Jambe Law Journal
ISSN 2598-795X (online); 2598-7925 (print)
Vol. 8 No. 1 (2025): 27-60, DOI: 10.22437/jlj.8.1.27-60

Indonesia's Open Banking Future: Designing Effective Regulatory Approaches

Umi Khaerah Pati[1] *& Anugrah Muhtarom Pratama*[2]

[1]Faculty of Law, Sebelas Maret University; Faculty of Law, Monash University, Australia (corresponding author)
umi_khaerah@staff.uns.ac.id
[2] Faculty of Law, Universitas Sebelas Maret, Indonesia
pratamanugrah23@gmail.com

Abstract

To determine the most suitable approach for framing open banking regulations, it is crucial to understand the specific goals of open banking adoption in a particular country. By employing a legal comparative approach, this paper explores regulatory frameworks for designing open banking regulation in Indonesia. The analysis encompasses key legislative instruments, such as the Payment Services Directive 2 (PSD2) in the UK, Consumer Data Right (CDR) in Australia, General Data Protection Regulation (GDPR) in the EU, and relevant Indonesian laws. The research finds that the Indonesian Financial Services Authority (OJK) Regulation adopts a 'bank-centric' model, granting financial institutions discretionary power over TPP access by establishing bilateral partnerships to facilitate data access. Contrastingly, jurisdictions like the EU, UK, and Australia employ legislative tools that obligate banks to provide TPPs access to customer data upon explicit consent. The 'bank-centric' model under OJK Regulation could reduce consumer choice. Additionally, conflicts of interest may arise, with banks favoring their TPPs, undermining fairness. Lack of standardized access might cause market fragmentation. To achieve the objectives outlined in visions two and three of the BSPI 2025, it is crucial to shift from a 'bank-centric' model to an inclusive framework that fosters broader participation. This objective

can be achieved through the implementation of standardized APIs and a centralized accreditation system for Third-Party Providers (TPPs), as observed in the three countries.

Keywords: open banking; open API; financial regulation; regulatory-driven; standardized API

A. Introduction

Indonesia, has the most significant Fintech and e-commerce market shares in Southeast Asia, although it has been lagging in adopting open banking.[1] In 2020, Central Bank of Indonesia ("BI", *Bank Indonesia*) initiated visions two and three through the Blueprint for Indonesia Payment System 2025 ("BSPI 2025", *Blueprint Sistem Pembayaran Indonesia 2025*). The essence is to promote the role of banking in the payment system by formulating an Open API Standard.[2] In 2021, BI issued Regulation of the Members of the Board of Governors ("PADG", *Peraturan Anggota Dewan Gubernur*) Number 23/15/PADG/2021 concerning the National Standard for Open Application Programming Payment Interfaces ("PADG 23/2021"). Moreover, in the same year, BI, together with the Indonesian Payment System Association ("ASPI", *Asosiasi Sistem Pembayaran Indonesia*), introduced the National Standard Open API Payment ("SNAP", *Standar Nasional Open API Pembayaran*) as a Regulatory Technical Standard ("RTS") from PADG 23/2021.[3] Regarding market regulations, several banks in the country are more progressive and independently adopted the Open API. These include the pioneer bank BRI, followed by BCA. The challenge is centered on the fact that the two banks have different standards of uniformity detected during the implementation of

1 Google, Temasek, and Bain & Company, "E-Conomy SEA 2021—Roaring 20s: The SEA Digital Decade," 2021, https://seads.adb.org/report/e-conomy-sea-2021-roaring-20s-sea-digital-decade.

2 Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia 2025," 2020, https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx.

3 ASPI and BI, "Standar Nasional Open API Pembayaran," 2021, https://www.bi.go.id/id/layanan/Standar/SNAP/default.aspx.

Open API connectivity. The UK's Competition and Markets Authority ("CMA") determined that the lack of standardized APIs caused significant difficulties for new entrants, who faced high costs either developing applications compatible with multiple API standards or relying on third-party services to achieve interoperability. Banks that use proprietary or non-standard APIs may unintentionally erect barriers for third-party developers.[4]

The regulatory frameworks established in the European Union, the United Kingdom, and Australia provide compelling evidence of a decisive shift towards mandating Third-Party Provider ("TPP") access to bank-held customer data. Through specific legislative instruments such as the EU's PSD2 (notably Articles 66 and 67), the UK's CMA Order 2017 (particularly Articles 10 and 14), and Australia's Competition and Consumer Act 2010 (Part IVD) complemented by the Consumer Data Right (CDR) Rules, these jurisdictions have created clear legal obligations for banks and other data holders. Supporting these primary legal mandates are detailed technical and operational standards, such as the EU's Regulatory Technical Standards on SCA and CSC, the UK's OBIE Standards, and Australia's Consumer Data Standards. These standards ensure that the mandated access is not only a legal right but also a practical reality, implemented in a secure, consistent, and interoperable manner.

While in Indonesia, we find that the Financial Services Authority of Indonesia Regulation ("POJK", *Financial Services Authority Regulations*) No. 21 of 2023 on Digital Services ("POJK 21/2023") by Commercial Banks adopts a 'bank-centric' model, granting financial institutions discretionary power over TPP access by establishing bilateral partnerships to facilitate data access. The 'bank-centric' model under OJK Regulation No. 21 of 2023 might pose limitations by confining TPP access to those with established bank partnerships. This constraint can potentially hamper innovation and diminish consumer choice. Furthermore, conflicts of interest may emerge as banks

4 Giuseppe Colangelo and Oscar Borgogno, "Shaping Interoperability for the Internet of Things: The Case for Ecosystem-Tailored Standardisation," *European Journal of Risk Regulation* 15, no. 1 (March 1, 2024): 137–52.

could prefer their associated TPPs, thus jeopardizing fairness within the financial landscape. The absence of standardized access might also contribute to market fragmentation, elevating operational intricacies for TPPs and obstructing the evolution of a unified open banking system in Indonesia.[5] Our recommendation is to transition from a 'bank-centric' model to a more inclusive framework by implementing standardized APIs and a centralized accreditation scheme for TPPs. This approach ensures secure and equitable access to customer data based on explicit consumer consent, rather than bilateral agreements.

Recent studies have touched upon the topic, including the "Triangular Insight on Open Banking in Indonesia, Singapore, and Australia."[6] This research examines open banking implementations across these countries, focusing on API standardization, security, regulatory sandboxes, customer insights, and user experiences. While it offers a broad overview, my research delves into regulatory frameworks and technical standards in Australia, the EU, and the UK, comparing them with Indonesia's approach. Specifically, I critically assess the 'bank-centric' model outlined in Indonesia's Regulation No. 21 of 2023 on Digital Services by Commercial Banks, and propose recommendations to align it with the broader vision of open banking in Indonesia, promoting financial inclusion and competition. Another relevant study, "Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment," conducts a comprehensive review of open banking in Indonesian addressing various potential issues for balanced regulatory frameworks that promote financial innovation while safeguarding consumer rights.[7] However,

5 Jamal Wiwoho, Umi Khaerah Pati, and Anugrah Muhtarom Pratama, "Reciprocal Data Portability to Foster Financial Services Competition in the Open Banking System Era," *Yustisia Jurnal Hukum* 13, no. 2 (August 27, 2024): 134.

6 Sapto Hermawan, Zenia Aziz Khoirunisa, and Kukuh Tejomurti, "Triangular Insight on Open Banking in Indonesia, Singapore, and Australia," *International Journal of Legal Information* 51, no. 3 (November 25, 2023): 197–215.

7 Camila Amalia, "Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment," *Journal of Central Banking Law and Institutions* 1, no. 2 (May 31, 2022).

it provides a general overview of open banking in Indonesia, especially personal data protection and consumer protection aspect. In contrast, my research focuses on analyzing open banking regulations and technical standards, offering a comparative perspective with Australia, the EU, and the UK. Through a comparative legal analysis, the study identifies key differences, regulatory gaps, and areas for improvement in transparency, and responsible data-sharing practices.

B. Open Banking Concept

In the financial services sector, banking has produced useful monetary data such as deposits, credit, transaction histories, transfer checks, balances, and other information to predict consumer eligibility while avoiding the risk of failure. Fintech further utilized these benefits, which emerged due to the global crisis in 2008. Fintech tries to take advantange by creating new technology-based opportunities that are rapidly changing and radically adopting the financial services approach to innovation.[8] On the other hand, Fintech raises concerns about data collection, as these have been obtained through screen scraping—a process that requires customers to provide their bank authentication credentials (namely login and password information) to the TPP.[9] The adoption of this approach by Fintech raises several concerns: First, its main weakness is that the scraped banking web does not have an expiration date;[10] Second, screen scraping is perceived as dangerous because it alows Fintech to copy individual data without their consent, thereby increasing the risk of identitiy fraud;[11]

8 Tania Babina, Greg Buchak, and Will Gornall, "Customer Data Access and Fintech Entry: Early Evidence from Open Banking," *SSRN Electronic Journal*, 2022, 1–74.

9 Peter Gomber et al., "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services," *Journal of Management Information Systems* 35, no. 1 (2018): 220–265.

10 Benjamin L.W. Sobel, "A New Common Law of Web Scraping," *Lewis & Clarck Law Review* 25, no. 1 (2021): 149–206.

11 Andrew M. Parks, "Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers," *Michigan Law Review* 20, no. 5 (2022): 914–945.

and Third, there are no mandatory data sharing standards.[12] This allows Fintech to receive more information than necessary, leading to cyber threat crimes.

Given that screen scrapping raises concerns about potential security risks and is detrimental to both consumers and banks, the idea of an open banking framework emerged to respond to these challenges. It is designed to maintain a more secure financial system while enabling consumers to seamlessly transfer their monetary data through Application Programming Interfaces (API) infrastructure.[13] At the same time, it also provides Fintech with easier access to connect with banks while preventing data collection through screen scraping.[14] Gradually, the open banking framework was no longer limited to finance and Fintech because e-commerce, startups, and other financial institutions joined forces and eventually became known as TPP.[15] In this situation, consumers do not only play a significant role, rather they also benefit from the presence of interlink open banking. These efforts ultimately led to the creation of a more open or transparent data-sharing environment. This eventually became widely known and also served as an attraction for regulators in various jurisdictions to adopt open banking. Several jurisdictions, such as the EU, UK, Australia, US, Singapore, and Hong Kong, have advanced to adopt this framework.

The concept of open banking demands an interface that allows sharing of data flows from one institution to another, specifically a third party, based on the customer's approval for the transfer process to be successful.[16] Its presence brings substantial benefits, such as improving customer experience, generating new revenue streams,

12 Han-Wei Liu, "Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment," *Washington International Law Journal* 30, no. 1 (2020): 28–62.

13 Linda Jeng, *Open Banking* (Oxford: Oxford University Press, 2022).

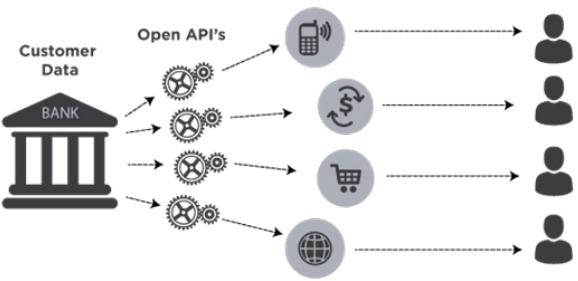
14 Jeng, *Open Banking…*

15 Jeng, *Open Banking…*

16 Anshu Premchand and Anurag Choudhry, "Open Banking & APIs for Transformation in Banking," in *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)* (IEEE, 2018), 25–29.

and enabling a sustainable service model in underserved traditional markets.[17]

Figure 1. Open Banking Concept



Source: The Institute of International Finance (2022)

The data ocean wave interface is used through API, a communication protocol with programmed standards. The essence is to facilitate data sharing without needing additional infrastructure.[18] However, through the API, different systems or applications can directly interact with one another in terms of utilizing data sharing, thereby creating a new customer experience.[19] It is also perceived as the key interface adopted in various jurisdictions. The largest benefit of API is providing an integrated system that supports data protection and reduces screen scraping practices, thereby minimizing risks.[20]

Technically, the presence of an API can either be opened or closed. The difference is relatrelated to third-party access to the acquired data. Incidentally, when it is exposed to the public, the Open API is used, and assuming the data is only limited within the insti-

17 Theo Lynn, Pierangelo Rosati, and Mark Cummins, "Exploring Open Banking and Banking-as-a-Platform: Opportunities and Risks for Emerging Markets," in *Entrepreneurial Finance in Emerging Markets* (Cham: Springer International Publishing, 2020), 319–334.

18 Steve Mansfield-Devine, "Open Banking: Opportunity and Danger," *Computer Fraud & Security* 2016, no. 10 (2016): 8–13.

19 Devine, "Open Banking...."

20 Bank for International Settlements, "Report on Open Banking and Application Programming Interfaces (APIs)" (Switzerland, 2019), https://www.bis.org/bcbs/publ/d486.htm.

tution that developed it, the closed API is employed.[21] Open API is adopted in open banking because it allows interaction with TPP. Its presence in open banking initiatives serves as a catalyst with respect to future transformation for mainstream use. Zachariadis and Ozcan stated that banks are not burdened with the presence of the Open API. It is an opportunity for connectivity through standardization.[22]

C. Regulatory Approach to Open Banking Regime

Globally, there is no single framework approach related to the adoption of open banking because it is regulated differently depending on the country's objectives. However, the global open banking framework can be grouped into two approaches, namely market, and regulatory-driven. UK and Australia are regulatory-driven due to comprehensive regulations.[23] Singapore and Hong Kong are market-driven nations. They facilitate market movements towards self-regulation by introducing standardized guidelines.[24] Even though there are certain differences globally in general, the jurisdictions that have taken the lead in adopting an open banking framework have more or less similar regulations. These include (i) the types of product data and services shared, (ii) implementation phase schedule, (iii) regulatory agencies and other participating institutions, (iv) the parties involved, and (v) standardization (data, technical, and security). A detailed explanation of an open banking approach adopted by various jurisdictions globally is shown in Table 1.

---

21 Yuanbo Qiu, "The Openness of Open Application Programming Interfaces," *Information, Communication & Society* 20, no. 11 (November 2, 2017): 1720–1736.

22 Markos Zachariadis and Pinar Ozcan, "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking," *SWIFT Institute Working Paper No. 2016-001*, 2017.

23 Ross P. Buckley, Natalia Jevglevskaja, and Scott Farrell, "Australia's Data-Sharing Regime: Six Lessons for Europe," *King's Law Journal 33*, no. 1 (2022): 1–31.

24 Emma Leong, "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia And Singapore," 2020, https://ssrn.com/abstract=3678458.

Table 1. Regulatory Framework of Open Banking Across Various Countries

Aspect	EU	UK	Australia	Hong Kong	Singapore
Approach	Regulatory-driven	Regulatory-driven	Regulatory-driven	Market-driven	Market-driven
Key Legislative/ Regulatory Instrument(s)	Directive (EU) 2015/2366 (PSD2) & RTS (Reg. (EU) 2018/389)	CMA Retail Banking Market Investigation Order 2017 & FCA Rules	Competition and Consumer Act 2010 (Part IVD) & CDR Rules 2020	Open API Framework for the Hong Kong Banking	API Playbook
Key Regulatory/ Oversight Bodies	European Banking Authority (EBA), National Competent Authorities (NCAs)	Competition and Markets Authority (CMA), Open Banking Implementation Entity (OBIE), Financial Conduct Authority (FCA)	Australian Competition and Consumer Commission (ACCC), Office of the Australian Information Commissioner (OAIC), Data Standards Body (DSB), The Treasury	Hong Kong Monetary Authority	Monetary Authority Singapore
Scope of data to be shared	(1) Transaction account (payment account) (2) Saving account	(1) Transaction account; (2) Customer acquisition (credit cards); (3) Saving account	(1) Account information (saving account, cheque account, account balance); (2) Product information (credit card offerings, deposit rates, service changes); (3) Customer acquisition (credit card, loans, mortgage, investment loans); (4) Transaction account (payment and transfer)	(1) Product information (credit card offerings, deposit rates, service changes); (2) Customer acquisition (credit card, loans); (3) Account information (saving account, account balance); (4) Transaction account (payment and transfer)	(1) Financial information (deposits, credit cards, loans, and investment) (2) Saving account
Participant	ASPSP (Account Servicing Payment Services Providers) – Bank and similar institution	CMA 9 (Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, Natwest Group, and Santander)	All banks and Authorized Deposit-Taking Institution (ADI)	28 participating banks	Citibank, DBS, HSBC, Maybank, OCBC, Standard Chartered, and UOB
Open API standards	Yes	Yes	Yes	Yes	Yes

Source: World Bank (2022)

In the context of adoption, the EU and UK employed a regulatory-driven approach. This is because their narrative is based on a desirable balance between innovation and competition while maintaining the resilience of data access systems to improve the financial services sector.[25] Furthermore, Australia has certain similarities with the EU and UK. Data protection is not only limited to the banking sector, it also includes the telecommunications and energy fields.[26] For the under regulatory-driven, the regulators during the early phase of the transition from market-led to an established framework include the implementation phase or mandatory deadline, the imposition of specific rules for different categories of financial institutions, setting standards, and demanding compliance with certain requirements.[27]

On the other hand, Singapore and Hong Kong both have broader market development goals.[28] With strong conviction, the transition to data collection becomes more successful with standard guidance without the imposition of special requirements by regulators.[29] They are mainly responsible for issuing recommended standard guidelines without complying with the adopted order.[30] The major goal is to create a collaborative ecosystem that promotes innovations, openness to new businesses, and digitalization of the banking sector, thereby generating financial inclusion and advancing the industry.

---

25 Alan Brener, "Payment Service Directive II and Its Implications," in *Disrupting Finance* (Cham: Springer International Publishing, 2019), 103–119.

26 Bruno Zeller and Andrew M. 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.

27 Rachel Gauci, "Is Europe a Good Example of Open Banking?," in *The PayTech Book* (Wiley, 2019), 86–87.

28 Leong, "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia And Singapore."

29 Nydia Remolina, "Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World," *SMU Centre for AI & Data Governance Research Paper No. 2019/05*, 2019.

30 Aurelio Gurrea-Martṭnez, "Disruptive Technologies and Digital Transformation of the Financial Services Industry in Singapore: Regulatory Framework and Challenges Ahead," *SMU Centre for AI & Data Governance Research Paper No. 11*, 2020.

D. Regulatory Issues for Indonesia's Open Banking Regime

1. TPPs Data Access: Review for POJK Regulation No. 21 of 2023 on Digital Services by Commercial Banks

The current situation in the country regarding the adoption of open banking is at an intersection between market-drivenor regulatory-driven options. Based on the regulator's perspective, both BI and the Financial Services Authority of Indonesia ("OJK", *Otoritas Jasa Keuangan*) have not provided directives on the framework or approach to be adopted in order to enact comprehensive regulations, even though the implementation of an open banking system is a major goal that must be achieved by 2025. In 2023, the OJK issued POJK 21/2023, which addresses the provision of digital services by commercial banks. Effective from December 22, 2023, this regulation replaces the earlier Regulation No. 12/POJK.03/2018. A significant aspect of the new regulation pertains to the partnership between banks and third parties, emphasizing the importance of meeting minimum standards without imposing sanctions for non-compliance in instances where banks do not provide customer-requested data.

Consequently, banks are mandated to share data in accordance with agreements between the third parties involved, and only those third parties that have established partnerships with banks are granted access to customer data. The regulation, however, does not specify standards pertaining to data sharing limitations. Instead, it grants discretion to the parties involved and relies on customer consent. Technical standards for interoperability and security are stipulated in the aforementioned OJK regulation and SNAP. This contrasts with the regulatory frameworks in place in the UK, EU, and Australia, which may adopt a more prescriptive approach in defining standards for data sharing and access.[31] In Indonesia, it is the bank that determines the policies and procedures for designating partners, as well as the rights and obligations of partners.[32] Characterized as 'bank-centric,'

31 See Article 31 POJK 21/2023
32 See Article 2, 15, 16 POJK 21/2023

potentially lacking legally mandated right for licensed or accredited TPPs to access customer data.[33]

In essence, PSD2 contains provisions that establish the legal foundation for open banking services. Specifically, Articles 66 and 67 of the directive are critical for payment initiation service providers (PISPs) and account information service providers (AISPs). Article 66 ensures that customers can use a PISP to initiate a payment. Once the customer consents to this, the account servicing payment service provider (ASPSP) must:

a) Communicate securely with the PISP;
b) Immediately provide all relevant payment information to the PISP;
c) Treat payments initiated by a PISP on par with direct customer payments.[34]

Article 67 gives AISPs the legal right to access account information with customer consent. AISPs can access designated payment accounts and associated transactions without requesting sensitive data. The ASPSPs are obligated to provide this information securely. These articles essentially give TPPs a right to initiate payments and access account information, while obliging ASPSPs to facilitate these rights. However, ASPSPs can deny access if they have justified reasons related to unauthorized or fraudulent activity by the TPP.[35]

Moreover, The EU's PSD2 empowered the European Banking Authority (EBA) to create Regulatory Technical Standards (RTS) for consistent and secure implementation across the region. The RTS for Strong Customer Authentication (SCA) and common and secure communication standards are laid out in the Commission Delegated Regulation (EU) 2018/389.

These standards operationalize PSD2's access provisions. Article

33 Annisa Rahma Diasti, "Regulating Data Exclusivity of Ride-Hailing Service in Indonesian Competition Law," *Indonesia Law Review* 11, no. 3 (2021): 285–302.

34 See Article 66 Directive (EU) 2015/2366 of The European Parliament and of the Council on Payment Services in the Internal Market

35 See Article 67 Directive (EU) 2015/2366 of The European Parliament and of the Council on Payment Services in the Internal Market

30 specifically mandates that account servicing payment service providers (ASPSPs) must provide at least one secure interface for TPPs to identify themselves and initiate payments or access account information. This interface must also allow TPPs to rely on ASPSP's authentication procedures. ASPSPs are required to adhere to European or international communication standards, document their interface specifications, and make them available to authorized TPPs free of charge.[36]

Regulatory Technical Standards (RTS) Article 34, which pertains to certificates, mandates that third-party providers (TPPs) must utilize qualified certificates for electronic seals or website authentication, as outlined in the EU's eIDAS Regulation No 910/2014. These certificates, containing the TPP's authorization number, its role (AISP, PISP, etc.), and the name of its competent authority, serve as a secure identification method when TPPs interact with account servicing payment service providers (ASPSPs). This standardized approach not only ensures a trusted identification process but also forms the basis for ASPSPs to grant access to TPPs, thereby fostering overall trust within the open banking ecosystem.

While in Australia, Part IVD of the CCA and the CDR Rules establish a legal obligation for Data Holders to share CDR data with Accredited Data Recipients via standardized APIs upon valid consumer request.[37] In the United Kingdom, EU and Australia, open banking regulations do not mandate that banks and third-party providers (TPPs) establish bilateral partnerships to facilitate data access. Instead, the regulatory framework is designed to promote a standardized and competitive environment where any authorized TPP can ac-

36 See Article 30 Commission Delegated Regulation (EU) 2018/389 Supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication

37 Office of the Australian Information Commissioner, "Consumer Data Right Legislation," 2020, https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-legislation.

cess customer data—provided they have obtained explicit customer consent—without the need for individual agreements with banks.[38] By presenting concrete examples and detailing the operational mechanisms, illustrates how these regions have proactively legislated for TPP access to foster a more dynamic, competitive, and consumer-focused financial ecosystem. This mandate for sharing data to TPPs is enforced through **regulatory mechanisms (called regulatory-driven approach),** requiring national regulators to oversee and ensure compliance by financial institutions. Without such regulation, banks may not voluntarily comply.

Table 2. Comparative Overview of Mandated TPP Access Rights

Feature	European Union (PSD2)	United Kingdom (Open Banking)	Australia (Consumer Data Right)
Basis of Access Mandate (Specific Articles/ Sections)	PSD2 Arts. 66 (PISPs), 67 (AISPs); RTS Arts. 30-32	CMA Order 2017 Arts. 10, 14	CCA Part IVD (esp. ss. 56AC, 56BL); CDR Rules (e.g., Part 4, 7)
Mechanism for Access (API Standards Source)	ASPSP-implemented APIs based on RTS (EBA)	Standard APIs based on OBIE Standards	DH-implemented APIs based on Consumer Data Standards (CDS) by DSB

Although it is admittedly difficult to ascertain which approach is best or suitable for Indonesia, the ability to determine this is centered on the initial goal of adopting an open banking framework. However, this, in turn, is based on the realization of visions two and three of the BSPI 2025, which supports banking digitalization. This involves the use of an Open API to create a healthy, competitive, and innovative payment system that is integrated, interconected, and interoperability, as well as the security and reliability of infrastructure by 2025.[39] It is implicitly understood that the purpose of adoption in

38 Anis H. Bajrektarevic et al., "Costumer Explicit Consent Under Indonesian Open Banking Regulations," *Jambura Law Review* 4, no. 2 (July 30, 2022): 176–94.

39 Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia 2025."

Indonesia is similar to the EU and UK in terms of boosting competition and innovation in a balanced manner while maintaining system security.[40] Preliminary evidence can be used to prove that a market-driven approach is unsuitable for achieving the targets set by BI in promoting the adoption of open banking by 2025.

Furthermore, several reasons need to be considered. First and foremost, through a market-driven approach, the adoption is voluntary. Not being mandatory can hinder the entire process, even though regulators have employed various promotional and encouraging steps.[41] It is feared that in Indonesia, banks are slow and have failed to immediately adopt the necessary step, thereby being unable to realize the set target by 2025.

Second, it was recently discovered that the OJK as the banking supervisor that monitors all activities through a Roadmap for Indonesia Banking Development 2020 – 2025 ("RP2I 2020-2025", *Roadmap Pengembangan Perbankan Indonesia 2020 – 2025*), recommended the adoption of an open banking framework by issuing mandatory regulations as a step to accelerate digital transformation in the finance sector.[42]

Third, Chan et al stated that using a regulatory-driven approach offers more benefits to both the regulators and participating parties than a market-driven method.[43] This is because, initially, it builds consumer confidence and contributes to improving the reputation of the participating parties. Furthermore, regulatory-driven technical

40 Billiam Billiam, Lastuti Abubakar, and Tri Handayani, "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking," *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 9, no. 1 (2022): 67–88.

41 Leong, "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia And Singapore."

42 OJK, "Roadmap Pengembangan Perbankan Indonesia 2020 – 2025," 2020, https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/-Roadmap-Pengembangan-Perbankan-Indonesia-2020---2025.aspx.

43 Rebecca Chan et al., "Towards an Understanding of Consumers' FinTech Adoption: The Case of Open Banking," *International Journal of Bank Marketing* 40, no. 4 (2022): 886–917.

standards can improve the interoperability of data exchange through API to stimulate consumer expectations in facilitating the adoption of open banking. This finding is useful, specifically in the Indonesian context, where consumers are confident enough to share their financial data to adopt open banking.

With the earlier mentioned considerations, irrespective of the fact that the regulatory-driven approach is mandatory and coercive, there is a greater chance of achieving BI's target of adopting an open banking framework in accordance with BSPI 2025. Therefore, this method needs to be promoted during the preparatory process to continue the SNAP program that was previously issued. This approach is expected to create a holistic view of a real banking transformation engine. This is despite the reluctance of many consumers to share their financial data, specifically when the market drives the initiative. At the same time, assuming this is regulatory-driven, it will help existing banks to become more innovative, thereby leading to greater consumer benefits.

One of the most important elements of this framework is the Open API infrastructure. It helps create an ecosystem that allows players to share their data in a uniform way. Furthermore, Open API seamlessly connects protocol standards as it promotes integration, interconnection, interoperability as well as security and reliability of infrastructure among players. Its benefits offer individuals more control because data needs to be collected based on their consent, there by enabling practitioners and regulators to increasingly consider and treat it as a proper protocol infrastructure. This facilitates open banking as well as ensures smooth data sharing on platforms, primarily providing a more competitive playing field between Fintechs and banks.

This is also related to RtDP which was earlier explained in the previous section. During the application of open banking, its existence leads to related characteristics where information is subject to portability without violating the provisions of personal data protec-

tion through Open API standardization.[44] The creation of Open API standardization is important in terms of providing data, and technical standards as well as its security through consumer protection obligations and ensuring consistent Open API implementation across all banks.

In respect to its accommodation, it needs to be strengthened by its inclusion in SNAP. It is perceived as part of an open banking in regulating data standards in the Open API. This is beacuse the existing regulations allow for data sharing between banks and third parties which are also allowed to use the Open API platform. However, there is no specific regulation regarding data standardization. Previously, how participants, data standards in the Open API, consumer protection obligations and liability as well as RtDB support needed were summarized, but there have been no further steps since SNAP was issued. Learning from the EU, UK, and Australia on how to adopt regulatory-driven open banking, it was discovered that they had selected a top-down model with a regulatory body that guides and oversees the process in data standards. In the regulatory-driven approach, regulators develop highly prescriptive technical standards that mandate specific processes for sharing data, while strictly enforcing compliance.

Therefore, as discussed in the previous sections, Indonesia needs additional strengthening in regulating the legal substance that has been suggested through SNAP as RTS. This can not only regulate the substance of the previous law, but also the role of ASPI that can be maximixed to support and assist BI in the implementation, development, and supervision of open banking in the country, as implemented in the UK and Australia with OBIE and CSIRO Data61, respectively.[45]

---

44 Jamal Wiwoho, Umi Khaerah Pati, and Anugrah Muhtarom Pratama, "Enabling Data Portability and Interoperability Under Indonesia's Data Protection Law," *Masalah-Masalah Hukum* 53, no. 3 (December 30, 2024): 271–82.

45 Dian Purnama Anugerah and Masitoh Indriani, "Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective)," *Sriwijaya Law Review* 2, no. 1 (January 31, 2018): 82.

2. Participant

In global practice, the two models used in engagement are related to the adoption of open banking. First, using entities that specifically mention providers through appointments, such as the UK, which directly appointed CMA 9 because it accommodates the nine largest banks apointed to adopt open banking. Second, using a broad provider entity for all banks or other non-banking institutions, as is executed by some jurisdictions. Examples include ASPSP (Account Servicing Payment Services Providers) in the EU, Authorized Deposit-Taking Institution (ADI) in Australia, as well as Hong Kong, and Singapore.

Furthermore, the broad provider entity model is further divided into two schemes. These include the mandated and provider entities permitted to adopt open banking. The mandated entity is found in the EU and open to all banks and non-banking institutions because it is required for immediate adoption within a predetermined time limit.[46] This temporary entity is also permitted, as is the practice carried out in Australia, although all banks and other non-banking institutions. Although the implementation process is carried out in stages.[47] In Australia, adoption started in November 2020 for the four big banks first and is bound to continue from July 1, 2021. All banks and non-banking institutions are allowed to adopt the procedure, irrespective of the fact that there is no time limit exception.[48] This is indeed similar to an entity that specifically mentions providers that can adopt open banking as practiced in the UK. In this case, there is a specificity where in the long term the regulator assesses and designs a timeframe in accordance with the country's conditions and the context of an open banking adoption.

Meanwhile, in Indonesia, the provider is known as a Payment

46 Gauci, "Is Europe a Good Example of Open Banking?"

47 Bruno Zeller and Brian Lynch, "Challenges in Open Banking - What Are the Practical Steps to Be Taken Now?," *University of Western Australia Law Review* 48, no. 2 (2021): 579–605.

48 Clare Sullivan, "The New Australian Consumer Data Right: An Exemplary Model for Open Banking," *WIREs Forensic Science*, March 15, 2022.

Service Provider (PJB). It is either a Bank or Non-banking Institution that facilitates payment transactions. Regarding adopting an open banking framework in the country, BI through PADG 23/2021 was used to determine the most recent time for implementing SNAP on Open API. It was reported to be effective no later than June 30, 2022, for PJB, which had previously implemented the API. The PJB candidates who wish to implement the API should apply no later than December 31, 2022.

Table 3. Comparative Overview of Participant on Open Banking

Feature	European Union (PSD2)	United Kingdom (Open Banking)	Australia (Consumer Data Right)	Indonesia
Key Terminology for TPPs	Account Information Service Provider (AISP), Payment Initiation Service Provider (PISP)	Third Party Provider (TPP) (acting as AISP/PISP)	Accredited Data Recipient (ADR)	Payment Open API Service Provider (Service Provider) • Open API Payment Service Users, (Service Users) • PJP Service User Open API Payment (PJP Service User) • Non-PJP Service Users Open API Payments (Non-PJP Service Users)
Key Terminology for Data Holders/Banks	Account Servicing Payment Service Provider (ASPSP)	ASPSP (Bank/Provider)	Data Holder (DH)	Bank or Payment Open API Service Provider (Service Provider)

The model used by Indonesia is also similar to the EU, which involves the use of a time limit. However, this is not limited to several providers, including banks and non-banking institutions. Certainly, some benefits are associated with using a broad category of provider

entities. It ensures all providers, including banks and non-banking institutions, are involved without exception, thereby having a greater impact on various financial services that can be activated. This also triggers competition, increasing financial inclusion and making fiscal services more affordable.[49] It is interesting to create high inclusiveness, specifically since the regulators target at this time is to pursue the financial service sector.

However, there are legitimate concerns about forcing all providers to participate rapidly, given that their preparation for adoption has not been uniform. This consideration considers that initially, the EU had set an adoption schedule of which the maximum limit was January 2020. Although the EU had repeatedly extended the deadline for PSD2 compliance, January 1, 2021, was the final date.[50] The regulator is to be on guard in terms of providing additional options when, after December 31, 2022, there are providers, both banks and non-banking institutions, that wish to adopt API, to be allowed. There is a need to set aside time for these providers to have the last chance.

In contrast to the Indonesian model, the UK, EU, and Australia adopt a different approach to TPPs accessing consumer data. These jurisdictions require TPPs to secure accreditation before accessing bank data through open APIs. In **Australia,** the **Consumer Data Right** (**CDR**) requires TPPs, termed Accredited Data Recipients (ADRs), to be accredited by the **Australian Competition and Consumer Commission** (**ACCC**)**,** following strict cybersecurity and operational guidelines (Competition and Consumer Act 2010, Part IVD). In the **EU**, under the **Revised Payment Services Directive** (**PSD2**)**,** TPPs like Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) must comply with **Regulatory Technical Standards** (**RTS**) **on Strong Customer Au-**

49 Ria Setyawati, Stefan Koos, and Zalfa A.F. Jatmiko, "Data Driven Dominance in Digital Markets: Assessing Indonesian Competition Law in the Digital Age," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 2 (August 28, 2024): 264–84.

50 Oscar Borgogno and Giuseppe Colangelo, "Data, Innovation and Competition in Finance: The Case of the Access to Account Rule," *European Business Law Review* 31, no. 4 (2020): 573–610.

thentication (**SCA**) **and Common and Secure Communication** (**CSC**) (EU Regulation 2018/389). Similarly, in the **UK,** TPPs must be authorized by the **Financial Conduct Authority** (**FCA**) under PSD2 and adhere to the **Open Banking Implementation Entity** (**OBIE**) **Standards,** ensuring secure and uniform access across the banking ecosystem.[51] Currently, Indonesia lacks a centralized accreditation scheme for Third-Party Providers (TPPs) to access consumer data within an open banking framework, in contrast to the systems implemented in the European Union, the United Kingdom, and Australia.

Table 4. Comparative Overview of TPP Authorization Access Rights

Feature	European Union (PSD2)	United Kingdom (Open Banking)	Australia (Consumer Data Right)
TPP Authorisation/ Accreditation Requirement	Authorisation/ registration by NCA	FCA Authorisation/ registration & OBIE Directory Enrolment	ACCC Accreditation
Core Principle of Customer Consent	Explicit Consent	Explicit Consent	Consumer-directed, explicit, informed Consent

Instead, OJK Regulation No. 21 of 2023 on Digital Services by Commercial Banks stipulates that TPPs seeking to collaborate with banks must obtain authorization from OJK or other competent authorities, and such partnerships must be founded on bilateral cooperation agreements between the banks and TPPs.

3. Data Standards in Open API

For open banking to function, there must be certain minimum requirements. These include data and technical standards, which are essential for implementing this framework. With respect to informa-

51 Paripurna P Sugarda and Muhammad Rifky Wicaksono, "Enhancing The Competitiveness Of Indonesia's Financial Services Sector in the Digital Era Through Open Banking: Lessons Learned From The Uk's Experience," *Journal of Central Banking Law and Institutions* 2, no. 1 (2023): 153–78.

tion exchange, the provision of data standards helps define the Open API terms of reference.[52]By determining its appearance or form, sharing information between two or more parties is easier. Several advantages can be obtained by entering standard data into the Open API. This includes improving its quality, allowing for the reuse of data elements and other information, and reducing costs. Another benefit is maintaining code consistency by defining semantics and syntax for data sent through the Open API, thereby creating a common language for communication between the parties.

Determining the desired data standard can be carried out simultaneously by discerning the technical standards that do not support the Open API specification reference. These include communication protocols, architecture types, data formats, and structures realized through a sandbox that can be accessed through the developer site portal to create uniform standards. However, during the determination, several models can be set. Firstly, establishing technical regulations as an inseparable part issued by the regulators, such as the EU under the EBA, which forms Regulatory Technical Standards (RTS), based on strong customer authentication and secure communication (SCA&CSC).[53] Secondly, on a hybrid basis, it delegates the implementation of assistance entities which the regulator then reviews for approval. An example of this scenario is found in Australia, where CSIRO's Data61 was appointed as the Data Standards Body (DSB) under the CDR regime to regulate data and Open API technical standards.[54] A similar incident is also witnessed in the UK, CMA delegates Open Banking as the Implementation Entity (OBIE), which is tasked with determining and supervising API, and data standards, including

52 Abdulaziz Almehrej, Leo Freitas, and Paolo Modesti, "Account and Transaction Protocol of the Open Banking Standard," in *Rigorous State-Based Methods*, 2020, 230–236.

53 European Banking Authority, "EBA Industry Working Group on APIs under PSD2," 2021, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2.

54 Leila Fourie and Thomas K. Bennett, "The Open Banking Era: Surfing the Australian Data Wave," in *Transformation Dynamics in FinTech: An Open Innovation Ecosystem Outlook*, 2021, 247–279.

governance structures.[55] For example, in this country, OBIE has standardized the data in their API based on the following:

- All functional and non-functional technical standards published by OBIE, including (but not limited to) the RAML and Swagger specifications, naming standards, versioning, error messages, availability, performance, caching, throttling, security ciphers, and use of headers or metadata;
- ISO20022 standards for data structure as a primary requirement. When this is not possible, the data structure must contain elements that are ISO20022 compliant as a minimum;
- World Wide Web Consortium (W3C) specifications that are considered relevant;
- The Data Protection Act 2018 and General Data Protection Regulation (EU 2016/679), when applicable.[56]

Where these standards are altered occasionally, API Providers ensure that they support versions in line with the OBIE's service levels and policy for releasing new management and versioning.

Meanwhile, data standards in Indonesia are unavailable at the law and regulation level, as summarized in Table 2. Recently, BI, through PADG 23/2021, stated that the data categories applied in the Open API include registration and balance information, transaction history, credit, and debit transfers, as determined by this financial institution. Article 9 paragraph (1) of PADG 23/2021 states that the implementation of data standards is published on the SNAP developer site. The data standards in the SNAP developer site are not yet available. The PADG SNAP requires its application for the parties involved to be applied in the Open API. According to this research, the operation of open banking in Indonesia can occur in a similar manner as in the EU, where PSD2 came into effect in January 2018. Its practical implementation started in September 2019, when data

55 Open Banking is the Implementation Entitiy, "About the OBIE," 2022, https://www.openbanking.org.uk/about-us/.

56 OBIE, "Open Banking: Guidelines for Open Data Participants," 2018, https://www.openbanking.org.uk/document/guidelines-for-open-data-participants/.

Table 5. Standard Data in Laws and Regulations in Indonesia

Type of laws and regulations	Remarks
Law Number 7 of 1992 concerning Banking as Amended by Law Number 10 of 1998	Banks are obligated to maintain the confidentiality of customer data, except as long as it is used for the purposes of, among others: taxation, interests in criminal and civil cases, settlement of bank receivables, exchange of information between banks, and regulated by law, and approval, request or written authorization from customers including heirs when the customer has died.
Law Number 21 of 2008 concerning Sharia Banking	It is the same as the Banking Law.
Bank Indonesia Regulation Number 22/23/PBI/2020 concerning Payment Systems	Banks are allowed to use Open API as long as they obtain consumer approval but do not further regulate data standards in the use of Open API.
Bank Indonesia Regulation Number 23/11/PBI/2021 concerning Payment System National Standards	Only set the standard provisions in QRIS (QR Code National Payment Standards).
Bank Indonesia Regulation Number 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection	Operators are required to maintain the confidentiality and security of consumer data, including when working with other parties, and are prohibited from providing consumer data to other parties without the consumer's consent.
Financial Services Authority Regulation Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector	Financial services business actors are prohibited from providing data about their consumers to third parties. However, this prohibition is excluded when the consumer gives written consent and required by laws and regulations.
Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks	confidentiality of customer data, among others, in accordance with the provisions of the legislation regarding bank secrecy in the law concerning banking, the Law concerning Islamic banking, and the Financial Services Authority Regulation concerning consumer protection in the financial services sector.
Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector	Same as Financial Services Authority Regulation in Commercial Banks.
Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks	Banks are allowed to use Open API as long as they obtain consumer approval but do not further regulate data standards in using Open API.
OJK Regulation No. 21 of 2023 on Digital Services by Commercial Banks	This regulation does not explicitly specify the types of customer data that can be shared with Third-Party Providers (TPPs). Instead, the regulation emphasizes that collaboration between banks and partners, including TPPs, should be based on agreements outlining the rights and obligations of each party. This approach provides flexibility for banks and partners to determine the scope of data sharing while adhering to data protection and information security principles.

Source: Analysed from the primary source

standards in user protection were enacted. This simply means that the existence and availability of standard data are important.

Considering the void of data standards in Indonesian Open API, it becomes necessary to pay special attention to regulators in order to promote discussions or dialogues on market players. Data standardization in the Open API should be a priority during adoption because lack of standardization can lead to an imbalance between one market player and another, thereby resulting in possible failure.[57]

4. Consumer Protection Obligations and Liability

Boms and Taussig stated that consumer protection obligations and liability are challenging issues that can be resolved in various jurisdictions in the open banking ecosystem.[58] These issues arise from the main accompanying risks such as personal data breaches, unauthorized, and defective payments.[59] Given these risks, it is inevitable that consumer-centered security standards are needed to provide protection as the key success of open banking initiatives.[60] Further assessment of the responsibility of whether only the bank or together with third parties should be responsible in the open banking ecosystem is beyond the scope of this research. However, it is perceived as an important element in Indonesia. This is because, in the open banking ecosystem, banks are not the only parties that process consumer data. To a certain extent, the regime addresses the issue by stating that when there is a system error or unauthorized transaction, then

57 Ron Babin and Donna Smith, "Open Banking and Regulation: Please Advise the Government," *Journal of Information Technology Teaching Cases*, 2022, 204.

58 Steven Boms and Sam Taussig, "Customer Protection and the Liability Conundrum in an Open Finance Ecosystem," in *Open Banking* (Oxford University Press, 2022), 55–74.

59 The Institute of International Finance, "Liability and Consumer Protection in Open Banking," 2018, https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf.

60 Tania Ziegler, "Implementation of Open Banking Protocols Around the World," in *The Palgrave Handbook of Technological Finance* (Cham: Springer International Publishing, 2021), 751–79.

the responsibility is borne by the bank (liability based on fault) based on Article 8 POJK (Issuance of Financial Services Authority Regulations) No. 15/22 in conjunction with Article 19 Consumer Protection Act in conjunction with Article 21 ITE Act. It essentially states that they are required to provide compensation, and replacement when the goods or services received or used are not in accordance with the agreement reached.[61] The Bank as a business actor is also responsible for providing compensation for any damages, pollution or consumer losses due to goods or services produced or traded. But in the era of open banking, data is also processed by TPP, and it is feared that banks are free to make unfair demands at the expense of TPP or in other words, engage in discriminatory practices.[62] Further research on this aspect is recommended by analyzing its practices in other countries such as sharing liability.

In the European Union's Payment Services Directive 2 (PSD2), Articles 95 and 100 enforce strict regulations and significant penalties to ensure the security of consumer data in open banking ecosystems. Article 95 mandates that payment service providers implement appropriate technical and organizational measures to safeguard sensitive data, with potential sanctions for violations. Article 100 requires EU member states to establish effective, proportionate, and dissuasive administrative sanctions for providers that infringe data security or TPP access rules. Member states determine specific fines, which can reach millions of euros. PSD2 also aligns with the General Data Protection Regulation (GDPR), imposing penalties of up to €20 million or 4% of global annual revenue for data breaches under GDPR's provisions.

Similarly, Australia's Consumer Data Right (CDR) enforces privacy and data security requirements, imposing severe sanctions under Part 56BU of the Competition and Consumer Act 2010. Viola-

61 Ridwan Arifin et al., "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia," *Jambura Law Review* 3 (April 30, 2021): 135–60.

62 Oscar Borgogno and Giuseppe Colangelo, "Data Sharing and Interoperability: Fostering Innovation and Competition through APIs," *Computer Law & Security Review* 35, no. 5 (2019): 105314.

tions can result in fines of up to $2.5 million AUD for individuals or higher for legal entities. For breaches affecting many consumers, the maximum penalty is $50 million AUD or 30% of annual turnover, whichever is greater. Both PSD2 and CDR demonstrate the importance of robust data protection regulations and substantial penalties for non-compliance in open banking ecosystems. [63]

OJK Regulation No. 21 of 2023 on Digital Services by Commercial Banks outlines bank responsibilities regarding customer data protection with a focus on security. Key responsibilities include:

a) Safeguarding data confidentiality from unauthorized access or usage, ensuring data encryption, authentication, and leak prevention per national laws, including the Personal Data Protection Act (UU PDP).
b) In TPP partnerships, banks must establish clear responsibility divisions in agreements and monitor TPP adherence to agreed-upon security standards.
c) Risk and Liability for Data Breaches: Banks must promptly report breaches to OJK and affected customers, coordinate with relevant parties for mitigation, and ensure liability coverage for financial losses due to cyber incidents

It seems that Indonesia currently lacks a comprehensive legal framework governing sanction for data breaches within the context of open banking.

In EU, A crucial aspect of the PSD2 framework is that these TPPs cannot operate without prior authorization or registration from the national competent authority (NCA) in their home Member State. This licensing regime ensures that only entities meeting specific prudential and operational requirements, including security measures and professional indemnity insurance, are permitted to offer these services and exercise the access rights granted under PSD2. The mandate for ASPSPs to provide access is thus not an open door to any third party, but is specifically tied to these defined and regu-

63 Consumer Data Right, "Compliance and Enforcement Policy," 2023, https://www.cdr.gov.au/resources/guides/compliance-and-enforcement-policy.

lated TPP roles, ensuring that only authorized and supervised entities performing specific, recognized functions can claim these access rights.

E. Conclusion

In response to the rise of open banking and the shift towards data sharing, Indonesian legislators and regulators must focus on building a regulatory system that reflects the benefits of this new paradigm. Aligning with the second and third visions of the BSPI 2025, policymakers should adopt a regulatory-driven approach to ensure that policies promote a dynamic, competitive, and consumer-focused financial ecosystem. Key considerations for such a framework include implementing mandatory requirements for banks to share data with accredited Third-Party Payment Service Providers (TPPs), establishing an accreditation body to manage TPP participation in the open banking ecosystem, and ensuring strict liability sanctions for data breaches by both banks and TPPs. To achieve these goals and move away from the bank-centric model outlined in POJK No. 21 of 2023 on Digital Services, Indonesia must prioritize standardization and align policies with the BSPI 2025 objectives.

Bibliography

Almehrej, Abdulaziz, Leo Freitas, and Paolo Modesti. "Account and Transaction Protocol of the Open Banking Standard." In *Rigorous State-Based Methods*, 230–36, 2020. https://doi.org/10.1007/978-3-030-48077-6_16.

Amalia, Camila. "Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment." *Journal of Central Banking Law and Institutions* 1, no. 2 (May 31, 2022). https://doi.org/10.21098/jcli.v1i2.19.

Anugerah, Dian Purnama, and Masitoh Indriani. "Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective)." *Sriwijaya Law Review* 2, no. 1 (January 31, 2018): 82. https://doi.org/10.28946/slrev.Vol2.Iss1.112.pp82-92.

Arifin, Ridwan, Juan Anthonio Kambuno, Waspiah Waspiah, and Dian Latifiani. "Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia." *Jambura Law Review* 3 (April 30, 2021): 135–60. https://doi.org/10.33756/jlr.v3i0.9635.

ASPI, and BI. "Standar Nasional Open API Pembayaran," 2021. https://www.bi.go.id/id/layanan/Standar/SNAP/default.aspx.

Babin, Ron, and Donna Smith. "Open Banking and Regulation: Please Advise the Government." *Journal of Information Technology Teaching Cases*, 2022, 204. https://doi.org/10.1177/20438869221082316.

Babina, Tania, Greg Buchak, and Will Gornall. "Customer Data Access and Fintech Entry: Early Evidence from Open Banking." *SSRN Electronic Journal*, 2022, 1–74. https://doi.org/10.2139/ssrn.4071214.

Bajrektarevic, Anis H., Umi Khaerah Pati, Mellisa Towadi, and Anugrah Muhtarom Pratama. "Costumer Explicit Consent Under Indonesian Open Banking Regulations." *Jambura Law Review* 4, no. 2 (July 30, 2022): 176–94. https://doi.org/10.33756/jlr.v4i2.15377.

Bank for International Settlements. "Report on Open Banking and Application Programming Interfaces (APIs)." Switzerland, 2019. https://www.bis.org/bcbs/publ/d486.htm.

Bank Indonesia. "Blueprint Sistem Pembayaran Indonesia 2025," 2020. https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx.

Billiam, Billiam, Lastuti Abubakar, and Tri Handayani. "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 9, no. 1 (2022): 67–88. https://doi.org/10.22304/pjih.v9n1.a4.

Boms, Steven, and Sam Taussig. "Customer Protection and the Liability Conundrum in an Open Finance Ecosystem." In *Open*

Banking, 55–74. Oxford University Press, 2022. https://doi.org/10.1093/oso/9780197582879.003.0004.

Borgogno, Oscar, and Giuseppe Colangelo. "Data, Innovation and Competition in Finance: The Case of the Access to Account Rule." *European Business Law Review* 31, no. 4 (2020): 573–610. https://doi.org/10.54648/EULR2020023.

———. "Data Sharing and Interoperability: Fostering Innovation and Competition through APIs." *Computer Law & Security Review* 35, no. 5 (2019): 105314. https://doi.org/10.1016/j.clsr.2019.03.008.

Brener, Alan. "Payment Service Directive II and Its Implications." In *Disrupting Finance*, 103–19. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-02330-0_7.

Buckley, Ross P., Natalia Jevglevskaja, and Scott Farrell. "Australia's Data-Sharing Regime: Six Lessons for Europe." *King's Law Journal 33*, no. 1 (2022): 1–31. https://doi.org/10.1080/09615768.2022.2034582.

Chan, Rebecca, Indrit Troshani, Sally Rao Hill, and Arvid Hoffmann. "Towards an Understanding of Consumers' FinTech Adoption: The Case of Open Banking." *International Journal of Bank Marketing* 40, no. 4 (2022): 886–917. https://doi.org/10.1108/IJBM-08-2021-0397.

Colangelo, Giuseppe, and Oscar Borgogno. "Shaping Interoperability for the Internet of Things: The Case for Ecosystem-Tailored Standardisation." *European Journal of Risk Regulation* 15, no. 1 (March 1, 2024): 137–52. https://doi.org/10.1017/err.2023.8.

Consumer Data Right. "Compliance and Enforcement Policy," 2023. https://www.cdr.gov.au/resources/guides/compliance-and-enforcement-policy.

Diasti, Annisa Rahma. "Regulating Data Exclusivity of Ride-Hailing Service in Indonesian Competition Law." *Indonesia Law Review* 11, no. 3 (2021): 285–302. https://doi.org/https://doi.org/10.15742/ilrev.v11n3.4.

European Banking Authority. "EBA Industry Working Group on APIs under PSD2," 2021. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-

working-group-on-apis-under-psd2.

Fourie, Leila, and Thomas K. Bennett. "The Open Banking Era: Surfing the Australian Data Wave." In *Transformation Dynamics in FinTech: An Open Innovation Ecosystem Outlook*, 247–79, 2021. https://doi.org/10.1142/9789811239731_0009.

Gauci, Rachel. "Is Europe a Good Example of Open Banking?" In *The PayTech Book*, 86–87. Wiley, 2019. https://doi.org/10.1002/9781119551973.ch25.

Gomber, Peter, Robert J. Kauffman, Chris Parker, and Bruce W. Weber. "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services." *Journal of Management Information Systems* 35, no. 1 (2018): 220–65. https://doi.org/10.1080/07421222.2018.1440766.

Google, Temasek, and Bain & Company. "E-Conomy SEA 2021—Roaring 20s: The SEA Digital Decade," 2021. https://seads.adb.org/report/e-conomy-sea-2021-roaring-20s-sea-digital-decade.

Gurrea-Martṭnez, Aurelio. "Disruptive Technologies and Digital Transformation of the Financial Services Industry in Singapore: Regulatory Framework and Challenges Ahead." *SMU Centre for AI & Data Governance Research Paper No. 11*, 2020. https://doi.org/10.2139/ssrn.3741759.

Hermawan, Sapto, Zenia Aziz Khoirunisa, and Kukuh Tejomurti. "Triangular Insight on Open Banking in Indonesia, Singapore, and Australia." *International Journal of Legal Information* 51, no. 3 (November 25, 2023): 197–215. https://doi.org/10.1017/jli.2024.11.

Jeng, Linda. *Open Banking*. Oxford: Oxford University Press, 2022.

Leong, Emma. "Open Banking: The Changing Nature of Regulating Banking Data-A Case Study of Australia And Singapore," 2020. https://ssrn.com/abstract=3678458.

Liu, Han-Wei. "Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment." *Washington International Law Journal* 30, no. 1 (2020): 28–62. https://digitalcommons.law.uw.edu/wilj/vol30/iss1/5.

Lynn, Theo, Pierangelo Rosati, and Mark Cummins. "Exploring Open Banking and Banking-as-a-Platform: Opportunities and Risks for Emerging Markets." In *Entrepreneurial Finance in Emerging Markets*, 319–34. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-46220-8_20.

Mansfield-Devine, Steve. "Open Banking: Opportunity and Danger." *Computer Fraud & Security* 2016, no. 10 (2016): 8–13. https://doi.org/10.1016/S1361-3723(16)30080-X.

OBIE. "Open Banking: Guidelines for Open Data Participants," 2018. https://www.openbanking.org.uk/document/guidelines-for-open-data-participants/.

Office of the Australian Information Commissioner. "Consumer Data Right Legislation," 2020. https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-legislation.

OJK. "Roadmap Pengembangan Perbankan Indonesia 2020 – 2025," 2020. https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/-Roadmap-Pengembangan-Perbankan-Indonesia-2020---2025.aspx.

Open Banking is the Implementation Entitiy. "About the OBIE," 2022. https://www.openbanking.org.uk/about-us/.

Parks, Andrew M. "Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers." *Michigan Law Review* 20, no. 5 (2022): 914–45. https://doi.org/https://doi.org/10.36644/mlr.120.5.unfair.

Premchand, Anshu, and Anurag Choudhry. "Open Banking & APIs for Transformation in Banking." In *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 25–29. IEEE, 2018. https://doi.org/10.1109/IC3IoT.2018.8668107.

Qiu, Yuanbo. "The Openness of Open Application Programming Interfaces." *Information, Communication & Society* 20, no. 11 (November 2, 2017): 1720–36. https://doi.org/10.1080/1369118X.2016.1254268.

Remolina, Nydia. "Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World."

SMU Centre for AI & Data Governance Research Paper No. 2019/05, 2019. https://doi.org/10.2139/ssrn.3475019.

Ria Setyawati, Stefan Koos, and Zalfa A.F. Jatmiko. "Data Driven Dominance in Digital Markets: Assessing Indonesian Competition Law in the Digital Age." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 2 (August 28, 2024): 264–84. https://doi.org/10.29303/ius.v12i2.1377.

Sobel, Benjamin L.W. "A New Common Law of Web Scraping." *Lewis & Clarck Law Review* 25, no. 1 (2021): 149–206. https://law.lclark.edu/live/files/31605-7-sobel-article-251pdf.

Sugarda, Paripurna P, and Muhammad Rifky Wicaksono. "Enhancing The Competitiveness Of Indonesia's Financial Services Sector in the Digital Era Through Open Banking: Lessons Learned From The Uk's Experience." *Journal of Central Banking Law and Institutions* 2, no. 1 (2023): 153–78. https://doi.org/10.21098/jcli.v2i1.63.

Sullivan, Clare. "The New Australian Consumer Data Right: An Exemplary Model for Open Banking." *WIREs Forensic Science*, March 15, 2022. https://doi.org/10.1002/wfs2.1458.

The Institute of International Finance. "Liability and Consumer Protection in Open Banking," 2018. https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf.

Wiwoho, Jamal, Umi Khaerah Pati, and Anugrah Muhtarom Pratama. "Enabling Data Portability and Interoperability Under Indonesia's Data Protection Law." *Masalah-Masalah Hukum* 53, no. 3 (December 30, 2024): 271–82. https://doi.org/10.14710/mmh.53.3.2024.271-282.

———. "Reciprocal Data Portability to Foster Financial Services Competition in the Open Banking System Era." *Yustisia Jurnal Hukum* 13, no. 2 (August 27, 2024): 134. https://doi.org/10.20961/yustisia.v13i2.75786.

Zachariadis, Markos, and Pinar Ozcan. "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking." *SWIFT Institute Working Paper No. 2016-001*, 2017.

https://doi.org/10.2139/ssrn.2975199.

Zeller, Bruno, and Andrew M. 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/10.2139/ssrn.3766076.

Zeller, Bruno, and Brian Lynch. "Challenges in Open Banking - What Are the Practical Steps to Be Taken Now?" *University of Western Australia Law Review* 48, no. 2 (2021): 579–605.

Ziegler, Tania. "Implementation of Open Banking Protocols Around the World." In *The Palgrave Handbook of Technological Finance*, 751–79. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-65117-6_27.