Costumer Explicit Consent Under Indonesian Open Banking Regulations

Anis H. Bajrektarevic¹
Umi Khaerah Pati²
Melisa Towadi³
Anugrah Muhtarom Pratama⁴

¹ International Law and Global Political Studies, IMC University of Austria. Austria E-mail: anis@bajrektarevic.eu
² Faculty of Law, Universitas Sebelas Maret, Indonesia. E-mail: umi.khaerah@staff.uns.ac.id
³ Faculty of Law, Universitas Negeri Gorontalo, Indonesia. E-mail: mellisa.towadi@ung.ac.id
⁴ Faculty of Law, Universitas Sebelas Maret, Indonesia. E-mail: pratamanugrah23@gmail.com

Abstract

The implementation of GDPR and PSD2 in the EU as well as the PSD2 alignment with GDPR, encourage central banks in various countries including Indonesia to immediately implement an open banking system that also prioritizes privacy data protection. The PDP bill principle of explicit consent must be applied in open banking financial transactions that in Indonesia as stated in the National Standard Open API Payment (SNAP) 2021 (a Technical Standards and Governance Guideline). The purpose of this article is to describe the concept of explicit consent as it applies to the Indonesian open banking regulation (SNAP) and compare it to the concept of explicit consent as it's being regulated in the European Union PSD2 regulations as the world's originator of open banking and data privacy regulations. However, there are some fundamental differences regulated in PSD2 when compared to SNAP which will hinder Indonesia's data privacy regulation in the open banking era. The goal of this comparison is to see if SNAP and PSD2 have anything in common in terms of data privacy protection in order to strengthen data privacy rules in the banking sector in the open banking era. This research is normative research with statutory approach and comparative approach. The results showed that there are some fundamental differences between PSD2 and SNAP, including the parties involved, data portability and the concept of re-consent or re-confirmation which are not regulated in SNAP but regulated in PSD2, for the concept of sensitive data payment, neither SNAP nor PSD2 provide the specific concept, both define it broadly.

Article Info

Keywords:
Open Banking; Explicit consent; Data protection.

How to cite (APA Citation Style):
1. Introduction

In the era of business orchestration, Indonesia’s Personal Data Protection (PDP) bill has yet to be passed. Nevertheless, during PDP’s work, Bank Indonesia and other central banks in various countries are confronted with implementing open banking APIs initiated by the European Union through the PSD2 directive simultaneously released with the GDPR directive in 2018. These two rules developed from very different perspectives; while GDPR requires the protection of personal data, PSD2, on the other hand, requires opening up banking markets that have the impact of sharing bank customer data with third-party providers ("TPPs") (fintech, ride hailing platforms, e-commerce and other startup companies) to encourage competition and innovation. GDPR and PSD2 are built on the principle that individuals own their data and, therefore should be able to choose how their data is used and with whom their data is shared, in the sense that all actions on customer data are with the control and consent of the customer explicit consent. Under PSD2, TPPs shall access, process, and retain only the necessary personal data for the provision of their payment services and only with the "explicit consent" of the payment service user. Explicit consent is legal bases for processing special category data, respectively. However, Indonesia, which has the most prominent fintech and e-commerce market share in Southeast Asia, has been slow in adopting open banking.

In 2020, Bank Indonesia (BI), through the Blueprint for Indonesia Payment System 2025 (BSPI 2025, Blueprint for the Indonesian Payment System 2025) has just initiated its second and third vision to encourage the role of banks in developing open banking in the payment system through the formulation of the Open API Standard (BI

---

2020). Starting in 2021, BI, together with the Indonesian Payment System Association (ASPI, the Indonesian Payment System Association), introduced the National Standard Open API Payment (SNAP) (a Technical Standards and Governance Guideline) as an initiation and is in the process of being prepared. Along with the establishment of SNAP as an RTS, in the same month (August 2021) a Regulation of Members of the Board of Governors Number 23/15/PADG/2021 concerning National Standards for Open Application Programming Interfaces was issued. The two policies are implementing regulations from bank Indonesia regulation number 23/11/PBI/2021 concerning the National Standard of Payment System and first introduced the implementation of open banking APIs. Similar with GDPR and PSD2 EU, the application of SNAP must also take into account the principles in the PDP bill and the PDP bill should be considered adequate with the EU GDPR. The GDPR includes a set of rules for transfers of personal data to third countries or international organizations; such transfers are legal if there is a positive adequacy decision and appropriate safeguards in place (in contractual relations).

2. Problem Statement

This paper will review the concept of explicit consent applied in the PDP bill and GDPR as well as its implementation in PSD2 and SNAP which in the end will find some similarities and differences, especially in relation to the application of explicit consent. A comparison is essential for the advancement of knowledge for improve national regulations, As the legal discipline becomes more multicultural in an environment called ‘globalized’.

3. Methods

This paper is adopting a comparative and statutory research. According of Raymond Saleilles and others saw comparative law mainly as an instrument for improving

---

7 Indonesian Central Bank

http://ejurnal.ung.ac.id/index.php/jalrev/ JALREV 4 Issue 01 2022
domestic law and legal doctrine.\textsuperscript{11} Since Indonesian personal data regulation and BI SNAP still in the form of bill and a Technical Standards and Governance Guideline that will be implemented, the need to refer to external policy goals is greater.\textsuperscript{12}

4. Discussion

4.1. The Impetus Behind the Establishment of Open Banking in Indonesia

Since the European Union issued a data protection directive known as the General Data Protection Regulation (GDPR) in 2018, many countries have begun to refer to this regulation including Indonesia in drafting the Personal Data Protection Law.\textsuperscript{13} The directive applies strict regulations on how EU citizen data is processed either within EU countries or by other countries referred to in the GDPR as third countries.\textsuperscript{14} To be considered a third country, the country must have implemented a personal data protection equivalent to GDPR or at least an adequate one.\textsuperscript{15} The GDPR therefore applies an adequate level of protection to designate that a country is categorized as a "third country" whose indicators will be assessed by the European Commission.\textsuperscript{16} To date, there are still 12 countries around the world that are considered adequate and Japan is the only Asian country to have received an adequate assessment by the European commission and Korea is currently waiting for approval. In the ASEAN scope, Indonesia is lagging behind in the preparation of the PDP Law compared to neighboring countries such as Malaysia, Thailand, Singapore.\textsuperscript{17} The consequence if the state is not adequate, it will hinder trade relations between countries because it is hindered by the protection of personal data. Not only countries outside the European Union, the alignment of personal data protection is also a consideration for digital

\textsuperscript{11} Taekema, S. (2018). Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice. \textit{Law and Method}. \url{https://doi.org/10.5553/rem/000031}
\textsuperscript{12} Ibid.
\textsuperscript{17} Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. Jurnal Cakrawala Hukum, 10(2). \url{https://doi.org/10.26905/idjch.v10i2.3349}
giants such as Google, Amazon, Facebook, Apple and Microsoft which initially refused and ultimately also had no other option but to implement GDPR. At least two considerations underlie this step. First, the European Union is the main market for the digital giant, secondly, it will be very troublesome if global companies have to face different personal data protection standards in each country.\textsuperscript{18}

The alignment of the personal data protection law has a great impact on the business sector, especially in the banking sector. Along with the issuance of GDPR, the European Union also issued regulations related to open banking, namely the payment services directive (PSD2) in the same year (2018).\textsuperscript{19} Open banking is a system that provides users with network data of financial institutions through APIs (application programming interface).\textsuperscript{20} These applications, which convert content from various applications into an integrated experience can be created by developers who are not directly associated with the original developers of reuse services.\textsuperscript{21} Open banks use APIs to open consumer financial data (with their permission) to third parties, and allow companies to then create and distribute their own financial products.\textsuperscript{22} However, the implementation of open banking must comply with GDPR.\textsuperscript{23} The overall open banking framework approach can be grouped into two approaches, namely market-driven and regulatory-driven. For example, some of them—the EU, UK, and Australia—use regulatory-driven by laying out comprehensive regulations.\textsuperscript{24} Others—Singapore and Hong Kong—use market-driven by providing facilitation to market movements to self-regulate through the introduction of standard guidelines.\textsuperscript{25}

In global practice, there is no single framework approach in the adoption of open banking because it is regulated variably depending on the goals of each country.

However, it seems that Indonesia is leading in the implementation of regulatory driven as OJK (Indonesian financial services authority) has issued POJK 12/2018, specifically regulated by Article 15 paragraph (3) for the use of Open API by banks in payments. However, regarding the Open API standard, it is not regulated by the OJK because it is the authority of BI. Furthermore, OJK as an independent institution carrying out the task of regulating and supervising the banking industry and protecting banking consumers in 2020 released the Roadmap for Indonesia Banking Development 2020–2025 (RP2I 2020-2025, Roadmap for Indonesian Banking Development 2020–2025) recommended to further accelerate the adoption of open banking through regulations by looking at the legal function as social engineering as a digital transformation step in the banking sector. So that it can be indirectly understood that OJK hopes that BI will adopt it faster and in accordance with the plan set out in the BSPI by using a regulatory-driven approach. Responding to the POJK dan roadmap, Starting in 2021, BI, together with the Indonesian Payment System Association (ASPI, the Indonesian Payment System Association), introduced the National Standard Open API Payment (SNAP) (a Technical Standards and Governance Guideline) as an initial initiation and is in the process of being prepared. Along with the establishment of SNAP as an RTS, in the same month (August 2021) a Regulation of Members of the Board of Governors Number 23/15/PADG/2021 concerning National Standards for Open Application Programming Interfaces was issued. The two policies are implementing regulations from bank Indonesia regulation number 23/11/PBI/2021 concerning the National Standard of Payment System and first introduced the implementation of open banking APIs. Nonetheless, SNAP and PADG SNAP does not have the same enforcement authority as PSD2. In hindsight, how to adopt the PSD2 directive in EU countries is handed over to each country, for example in the Netherlands, directive PSD2 were inserted, amended and/or deleted several regulations in the including the Financial Supervision Act, the Financial Supervision Funding Act, Book 7 of the Civil Code and the Consumer Protection Enforcement Act. However, PADG SNAP may impose administrative sanctions on violators in the form

27 Indonesian Central Bank
of reprimands; temporary, partial, or complete cessation of activities including the implementation of cooperation; fines; to the revocation of the license as a Payment services provider (PJP).

Looking at the steps taken by BI and OJK, Indonesia will implement regulatory-driven which is also embraced by European union countries, In addition, the Market-driven approach is not suitable for achieving the target interests set by Bank Indonesia in encouraging the adoption of open banking in 2025 because the approach is voluntary, so by not being required this can hinder adoption, although regulators have taken various steps to promote and embrace banks to participate. Some countries that have already used this approach are UK, EU, Hongkong and Australia.

4.2. The Costumer Explicit Consent Framework for further Indonesian’s Open API standard

In an effort to adopt regulatory driven, Indonesian personal data protection bill will soon be passed, while the Open Banking regulations proceeds to be drafted. Under the GDPR and the UK data protection regime, “consent” and “explicit consent” are legal bases for processing personal data and special category data, respectively. The threshold for valid consent is high: consent must be freely given, specific, fully informed, unambiguous, and capable of being withdrawn. Furthermore, explicit consent is one of ten points in Article 9 bases which allow for the processing of special categories of personal data, such as payment data. The term explicit refers to the way in which the GDPR consent is expressed by the data subject and raises the standard of the consent where there is a serious data protection risk. As for PSD2, it provides that TPPs shall access, process, and retain only the personal data that is necessary for the provision of their payment services, and only with the “explicit consent.”

---

https://doi.org/10.2139/ssrn.3475019

http://ejournal.ung.ac.id/index.php/jalrev/ JALREV 4 Issue 01 2022
consent” of the payment service user. In Indonesia, regulations relating to explicit consent is stipulated in the PDP Bill those states processing of Personal Data in the PDP Bill must go through the valid consent of the Personal Data Owner for one or several specific purposes. Legal consequences if the Clauses of the agreement in which there is a request for Personal Data that does not contain explicit consent from the Personal Data Owner are declared null and void. Customer explicit consent in SNAP includes aspects of obtaining consent, revoking consent, and deleting or destroying consumer data. Explicit consent is required to process sensitive or specific data or commonly referred to as sensitive payment data. However, SNAP is not specifically regulated regarding sensitive payment data even though in PDP bills financial data is considered as specific data which in the Explanation of the article states that what is meant by “personal financial data” is to include but is not limited to data on the number of deposits in banks including savings; deposits; and credit card data.

The GDPR does not mention financial data as a special categorize of personal data in article 9 GDPR, but PSD2 article 4 point 32 provides a definition that ‘sensitive payment data’ means data, including personalized security credentials which can be used to carry out fraud. Neither the RTS nor the PSD2 define the meaning of “sensitive payment data”, leaving to the discretion of the banks the task of determining which data they consider sensitive. The broad definition of sensitive payment data has far-reaching implications for AISPs and PISPs whose business models rely entirely on access to and processing of inherently sensitive customer data. While PSD 2 specifies that the account holder’s name and account number are not sensitive payment data in relation to AISP and PISP activity, this falls short of clarifying the scope of sensitive payment data and the obligations of AISPs and PISPs that access and use a wide range of customer data.

SNAP does not provide a definition related to sensitive data payments, but requires each PJP (Payment Services Provider) of Service Users and PJP of service providers to

34 Article 8 PDP Bill
35 Article 20 PDP Bill
36 Article 3 letter h PDP Bill
apply the data standards set by SNAP. Data Standards Standard data rules for
describing and recording data, which may include, among other things,
characteristics, agreements on representation, format, definition, and structure.\(^{37}\) As
a result, it is necessary to simplify and standardize the data required for the Open
Banking API. This is critical in ensuring that common data is made available in a
consistent and uniform manner. In this data standard, it will provide the concept of
specifications and data characteristics (such as data general payment and sensitive
data payment) that need to be applied within the framework of explicit consent.
Regulation of Members of the Board of Governors Number 23/15/PADG/2021
concerning the National Standard for Open Application Programming Interface
Payments (hereafter called PADG SNAP) states that the categories of data standards
applied in the API include registration data; balance information; transaction history
information; credit transfer; debit transfers; and other categories set by Bank
Indonesia. PADG SNAP states that the application of standard data will be published
on the SNAP Developer Site. However, until now the SNAP Data Standard Concept has
not been available, while SNAP and SNAP PADG require the Implementation for those
involved in the preparation of SNAP, both Prospective Service Users and Prospective
Service Providers of the Indonesian Payment System Association (ASPI) no later than
June 30, 2022 and other Prospective Service Users and Prospective Service Providers
to implement SNAP no later than December 2022.

Moreover, there are differences between the parties determined by SNAP and PSD2
to be obliged to obtain explicit consent from consumers in processing their data. In
SNAP, the parties who are required to get explicit consent are service providers and
users of open api services. In PADG SNAP, Open API Payment Service Users are PJP or
parties other than PJP who use SNAP-based Open API Payment services while Open
API Payment Service Providers are PJP who provide SNAP-based Open API Payment
services. PJP can be in the form of a bank or non-bank. These two forms of business
have different implications for licensing mechanisms. In practice, some of the well-
known PJPs in Indonesia are OVO, GoPay, ShopeePay, and the like. OVO, GoPay and
Shoope are digital payment services recognized as Indonesia’s finance-tech business

content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf
unicorn, and Indonesia’s leading digital payment service that is not in the form of a bank. In SNAP, in addition to banks, several unicorn digital payment services are mandated to be pioneers for the initial implementation of open banking (first mover) which in total there are 16 PJP, namely Banks, digital payments and e-commerce. Banks include Mandiri, Bank BNI, Bank BRI, Bank BCA, Bank Nobu; Digital payments include Gopay, OVO, LinkAja, Dana, DOKU, Midtrans, SPOTS, Yokke, and e-commerce, including BukaLapak, Tokopedia and Shopee which will be required to implement open banking apis no later than June 30, 2022. SNAP itself does not mention which of the 16 services are service providers and/or users of open API services.

Unlike the case with PSD2 which is applied in the UK and EU. In PSD2, the parties that are required to receive explicit consent from the customer in processing data are PISP and AISP. PISP, a Payment Initiation Services Provider (PISP) is a company that offers an online service to initiate a payment order at the request of a payment service user for a payment account held by another payment service provider. While AISP stands for Account Information Service Provider, it is an online service that provides consolidated information on one or more payment accounts held by a payment service user with one or more payment service providers. AISPs, on the other hand, can only provide their services with the explicit consent of the payment service user. They may only access information from designated payment accounts and associated payment transactions; they may not request sensitive payment data linked to those payment accounts; and, in accordance with data protection rules, they may not use, access, or store any data for purposes other than performing the service explicitly requested by the payment service user.

AISP or PISP are not banks but parties other than banks that can process data obtained from banks or other financial institutions with customer explicit consent. AISP services and tools include price comparison, money management tools, faster and more accurate access to financial products, and speeding up manual processes.

39 Ibid.
such as applying for a mortgage, a loan, and so on, whereas PISPs are digital payment services that allow payments to be initiated directly from a customer’s bank account rather than using a credit or debit card.

Banks in PSD2 are referred to as ASPSPs. ASPSPs stands for Account Servicing Payment Service Providers provide and maintain a payment account for a payer as defined by the PSRs and, in the context of the Open Banking Ecosystem are entities that publish Read/Write APIs to permit, with customer consent, payments initiated by third party providers and/or make their customers’ account transaction data available to third party providers via their API end points. Under PSD2, PISPs and AISPs must obtain explicit consent, and the manner in which this consent is provided is between the account holder and the PISP/AISP. Because the ASPSP is not a party to this, it cannot impose restrictions on how explicit consent is given. An AISP is a company that has been granted permission to access an individual’s or SME’s account data from their financial institutions. The UK’s nine largest banks are required by law to comply with these AISP requests. However, AISPs, on the other hand, have ‘read-only’ access. They can view bank account information but not touch it, which means they cannot move a customer's money. Businesses that are authorized PISPs can not only view consumer-permission financial data on a bank account, but they can also make payments on the customer’s behalf. As a result, some industry observers have referred to PISPs as having "read-write" access.

Furthermore, the scope of SNAP consists of aspects of interconnection and interoperability, not yet covering data portability. This is also found in the PDP Bill which only covers interoperability mentioned in article 14 paragraphs 1 and 2 of the PDP Bill mentioning that

"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format"

but it has not mentioned

---

41 Britain might have left the EU at the end of 2020, but it’s still subject to a variety of European regulations in areas like financial services, data protection and technology. Payment Services Directive 2 (PSD2) is one of those.
“The right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided” as referring to the principle of portability in GDPR article 20 point 1.

This also affects the formation of SNAP which only includes the interoperability process, among other the ability to exchange and use information (typically in a large heterogeneous network made up of several local area networks) (Diallo et al. 2011). The right to data portability (RtDP) differ with interpretabilities. RtDP or Data portability, namely “the ability to move, copy or transfer” data, is one of the instruments of such control. (Graef, Husovec, and Purtova 2018). Data portability gives rights to customers the right to obtain and reuse their personal data for their own purposes across different services, to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure manner, without affecting its usability, and to use applications and services that can use this data to find them a better deal or to help them understand their spending habits. The right only applies to information provided by an individual to a controller.

The absence of data portability principles in the PDP Bill, was adopted by SNAP and resulted in consumer rights being regulated only to the extent of the ability of exchanging information or the ability of two cloud systems to talk to another, i.e. to exchange messages and information in a way that both can understand within the scope of snap, namely the ability to exchange information about consenting to data processing by the customer to the PJP of the service provider and the PJP of the service user and obtaining information related to the use of data, convey information related to accessing and changing data by customers to PJP service providers and PJP service users. Meanwhile, customers do not have the ability to move data from one party to another. The next difference is also regarding the consent period. In the PSD2, renew consent after 90 days (being revise on March 2022 in article 10A PSD2 that re-consent become re-confirmation) instead of a consumer having to provide their bank with credentials every 90 days (re-authentication), they only need to provide their AISP with reconfirmation that they consent to having their data

---


---
accessed. So that if the consumer does not reconfirm to continue the use of data by the PJP of the service provider and the PJP of the service user, then the PJP must delete the customer data. However, Re-new consent is not known in SNAP, SNAP only regulates the withdrawal or revocation of consent, as long as the consent data is not withdrawn or revoked, then the data can still be used by the PJP service provider and the PJP service user.

The following table summarizes the costumer explicit consent-related rules found in PSD2 in the Netherlands, GDPR in Europe Union, Indonesia’s PDP Bill and Indonesian BI SNAP.

<table>
<thead>
<tr>
<th>Aspects</th>
<th>EU GDPR</th>
<th>EU PSD2</th>
<th>Indonesian PDP Bill principles</th>
<th>BI SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles</td>
<td>GDPR principles</td>
<td>Principles that align GDPR</td>
<td></td>
<td>1. purpose limitation, specific manner, consent, accountability, confidentiality,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Lawfulness, fairness and transparency</td>
<td></td>
<td>uniquely,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Purpose limitation</td>
<td></td>
<td>2. purpose limitation, accuracy, completely, not misleadingly, up-to-date, and accountable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Data minimization</td>
<td></td>
<td>3. Integrity and confidentiality (security)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Accuracy</td>
<td></td>
<td>4. In the event of a failure in the protection of personal data (data breach), the personal data controller is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Storage limitation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Integrity and confidentiality (security)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Accountability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Article 6(1)(b) of the GDPR about customer consent and adopted in Article 94 (2) of the PSD2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Article 5 (1) (b) of the GDPR adopted in Article 94 (2) of the PSD2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. The collection of personal data is carried out in a limited and specific manner, legally valid, appropriate, and transparent, purpose limitation, accuracy, completely, not misleadingly, up-to-date, and accountable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabel 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

http://ejurnal.ung.ac.id/index.php/jalrev/
1. Obliged to notify the failure at the first opportunity to the owner of the personal data.

5. Right to erasure

| Parties that should obtain Explicit consent | Article 4, 6, 9 GDPR | - Explicit consent to the payment service provider's access to personal data; - Explicit consent to the payment order or transaction; - Explicit consent to access to the payment account for account information service providers. | Article 18-19 PDP Bill | - Explicit consent to the Provider's service access to customer personal data; - Explicit consent to PJP Service Users |

<table>
<thead>
<tr>
<th>withdraw consent</th>
<th>Article 7 GDPR</th>
<th>Article 64</th>
<th>Article 25 and 38</th>
<th>Stipulated in the SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Exception for explicit consent requirements</td>
<td>Article 9 GDPR</td>
<td>No</td>
<td>Article 21</td>
<td>No</td>
</tr>
</tbody>
</table>

<p>| Data right | Article 12-21 GDPR | fundamental rights, Portability, right to access, right to erasure ('right to be forgotten'), restriction, notification, portability, right to object, Automated individual | Article 4-15 PDP Bill | Right to Transparent information, communication and modalities, Access, rectification, right to erasure ('right to be forgotten'), restriction and so on. | Interoperability, right to access, right to erasure ('right to be forgotten'), restriction. |</p>
<table>
<thead>
<tr>
<th>Consent expires</th>
<th>No</th>
<th>Renew consent after 90 days (being revise on March 2022 in article 10A that re-consent become re-confirmation)</th>
<th>No</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data categorizes</td>
<td>(Article 9(1), GDPR.) Personal data and special categorize data</td>
<td>Article 4(32) of PSD2</td>
<td>Article 3, generic and specific data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Financial data (current accounts, credit cards, and some but not all savings accounts)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Sensitive payment data. Defining sensitive payment data states that “sensitive payment data means data, including personalized security credentials which can be used to carry out fraud.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parties</td>
<td>Controller, Processor and Data holder</td>
<td>PSU, PIISP, AISP, ASPSP, TPP</td>
<td>Controller, Processor and Data holder</td>
<td>Payment Open API Service Provider (Service Provider)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Open API Payment Service Users</td>
</tr>
</tbody>
</table>
Based on the table, it is very noticeable that Indonesia has not regulated some points that will later become the reference for the formation of comprehensive customer explicit consent in the era of open banking.

5. Conclusion

The concept of explicit consent regulated in SNAP and PADG SNAP is strongly influenced by the principles adopted in the PDP Bill which will be legalized in the near future, but when compared to the concept of explicit consent applied in the EU PSD2, there are some significant differences, including parties who are required to obtain customer explicit consent, in PSD2 banks are not included in the party, while in SNAP there are several banks that fall into the PJP category that are required to comply with SNAP and PADG SNAP although it is not clear whether banks are also required to obtain consent from customers before data processing, the absence of the concept of data portability and data re-consent in SNAP, all of which are regulated in PSD2. This should be a concern as it can be a hindrance to Indonesia's efforts in adequate terms with the EU GDPR.
References

Books


Journal Article


**Laws**

POJK 12/2018 concerning the Implementation of Digital Banking Services by Commercial Banks
Draft Law of the Republic of Indonesia concerning Personal Data Protection (PDP Bill)
Payment Services Directive Two (PSD2) EU
General Data Protection Regulation EU
Indonesian Personal Data Protection Bill (PDP Bill)
National Standard Open API Payment (SNAP) (Regulatory Technical Standard)
Regulation of Members of the Board of Governors Number 23/15/PADG/2021 concerning National Standards for Open Application Programming Interfaces
Bank Indonesia regulation number 23/11/PBI/2021 concerning the National Standard of Payment System
Roadmap for Indonesia Banking Development 2020–2025

**Official Web**
