/2016, a personal data owner may restrict a data collector from displaying, announcing, delivering, disseminating and/or opening access to his/her data because these actions require prior consent from a data owner, unless otherwise provided by law, and after the accuracy and compatibility of the purpose of its acquisition and collection of the personal data.[48] Basically, Article 21 of the MCIT 20/2016 governs the right to restrict processing of data, but not in detail since it does not include the conditions specified in Article 18 GDPR.

In addition, Articles 16 and 19 of GDPR set forth the right to rectify when personal data is inaccurate.[49] A data owner has the right to rectify data without undue delay.[50] In Indonesia, the right to rectify is regulated in Article 26 of the MCIT 20/2016, where a personal data owner shall be entitled to have access to rectify or update his/her personal data without interfering with the management systems of personal data, unless otherwise regulated by laws and regulations.[51] Based on the above explanation, Indonesia's MCIT 20/2016 has codified the right to restrict data processing and the right to rectify.

IV.G. Consumer Consent

User consent becomes a critical point when API providers and API users perform personal data processing in Open API Payments. The principle of consumer approval is the foundation for the implementation of Open API to mitigate the risks of fraud and misuse of transactions, as well as to increase

---

[47] European Commission, "When Should I Exercise My Right to Restriction of Processing of My Personal Data?," n.d.

[48] Minister of Communication and Informatics, Protection of Personal Data in Electronic System, Article 21.

[49] Data Protection Commission, "The Right to Rectification," n.d.

[50] *Ibid.*

[51] Minister of Communication and Informatics, Protection of Personal Data in Electronic System, Article 21.

consumer confidence. This is based on the principle that: i) the consumer is the owner of their data stored by another party (data ownership); ii) the consumer is the only party that can give consent to share data with other parties; and iii) the consumer has the right to request that his/her personal data be deleted and not used by other parties ('right to be forgotten' or right to erasure).[52] For this reason, it is important to regulate how consent can be given and/or can be withdrawn by consumers.

The EIT Law states that the use of any information through electronic media concerning a person's personal data must be carried out only with the consent of the person concerned. The GR 71/2019, regulates in more detail that the processing of personal data must meet the provisions of a valid consent from the owner of the personal data for one or several specific purposes that have been submitted to the owner of the personal data.

In addition, the PBI CP states that a service provider is prohibited from furnishing consumer data and/or information to other parties, unless there is written approval by the owner or is required by law. This aspect of consumer approval is reaffirmed in PBI SP and PBI PJP that in processing data and/or information related to a payment system, PJPs and/or parties collaborating with PJPs are required to apply the principles of personal data protection including obtaining user approval for the use of their personal data.

The legal aspect of concern is whether the consumer's agreement to be regulated is a statement from the consumer or is contractual between the consumer and the API provider. This is because the two forms of agreement have different legal consequences. If it is only a written statement, it means that this agreement is only made by one party, namely by the consumer, in the form of a statement letter so that it can be withdrawn at any time. For example, Google services have a "revoke access" feature that can be chosen at any time when the consumer is about to withdraw consent.

However, if it is contractual obligation, then the assent is binding on both parties, namely the consumer and the API provider/API user. The nature of this contractual relationship is that the granting of consent cannot be withdrawn at any time, but by submission, then the API provider or API users are given time to stop processing personal data whose consent has been withdrawn by the consumer, or it can also be terminated after a set retention period, by notifying the consumer, whether they still want to continue to agree to the sharing of personal data by PJPs to third parties.

The MCIT 20/2016 regulates consumer consent, requiring a statement letter. This is reflected in the definition of consent of the owner of personal

[52] Working Group 1 BSPI 2025, *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran,* 21.

data in the form of a written statement both manually and/or electronically given by the personal data owner after receiving a complete explanation regarding the actions of acquiring, collecting, processing, analysing, storing, displaying, disclosure, transmission, or dissemination as well as confidentiality or non-confidentiality of personal data. Approval is given after the personal data owner confirms the validity, confidentiality status, and purpose of personal data management,[53] which is given by the consumer through a consent form.[54]

PBI CP stipulates that written approval can be in hard copy form and/or other electronic format supplied by the service provider. Written approval includes approval by telephone which is recorded and transcribed. PBI CP has covered any form of written approval that applied in the practice of transactions in payment system, which can be in the form of a transcript that must be administered by PJP or a third party.

The forms of consumer consent in PBI CP align with the provisions in the Open API Payment regime. Furthermore, the Open API payment sets more detailed provisions, among others: consumer approval is in the form of written consent electronically or non-electronically or verbally (recorded in a media) that shall be stated explicitly, specifically, informatively, and no hidden information.[55] Consumers have the right to revoke consent that has been given by verification and processing by API providers and API users. However, for Consumer transaction data that is inherent in the Consumer and becomes important data in supporting the activities of Service Providers and Service User PJPs as well as for authorities' purpose in the context of supervision, the management of transaction data, including the mechanism of revocation data, shall refer to the provisions of data retention and data sharing based on laws and regulations and BI provisions.[56]

Revocation of consumer consent in an Open API Payment transaction must be regulated because if consumers can withdraw their consent to the processing of consumer data at any time, there is a risk for API providers and API users. For example, providers could possibly be unable to follow up on outstanding transactions in the final settlement. Also, the authorities could be unable to obtain consumer data for the implementation of monitoring the payment system. To balance the interests of personal data protection and the needs of the industry as well as the authorities in managing personal data, the nature of consumer consent in the Open API payment regime is moving

[53] Minister of Communication and Informatics, Protection of Personal Data in Electronic System, Article 2 paragraph (4).

[54] *Ibid*., Article 6.

[55] Indonesian Payment System Association (ASPI), *SNAP - Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)*, ver. 1.0, 5.

[56] *Ibid*., 14.

toward contractual relationships to avoid the potential problems of withdrawal of consent at any time by consumers. However, there must be a verification process from API providers and API users, subject to the provisions of the data retention period, and does not apply concerning a request from the authority in the context of supervision. As long as each instance of processing of personal data for different purposes is preceded by consumer consent and consumers are given access to personal data controls including being able to withdraw consent in accordance with the contract mechanism with API providers and API users, the interests of consumers will be protected.

IV.H. Data Leak Management

In terms of consumer data leaks, API providers and API users must have an incident response plan in place in the event of an attack that includes, like the measures taken when a cyberattack incident occurs, procedures to mitigate cyber threats, and secure data and operating systems. All policies and chronology related to the handling of security incidents must be well documented because they will become the material for regulators and law enforcement officers in conducting surveillance.

In terms of PJP cooperation with non-PJP API users, PJPs must ensure that non-PJP users also implement data protection measures. This is because when PJPs provide access to information for non-PJP API users to consumer accounts, the data can be exposed if non-PJP parties do not take adequate cyber risk mitigation efforts, potentially endangering customers. To reduce this risk, PJPs and non-PJP users must have cyber risk handling procedures as outlined in a contract regarding the obligations of confidentiality and integrity of consumer security credentials, implementation of strong standards for communication between PJP and non-PJP, and technical measures to protect consumer data, including in the matter of data leaks.

However, if the consumer himself violates the terms and conditions of his account by disclosing his access credentials to other parties, the legal protections do not favor them. For this reason, BI requires PJPs to improve the literacy of consumers and/or the public regarding rights as data owners, the importance of data protection, benefits, costs, and risks of Open API Payments.[57]

In implementing Open API Payments, the most important thing to consider is how to make API providers and API users build adequate security standards and maintain strong information system resilience to mitigate cyber risks and if an attack occurs, companies can perform recovery, especially on data and consumer interests.

[57] *Ibid*., 4.

Under provisions of laws and regulations in other countries, data breaches must also be reported to the relevant authorities. For example, in the UK, data controllers must notify the Information Commissioners Office (the authority responsible for the protection of personal data) within 72 hours of becoming aware of a personal data breach that meets certain criteria. If the data controller is a regulated bank or company in the financial sector, they are also obliged to report to the regulator in the financial sector.

In Indonesia, GR 71/2019 stipulates the obligation for Electronic System Operators to apply security standards and report at the first opportunity to law enforcement officers or related Ministries/Agencies related to a system failure or disturbance resulting from the actions of other parties against the electronic system.[58] If there is a failure in the protection of personal data, it must notify the owner of the personal data.[59]

Currently, the absence of regulations at the statutory level regarding the agency appointed to handle personal data protection, whether carried out by sectoral authorities or special institutions, has resulted in uncertainty. The regulation of reporting on consumer data leakage in GR 71/2019 is also not clear when the providers must report to law enforcement officials; and to what extent they must report to the relevant authorities. This loophole is accommodated by the Open API payment provisions, that if there is a data protection failure, PJP shall report to BI in an incidental report. If this incident occurs to a non-PJP API user, a report to BI will be submitted through the API Provider PJPs. In addition, API providers and users must also notify in writing (electronic and/or non-electronic) no later than 3x24 hours after it is realised that there has been a breach of personal data to affected consumers, parties who cooperate in Open API Payment services, and/or the competent authorities. In such a case, an API Provider must report to all relevant authorities to meet the compliance aspects set by each authority.

In fact, reporting to all relevant authorities can incur significant costs for the providers and reporting will be inefficient. This is because in Indonesia there is no special agency to resolve any failures in personal data protection. In the future, a special agency is needed so that providers only coordinate with one agency. Furthermore, the agency can take further actions, including having coordination with other relevant authorities.

---

[58] Government of Republic Indonesia, The Implementation of Electronic Systems and Transactions, Article 24.

[59] Minister of Communication and Informatics, Protection of Personal Data in Electronic System, Article 28 point c.

IV.I. DISPUTE RESOLUTION

IV.I.1. Disputes between PJPs and Third Parties in Open API Payment

Under SNAP, putative parties may use the court system or alternative dispute resolution, based on the contractual forum selection.[60] SNAP requires standard contracts must use Indonesian language and can be translated into English or other languages. However, if there is a dispute or inconsistency I the interpretation of a contract clause, the Indonesian version shall prevail.[61] In addition, the dispute resolution process may harm the relationship between API providers and API users, so that cooperation is suspended or terminated. For this reason, SNAP regulates the fulfillment of obligations that must be completed by each party if there is a contract suspension or termination, in particular where the obligations related to consumers.[62]

In addition, PJPs and third parties must agree on clear allocation of liability and settlement arrangements to protect consumers in terms of damages. SNAP does not regulate the rights and obligations of the parties in detail when it comes to consumer losses. For example, the question of who should provide compensation to consumers is determined by the contract. However, SNAP provides general arrangements that API providers and API users are fully responsible independently or jointly to administer, follow up, and resolve the handling of consumer complaints.[63] This means that the responsibility for resolving consumer complaints must be allocated proportionally between API provider and API user depending on the terms and conditions by the parties.

The dispute resolution regime in Indonesia is based on negligence, where the blame can be placed on the consumer where there is contributory negligence. This regime is considered unfair because the API provider/ API user should be responsible for ensuring the security of the system, including ensuring that consumers are safe in transacting when using the platform, without having to see the element of consumer error which ultimately invalidates the API provider/API users' responsibility for losses suffered by consumers.[64]

---

[60] Indonesian Payment System Association (ASPI), *SNAP - Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)*, ver. 1.0, 35. As the illustration, the practice of the open banking dispute resolution in UK through *Dispute Management System* for API Provider and User that register based on voluntary so that they can communicate to resolve the disputes. DMS is a voluntary based mechanism where the participants comply with the best practice code, including how to handle cases at the first level, and how it may be brought to mediation, adjudication, or arbitrage.

[61] *Ibid*., 27.

[62] *Ibid*., 28.

[63] *Ibid*., 7.

[64] Camila Amalia, "Suptech: Penyiapan Ekosistem Digital untuk Mengawal Efektivitas Transformasi Digital di BI," *Buletin Hukum Kebanksentralan* 17, no. 2 (n.d.).

Based on Article 19 of the Consumer Law, businesses bear the responsibility to compensate consumer losses, but this does not apply if the business can prove otherwise, that the mistake is the consumer's fault. This regime places consumers at a disadvantage. This negligence regime is also embraced in the IET Law[65] and followed by PBI PJP.[66]

In the US, this concept works but it is starting to be questioned because it is considered unfair.[67] Meanwhile, in countries such as Australia, there is already a division of types of fraud liabilities that must be carried out by consumers and providers.[68]

BI can play a role in clarifying and strengthening the legal framework, by drafting bye laws to determine areas of fraud liabilities together with ASPI, Indonesia E-Commerce Association (idEA), and PJSP.[69] As applied in Australia, these guidelines minimise disputes if there are disputes over fraud liabilities. The point of compromise can be used to determine fraud liabilities, i.e., the party responsible is the party most able to reduce disputes or cybercrime,[70] which could be a provider of goods/services, a provider of electronic facilities, or a consumer.

IV.I.2. Consumer Disputes

PBI CP regulates the principles of effective complaint handling and settlement. SNAP also regulates the obligations of API providers and API users in handling consumer complaints, such as the mechanisms and media for complaints, including receiving complaints, resolving complaints, and monitoring complaints. If the consumer does not agree on the results of the handling and settlement carried out by the Operator, the consumer may submit a complaint to the dispute resolution agency or institution or directly to BI.

---

[65] See Minister of Communication and Informatics Circular No. 5 of 2016 on Limitation and Responsibilities of Platform and Merchant Electronic Commerce Provider, that platform provider is responsible for the operation of electronic system and content management on the platform reliably, safety, and responsibly. However, that obligation is not prevail if can be proven that the error and/or negligence comes from the merchants or platform users.

[66] Bank Indonesia, "Payment System Provider," Pub. L. No. Bank Indonesia Regulation No. 23/6/PBI/2021 (PBI PJP) (n.d.), Article 177 point c, https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI_230621.pdf.

[67] Cooter Robert and Edward L. Rubin, "Theory of Loss Allocation for Consumer Prayer," *Texas Law Review* 66 (1987): 64.

[68] Australian Securities and Investment Commissions (ASIC), "EPayments Code" (n.d.), Adopted March 29, 2016, 15-22, https://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf.

[69] Iwan Setiawan, "Risiko Theft, Fraud, dan Peningkatan Keamanan Sistem Pembayaran Melalui Penguatan Perlindungan Konsumen" (n.d.) (Sesmabi 3 BI Institute Presentation, May 10, 2020).

[70] *Ibid.*

There is no specific authority in Indonesia that is responsible for enforcing the protection of personal data. Rather, this falls under the purview of for consumer protection, it is sectoral and involves many institutions. In addition to BI which is authorised to supervise and monitor consumer protection in the payment system, there are relevant authorities in banking sector (OJK), electronic transaction (the MCIT) and cyber and intelligence agency (the State Cyber and Signal Agency) in supervising open banking. For this reason, it is necessary to coordinate and synergise among BI and related institutions so that the enforcement of personal data protection and consumer protection in Indonesia can run effectively (not overlapping) and efficiently.

To create efficiency related to the resolution of personal data protection disputes in the future, it is necessary to have a dispute resolution agency (such as the MCIT). In terms of consumer disputes related to data protection, BI and other authorities can act as a mediator or resource person at the dispute resolution institution in question, when a dispute arises regarding the implementation of the relevant authority.

V. CONCLUDING REMARKS

In the implementation of the Open API Payments, particularly related to personal data protection and consumer protection, there are legal issues that need to be considered, namely the scope of consumer personal data, types of personal data, access to consumer personal data, due diligence, the importance for contracts between API providers and users, data portability rights, including right to restriction of processing data and right to rectify, consumer consent, handling of data leakage, and dispute resolution. In general, the existing regulations encompass the legal issues in the Open API Payment (including the information security and privacy aspect). Although the protection of personal data and consumer protection has been accommodated by the existing regulations, the amendment to the Consumer Protection Law is demanded to change the "negligence" regime to elevate consumers' positions in dispute resolution.

In addition, considering that there are relevant authorities involved in open banking supervision (among others BI, OJK, Ministry of CIT, and BSSN), the PDP Bill should grant authority that is responsible for enforcing personal data protection, for example the Minister of CIT. In the context of coordination, the resolution of personal data protection cases may present representatives of the competent authorities in data protection in various sectors as panelists. Such coordination is aimed at ensuring that the enforcement of personal data protection and consumer protection in Indonesia can run effectively (not overlapping) and efficiently.

REFERENCES

Amalia, Camila. "Suptech: Penyiapan Ekosistem Digital untuk Mengawal Efektivitas Transformasi Digital di BI." *Buletin Hukum Kebanksentralan* 17, no. 2 (n.d.).

Australian Competition & Consumer Commission and Reserve Bank of Australia. MoU the ACCC and RBA (2018).

Australian Securities and Investment Commissions (ASIC). ePayments Code (n.d.).

Bank Indonesia. *Blueprint Sistem Pembayaran Indonesia 2025 BI: Menavigasi Sistem Pembayaran Nasional di Era Digital*. Jakarta: Bank Indonesia, 2019.

———. *Consultative Paper: Standar Open API dan Interlink Bank dengan Fintech Bagi Penyelenggara Jasa Sistem Pembayaran*. Jakarta: Bank Indonesia, 2020.

———. Payment System Provider, Pub. L. No. Bank Indonesia Regulation No. 23/6/PBI/2021 (PBI PJP) (n.d.).

———. "Standar Nasional Open API Pembayaran." Accessed March 29, 2022. https://apidevportal.bi.go.id/snap/docs/standar-data-spesifikasi-teknis.

Chaib, Ismail. "Regulating Open Banking - How Regulators around the World are Shaping the Future of Financial Services." Berlin, 2018.

CNN Indonesia. "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual." CNN Indonesia. Accessed May 3, 2021. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

Consultative Group to Assist The Poor and Hogan Lovells. *CGAP Guidance Note: Key Considerations When Developing Legal Terms and Conditions for Financial Services APIs*. Washington DC: CGAP, 2020.

Data Protection Commission. "The Right to Rectification," n.d.

European Commission. "Do the Data Protection Rules Apply to Data about a Company?" Accessed June 14, 2021. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en.

_____. "When Should I Exercise My Right to Restriction of Processing of My Personal Data?," n.d.

Goosen, Eric. "The Influence of Law & Regulations on The Process of Digital Transformation at Banks in The Netherlands." Leiden University, 2020.

Indonesia, Government Regulation No. 71 of 2019 on The Implementation of Electronic Systems and Transactions.

_____. Minister of Communication, and Informatics Regulation No. 20 of 2016 on Protection of Personal Data in Electronic System.

_____. Bank of Indonesia Regulation No. 22/20/PBI/2020 on Bank Indonesia's Consumer Protection.

_____. Bank of Indonesia Regulation No. 22/23/PBI/2020 on Payment System.

Indonesian Payment System Association (ASPI). *SNAP - Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)*. Ver. 1.0. Jakarta: Bank Indonesia, 2021.

Leong, Emma. "Open Banking: The Changing Nature of Regulating Banking Data – A Case Study of Australia and Singapore." *Banking & Finance Law Review* 35, no. 3 (2020): 443–69.

Minister of Communication and Informatics. Protection of Personal Data in Electronic System, Pub. L. No. the Regulation of Minister of Communication and Informative No. 20 of 2016 (2016).

Miru, Ahmadi, and Sutarman Yodo. *Hukum Perlindungan Konsumen*. Jakarta: Rajawali Pers, 2017.

Organisation for Economic Co-Operation and Development. "OECD Policies for Information Security & Privacy." Accessed January 10, 2022. https://www.oecd.org/sti/ieconomy/49338232.pdf.

_____. "Personal Data Use In Financial Services And The Role Of Financial Education: A Consumer-Centric Analysis." OECD, 2020.

Puspita, Sherly. "Polisi Bongkar Jual Beli Data Nasabah Bank via Situs Web." Kompas.com. Accessed November 20, 2021. https://megapolitan.kompas.com/read/2018/04/16/21312031/polisi-bongkar-praktik-jual-beli-data-nasabah-bank-via-situs-web?page=all.

Robert, Cooter, and Edward L. Rubin. "Theory of Loss Allocation for Consumer Prayer." *Texas Law Review* 66 (1987): 64.

Setiawan, Iwan. "Risiko Theft, Fraud, dan Peningkatan Keamanan Sistem Pembayaran Melalui Penguatan Perlindungan Konsumen." n.d.

Spire, and Whitesight. "Open Banking: A Game Changer for The Financial Eco-System," 2022. https://aqmen365.com/uploads/Open-Banking-Report---Part-1---V1.3-b32abcb8adfd7d589baff6322302758f.pdf.

The House of Representative. The Draft of Personal Data Protection Bill (2020).

Westpac New Zealand. "Open for Business: A Guide to Open Banking in NZ." Accessed August 7, 2021. https://www.westpac.co.nz/assets/Business/institutional/documents/Thought-Leadership-Articles/Guide-to-Open-Banking-Westpac-NZ.pdf.

Zeller, Bruno, and Andrew Dahdal. "Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection." *Qatar University College of Law, Working Paper Series, Working Paper No. 2021/001*, 2021. https://doi.org/http://dx.doi.org/10.2139/ssrn.3766076.