Journal of Central Banking Law and Institutions, Vol. 1 No. 1, 2022, pp. 119 - 140
e-ISSN: 2809-9885
DOI: 10.21098/jcli.v1i1.2

THE PRINCIPLE OF *AMANAH* IN THE UTILISATION OF CONSUMERS' PERSONAL DATA AND INFORMATION IN OPEN BANKING

Trisadini Prasastinah Usanti
Faculty of Law, Universitas Airlangga, Indonesia
trisandini@fh.unair.ac.id

Submitted: 8 November 2021 - Last revised: 8 December 2021 - Accepted: 5 January 2022

Abstract

Banks are generally prohibited in any possible way from providing customers' data or information to third parties unless there is a written consent from the customer, or it is required by laws or regulations. Open banking allows banks to obtain customer financial data and information and forward them to third parties to accelerate a digital transformation in banking. The existence of the customer's consent resulted in the bank's legal action providing customer data and information to a third party is not considered as a violation to the principle of confidentiality. However, the provision of customer data by banks to third parties must be based on the fiduciary principle, prudential principle, and principle of *amanah,* since the misuse of customers' data can lead to administrative sanctions, criminal sanctions, and civil liability.

Keyword: *Amanah, Data, Consumer, Open Banking*

I. INTRODUCTION

Banking is one of the financial services businesses that plays a strategic role in supporting the implementation of national development in the context of increasing equity, economic growth, and national stability for the welfare of the people, as mandated by the Law No. 7 of 1992 on Banking as amended by Law No. 10 of 1998 (hereinafter referred to as the Banking Law). On the other hand, banks should also be encouraged to conduct an end-to-end digital transformation to be able to compete in the current digital era.

By 2025, one of the visions of the Indonesian payment system (*Sistem Pembayaran Indonesia*, SPI) is to support banking digitisation as the main institution in the digital financial economy through open banking and the use of digital technology and data. Open banking is one of the five initiatives of the 2025 SPI Blueprint, in addition to the Retail Payment Systems, Financial Market Infrastructure, Data Regulation, as well as Licensing and Supervision.

The five initiatives will be implemented by five working groups that will collaborate with relevant ministries and institutions as well as industries and will be realised in the span of 2019 to 2025.[1] The fulfillment of the four pillars of digital banking, namely channels for consumers (omni banking), agile architecture and infrastructure (modular banking), open interaction with third parties (open banking), and efficient use of data-based resources (smart banking). The four pillars are aimed at accelerating digital transformation in the banking sector. Open Banking is defined as an approach that allows banks to disclose their consumers' financial data and information to third parties (fintech). Open Banking will be realised through Open API standards which include technical standards, security standards, and governance standards. In particular, the focus of development will be directed at standardising the disclosure of payment data for use cases of MSME lending based on consumers' consent.[2]

According to Stranieri, et. al., the Open Banking model is a data-sharing model emerging in the financial services sector that involves technological and regulatory innovations designed to facilitate access to banking records by third-party providers such as payment service providers. The model is predicted to disrupt the financial services industry and encourage a wave of new third-party providers offering innovative services that will change the relationship between customers and banks. The open banking data sharing (OBDS) model includes technological and legal innovations emerging in the financial services sector where banks and other financial institutions commit to having real-time customer data accessible to third parties through application programming interfaces (API).[3] As stated by on Phil Laplante and Nir Kshetri:[4]

> Open banking (OB) is a term that describes a special kind of financial ecosystem. The ecosystem is governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations. The OB ecosystem provides more choices and information to consumers and allows easier interaction with and movement of money between financial institutions and any other entity choosing to participate in the financial ecosystem. OB also makes it easier for new entries into the financial business sector through the OB ecosystem.

---

[1] Bank Indonesia, *Bank Indonesia : Menavigasi Sistem Pembayaran Nasional Di Era Digital BANK INDONESIA* (Jakarta: Bank Indonesia, 2019), 4.

[2] *Ibid*., 24.

[3] Andrew Stranieri et al., "Open Banking and Electronic Health Records," in ACSW '21: 2021 Australasian Computer Science Week (Association for Computing Machinery, 2021), 1–4, 2. https://doi.org/https://doi.org/10.1145/3437378.3437397.

[4] Phil Laplante and Nir Kshetri, "Open Banking: Definition and Description," Computer 54, no. 10 (2021): 122–28, 122. https://doi.org/10.1109/MC.2021.3055909.

In general, one banking activity is to collect funds from the public in the form of deposits that are governed by a fund deposit agreement between the bank and the depositor of the fund (hereinafter referred to as the "Consumer").[5] Based on said agreement, a legal relationship arises between the bank and the Consumer based on the fiduciary principle, the prudential principle and the confidentiality principle. As the manifestation of the confidentiality principle, there exists a norm that requires banks to keep confidential information regarding consumers who deposit funds and their deposit records as mandated under Article 40 paragraph (1) of the Banking Law. This provision aims to maintain public trust, especially for customers who deposit funds, since the more trust given to the bank, the more customers will use a bank's services. However, the Banking Law adheres to the theory of bank secrecy which, in nature, is relative, thus it is possible for banks to disclose confidential information regarding their customers and their deposits if it is authorised by law.

Open banking allows banks to obtain consumer financial data and information and provide it to third parties. Exceptions to bank secrecy under the Banking Law do not include legal actions taken by banks in open banking. The limited exceptions set forth in the Banking Law are for taxation interests, settlement of bank receivables, judicial interest in criminal cases, civil cases between banks and their customers, exchanging written information between banks, upon request, approval or power of attorney from depositors specified outside the Banking Law, which is under the crime of money laundering as regulated under the Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, and under the Constitutional Court Decision No. 64/PUU-X/2012 in relation to the interests of the judiciary regarding joint assets in divorce cases. As such, the legal basis for banks in open banking should be equivalent in statutory form.

Marnia Rani emphasised that maintaining the principle of confidentiality of the financial information of Consumers is very important for banks in carrying out their business activities, because the existence of such confidentiality

[5] Based on Article 2 of the Financial Services Authority Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector, what is meant by consumers are parties who place their funds and/or take advantage of the services available at Financial Services Institutions, including customers in banking, investors in the Capital Market, policyholders in insurance, and participants in Pension Funds, based on the laws and regulations in the financial services sector. Likewise, in Bank Indonesia Regulation No. 22/20/PBI/2020 on Bank Indonesia Consumer Protection, what is meant by consumers are individuals or entities, whether in the form of legal entities or non-legal entities, who take advantage of products and/or services from providers. Meanwhile, the organiser is any party, either a bank or an institution other than a bank, which carries out activities regulated and supervised by Bank Indonesia whose products and/or services are utilised by consumers.

guarantees it will create a sense of "confidence" for Consumers who need a "non-disclosure" atmosphere for their financial information. From this sense of "confidence" a fiduciary relationship arises between the bank and its customers which will also have an impact on the development of the banking business.[6] It was also stated by Revanthy that:[7]

> Mainly in banking since the foundation of banking lies in trust, confidentiality, and credibility. It's an important role is to protect our sensitive and personal data. It also defends the entire network from the malicious use of customer assets. Nowadays especially during the Covid times, more people use cashless transactions so many fraudulent activities are done online. As a result, customer lose trust in banks and other financial institutions where cyber security deals and resolves to give solution this problem by protection their data.

Some examples of bank account opening in both Islamic and conventional banks, which embodied clauses that give approval or non-approval for banks to provide and or disseminate consumers' personal data, are as follows:

1. BTN Syariah: I AGREE / DISAGREE* to give the bank the right to provide and or disseminate my personal data to other parties outside the bank's legal entity for commercial purposes.
2. BNI: The bank can provide my data and information to third parties, which include subsidiaries and/or companies that cooperate with the bank in the context of offering products and services from each of these companies. At BNI, there is a column to be selected by consumers to agree or to disagree with the above provision.
3. BCA: Account Holder hereby gives approval to BCA to provide account holder's data to parties outside BCA, who cooperate with BCA, in the context of promotional activities or for other commercial purposes.
4. MayBank: "I hereby give an approval and atuthorisation to the Bank to use, disclose information, or check information to third parties for all data, information and information obtained by the Bank regarding myself including but not limited to personal data, transactions, collectability status, and my personal means of communication for all other purposes in

[6] Marnia Rani, "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank," Jurnal Selat 2, no. 1 (2014): 168–81, 168.

[7] P. Revathy and G. Belshia Jebamalar, "A Review Based on Secure Banking Application against Server Attacks," in Smart Intelligent Computing and Communication Technology, ed. V.D. Ambeth Kumar et al., vol. 38 (Amsterdam: IOS Press, 2021), 241–45, 241. https://doi.org/10.3233/APC210044.

accordance with the laws and regulations, including for the marketing of bank products or other parties who cooperate with the Bank."

These clauses are common in every bank account opening. If being tracked, such clauses are the manifestation of the Financial Services Authority (*Otoritas Jasa Keuangan*, or OJK) Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector (POJK 1/2013) and the Financial Services Authority Circular Letter No. 14/SEOJK.07/2014 on Data Confidentiality and Security and/or Consumer Information (SEOJK 14/2014). It is stated that a bank, as one of the Financial Services Business Actors (PUJK), is prohibited in any way from providing personal data and/or information regarding its Consumers to third parties. However, this prohibition is excluded if: the consumer gives written consent, and/or as required by laws or regulations. As a consequence, an issue has arisen as to whether the existence of such a clause can override the principle of confidentiality that must be adhered to by the bank and can eliminate the bank's responsibility for the misuse of consumer data and/or information by third parties; further, what are the principles underlying the relationship between a bank and its customers in an open banking, in addition to the fiduciary principle, prudential principle, and the principle of confidentiality?

II. THE PRINCIPLE OF CONFIDENTIALITY

A bank's obligation to maintain bank secrecy may arise from a contractual relationship and/or as prescribed by the law. The obligation of secrecy, which is called the duty of confidentiality, consists of two parts, namely:[8]

a) the obligation not to provide information about its Consumers to third parties, and
b) the obligation not to use confidential information obtained from its Consumers for its own interests. This is intended to avoid any conflict of interest for the bank.

Samahir Abdullah stated that regarding the obligation of banks to keep their Consumer information confidential before, during and after the end of the relationship between the bank and its Consumers, as follows:[9]

---

[8] Akhmad Yasin, "Keterkaitan Kerahasiaan Bank Dan Pajak: Antara Kepentingan Negara Dan Pribadi," Jurnal Konstitusi 16, no. 2 (2019): 212–34, 221. https://doi.org/10.31078/jk1621.

[9] Samahir Abdullah, "The Bank's Duty of Confidentiality, Disclosure Versus Credit Reference Agencies; Further Steps for Consumer Protection: 'Approval Model,'" *European Journal of Current Legal Issues* 19, no. 4 (2013), https://webjcli.org/index.php/webjcli/article/view/296/405.

> The bank's duty of confidentiality covers all customers' information about themselves, and their accounts held by the bank, irrespective of the information source and for as long as the banker-customer relationship exists. There are many logical reasons for obliging the banks to keep customers' confidential data private before, during, and after their relationship. First, information provided to the bank before the beginning of the contractual agreement is possibly the same information that is provided by the customer after that agreement has been initiated; consequently, such information falls under the duty of confidentiality. Secondly, information provided to the bank at any period during the banker-customer relationship does indeed fall under the bank's duty of confidentiality according to the common law definition of confidentiality. Thirdly, in practice, there is nothing to prevent banks from adhering to an explicit duty to the customer to inhibit the disclosure of specific information, even if such information theoretically is not within the ambit of the bank's duty of confidentiality. Fourthly, the customer's right to privacy must certainly be respected, and the most important aspect of a person's rights is the right to keep his/her information private. There is the further possibility that disclosure of any confidential information after the termination of the banker-customer relationship may cause loss or damage to the person.

Graham Greenleaf and Alan Tyree said that the disclosure of customer privacy data by banks is to prevent money laundering, which is quoted bellow:

> An examination of the relationship between the traditional duties of banks to their customers and data privacy laws is of increasing international relevance because of the growing ubiquity of data privacy laws. at the end of the 1980s the Vienna Convention required state parties to criminalise money laundering, and the Financial Action Task Force (FATF) started development of its '40 recommendations' including 'suspicion-based reporting' to a state authority, exemption of banks from any consequent breaches of bank–customer confidentiality and similar exemption of international requests for mutual assistance. The enactment by legislatures across the world of those recommendations, and subsequent recommendations concerning measures for reporting of 'suspicious transactions', counter-terrorist financing, anti-sanctions avoidance and anti-corruption have led to the global retreat of the banker's traditional duty of confidentiality in an increasingly wide and complex range of circumstances. … Banks everywhere will increasingly have to take into

> account data privacy laws, in addition to their traditional duties. The breadth of obligations imposed by these laws, while often in parallel with traditional duties, is generally of much broader scope, and will require new accommodations in banking practice, particularly for banks with multinational operations.[10]

In the Ukraine, the arrangement is similar to Indonesia in which banks must guarantee customers' privacy during transactions with private or third parties. Basysta stated:[11]

> Art. 61 of the Law of Ukraine on Banks and Banking Activity obliges Ukrainian banks to maintain banking secrecy. The same article provides mechanisms for maintaining banking secrecy, which at first seems appropriate. Banks should guarantee each client's data revealed to the bank during servicing transactions, including private or third parties' relationships, will not be disclosed and used to benefit bank employees. Thus, according to the Law, bank employees must sign a commitment to banking secrecy upon taking office. Moreover, contracts and agreements between the bank and the client must stipulate banking secrecy and accountability for its disclosure. Furthermore, banks must limit the number of persons who have access to confidential data, provide special record-keeping sensitive documents, and technically prevent unauthorised access to electronic and other media.

Furthermore, consider banking in Netherlands: De Nederlandsche Bank n.v. Bank Act 1998 Section 20:

> To the extent that this Act provides for the performance of the acts to achieve the objective referred to in section 2 (1), anyone who, by virtue of the application of this Act or provisions based on it, performs any duty, shall be prohibited from using or divulging data or information obtained in the performance of that duty in any way beyond or other than that required for the performance of that duty or required by this Act. However, such obligations may be excluded as provided for in Section 18: Our Minister

[10] Graham Greenleaf and Alan Tyree, "Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons," in Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres around the World, ed. Dora Neo and Sandra Booysen (Cambridge: Cambridge University Press, 2017), 31–61, 31-32, https://doi.org/DOI: 10.1017/9781316535219.003.

[11] Basysta Iryna, Shepitko Iryna, and Shutova Olga, "Protection and Risks of Illegal Divulgation of Banking Secrecy in Ukrainian Criminal Proceeding*," Access to Justice in Eastern Europe 4, no. 8 (2020): 298–305, 300, https://doi.org/10.33327/AJEE-18-3.4-n000042.

> is authorised, with due observance of Article 107 of the Treaty, to request the Bank to provide such data or information, in connection with the tasks and activities performed in order to achieve the objective referred to in section 2(1), as he deems necessary for the purpose of determining the Government's financial and economic policy.

Referring to the results of research conducted by Muhammad Saiful Rizal on the protection of personal data in Malaysia, it is mentioned that the Personal Data Protection Act 2010 has been in force since 2013, where this law expressly protects the right to privacy of its citizens. There is even a fine or a maximum prison sentence of five years or both if someone interferes with the privacy of others, as set forth in the Malaysian Criminal Code.[12]

Yunus Husein also stated that there are five reasons that underly a bank's obligation to maintain the confidentiality of all information regarding customers and their accounts, including:[13]

a. Personal privacy;
b. Rights arising from the engagement relationship between the bank and its consumer;
c. Applicable laws and regulations;
d. Practice or prevalence in the banking industry; and
e. Characteristics of bank activities as a "trusted institution" that must uphold the trust of consumers who keep their money in the bank.

In term of violations, even a bank as a financial services business, will be subject to criminal sanctions and administrative sanctions by the Financial Services Authority, in the form of:

a. Penalties;
b. Written warnings;
c. Decrease in the rating of bank soundness;
d. Prohibition from participating in clearance activities;
e. Suspension of certain business activities, both for certain branch offices and/or for the bank as a whole;
f. Dismissal of bank management; and
g. Inclusion of management members, bank employees, shareholders in the list of questionable personnel in the banking sector.

---

[12] Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malaysia," Jurnal Cakrawala Hukum 10, no. 2 (2019): 218–27, 223, https://doi.org/10.26905/idjch.v10i2.3349.

[13] Dinda Anna Zatika, "Pembukaan Prinsip Kerahasiaan Bank Sebagai Perbuatan Melawan Hukum (Studi Kasus Bank BCA)," Sasi 26, no. 4 (2020): 500–513, 503, https://doi.org/10.47268/sasi.v26i4.238.

From a civil perspective, the violators can be sued individually for compensation based on civil wrongdoing due to violations of Article 40 of the Banking Law. Article 1365 of the Indonesian Civil Code (BW) states that every unlawful act or civil wrongdoing that causes harm to another person, obliges the person who committed the unlawful act to compensate the victim for the losses. Based on the formulation mentioned above, according to Sedyo Prayogo, it can be interpreted that an unlawful act is an act that violates another people's rights, or an act (or omission of a duty to act) that contradicts with one's obligation(s) under the law or unwritten law that shall be carried out as member of the society, subject to any legal justification.[14] In this case, where a bank violates the law by disclosing customers' confidential information and causes harm to the customers.

Under the existing statutes, namely Article 26 of Law No. 19 of 2016 on the Amendments to Law No. 11 of 2008 on Information and Electronic Transactions, unless otherwise specified by the laws and regulations, the use of any information through electronic media involving a person's data must be done with the consent of the person concerned, and where his rights are violated, he can file a lawsuit for the damages. Based on the Minister of Communication and Information Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems, personal data is "certain individual data that is stored, maintained, and maintained and protected confidentially." Personal data must be protected in electronic systems that include protection against the acquisition, collection, processing, analysis, storage, disclosure, delivery, dissemination, or destruction of personal data. However, personal data may be disclosed when the owner of the personal data expressly consents to such us, in writing provided by the electronic system operator or determined otherwise by following the provisions of the laws and regulations.

One of the visions of SPI 2025 is to support banking digitalisation as well as digital technology and data in the financial services industry.[15] In addition, four pillars are required in digital banking, channels for consumers, agile architecture and infrastructure, open interaction with third parties (open banking) and efficient use of data-based resources (smart banking), and efficient use of data-based resources (smart banking). These four pillars aim to encourage digital transformation in the banking sector.[16] However, there are other concerns about Open Banking based on Open API, namely Privacy and

[14] Sedyo Prayogo, "Penerapan Batas-Batas Wanprestasi Dan Perbuatan Melawan Hukum Dalam Perjanjian," Jurnal Pembaharuan Hukum 3, no. 2 (2016): 280–87, 282, https://doi.org/10.26532/jph.v3i2.1453.

[15] Bank Indonesia, Bank Indonesia : Menavigasi Sistem Pembayaran Nasional Di Era Digital BANK INDONESIA, 23.

[16] *Ibid.*, 24.

Data Protection, as stated by Masculine Muhammad Muqorobin.[17] This relates to the way banks maintain their security, consent and contracts, specific use-cases, and time restrictions. With Open API, data that has been submitted by consumers to a bank must be managed securely so that after the data is used by the bank, it is immediately returned to the original data storage location. Open Banking Standardisation based on Open API also must be performed on data, technical, security, and maintenance.[18] Similarly, Anna Eugenia Omarini also stated regarding open banking, that,[19] "[n]ow banks are mandated to be able to provide access and to communicate, to authorized third parties, customers, and payment account information. Within this framework, banks set up open interfaces, namely APIs, to ensure they are fully compliant."

The research conducted by Cortet, Rijks, & Nijland is also relevant, as they identified four different strategies that specifically address Open Banking models that a bank may pursue in a Payment Service Directive PSD2 context, including:[20]

a. Comply. The bank opens information only to the extent it is mandated to do so. Here, there is a strong reconsideration of the value proposition. Traditional revenue streams that were deemed as certain are impacted, third-party interfaces disintermediate the bank. Banks retain their role as an account services provider and backbone of the system.
b. Compete. Banks react and, aside from compliance, they try to fight for customer proximity through their own interfaces, with the implication of rethinking the overall model in terms of value proposition, processes, costs, revenues, and channels.
c. Expand. This strategy goes beyond exposing basic account information. Banks can expose Open APIs and pursue new revenue streams, especially by providing full account information and specific services, such as data management and identity verification, to third parties. Banks become the gateway through which third parties can access data and other services.
d. Transform. This is a specific subset of Open Banking, where a platform strategy can be implemented. Banks specifically offer a core around which other players can build their offering, in addition to connecting users across different groups, facilitating matchmaking. With this model, there

[17] Masculine Muhammad Muqorobin et al., "Pengaruh Open Banking Berbasis Open API Terhadap Eksistensi Perbankan," MAKSIMUM 11, no. 2 (2021): 75–84, 81, https://jurnal.unimus.ac.id/index.php/MAX/article/view/7877.

[18] *Ibid.*

[19] Anna Eugenia Omarini, "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future," International Business Research 11, no. 9 (2018): 23–36, 28, https://doi.org/10.5539/ibr.v11n9p23.

[20] *Ibid.*, 29.

> is a radical re-thinking of the business model. Banks indeed also try to monetise APIs as well as competing and profiting from an enhanced value proposition to customers, fulfilling shifting market needs.

Open Banking will come equipped with risk control mechanisms related to data protection, security, system operation, and transaction integrity. Open access to data will be based on the consumers' consent mechanism. Disclosure of consumer data by banks does not violate the article on confidentiality of consumer data if it is initiated by a consumer who owns the data and information.[21] In the digital era, data is the most valuable asset as well as the key to competitiveness. On the other hand, it also increases the risks and requires more attention, mainly to avoid the misuse of consumer's data.[22] This concern was also conveyed by Shahrazad Hadad that in fact, concerns about security, confidentiality, trust, and the risks involved are highlighted in all studies of Internet banking and cited as the most significant barriers to developing the online banking market.[23]

Open banking regulations can be found in Bank Indonesia Regulation No. 22/23/PBI/2020 on Payment Systems. In addition, Open banking is one of the initiatives of the Indonesia Payment System Blueprint 2025: This initiative will be achieved through an open API standardisation. The scope of standardisation will include data, technical aspects of API, security, and governance including contractual standards. This step enables the disclosure of financial information and interlinks between banks and fintech.

III. THE PRINCIPLE OF *PACTA SUNT SERVANDA*

The disclosure of consumer's data by the bank does not violate the data confidentiality provision if the consumer has given written consent to the bank as usually set forth in the opening of a bank account. For example, the clause in MayBank disclosure statement reads:

> I hereby give approval and authorisation to the Bank to use, disclose information, or check information to third parties for all data, information and information obtained by the Bank regarding me including but not

[21] Bank Indonesia, Bank Indonesia : Menavigasi Sistem Pembayaran Nasional Di Era Digital BANK INDONESIA, 28.

[22] *Ibid.*

[23] Shahrazad Hadad, "Challenges for Banking Services in the Knowledge Economy," Management Dynamics in the Knowledge Economy 7, no. 3 (2019): 337–52, 347, https://doi.org/10.25019/mdke/7.3.04.

limited to personal data, transactions, collectability status, and means my personal communication for all other purposes in accordance with the laws and regulations, including for marketing bank products and other parties who cooperate with banks.

However, the data included in that statement does not include information on consumers and their deposits because they are within the scope of bank secrecy laws that must be strictly adhered to by banks unless otherwise stipulated by law.

Consumers' personal data and/or information that can be provided to third parties by banks with their consent based on SEOJK No.14/2014 refers to data or information which includes the following:

a. For Individuals, including: name; address; date of birth and/or age; phone number; and/or the name of the birth mother.
b. For Corporations, including: name; address; phone number; composition of the board of directors and commissioners including identity documents in the form of ID/Passport/residence permit; and/or composition of shareholders.

The consent given by the consumer to the bank to provide data and/or information to third parties results in the consumer being bound by the disclosure statement. The clause in the account opening documentation that has been consented-to by the consumer will bind the parties as well. This is the embodiment of the principle of *pacta sunt servanda* in Article 1338 paragraphs (1) and (2) BW which states that, "[a]ll agreements made legally valid as law for those who make them. The agreement cannot be withdrawn other than by agreement of both parties, or for reasons determined by law."

According to Yunanto, "binding as a law" has the meaning that a valid agreement has the same legal position as the law. Hence, if a contracting party is harmed by the other party to the agreement, then it may seek legal recourse. For example, the aggrieved party can file a lawsuit against the other party; this is the power of a legally enforceable agreement.[24] It is also stated by Hernoko that parties who entered into the contract can independently construct their relationship according to their agreement. The parties' power to legally bind one another through a contract, has the same legal effect as the ones made by the legislature, which means the Constitution acknowledges and puts all parties who enter into a contract to be on the same level as the legislature. This binding power arose from the principle of freedom of contract which

[24] Yunanto Yunanto, "Hakikat Asas Pacta Sunt Servanda Dalam Sengketa Yang Dilandasi Perjanjian," Law, Development and Justice Review 2, no. 1 (2019): 33–49, 42, https://doi.org/10.14710/ldjr.v2i1.5000.

reflected the value of the trust.[25] As such, with the consent of the consumer provided to the bank to disclose personal data and/or information to third parties, it can be equated as a binding on both banks and consumers.

Pacta sunt servanda is a Latin term which means that promises must be kept, such is a principle in the civil law legal system. This principle relates to agreements between individuals that:[26]

a. Agreement is a law for the parties who make it; and
b. Denying the obligations contained in the agreement is a breach of promise or default.

Applying said principle to the context of the bank and its customers, because of this approval, the bank is responsible for any losses incurred by consumers due to misuse of their data either by the bank or by any third party. Therefore, banks should be extra careful in protecting consumer data and/or personal information that has been entrusted to the bank.

According to Rosadi and Pratama, data can be deemed as a personal data if the data relates to a person and can be used to identify that person, namely the owner of the data. For instance, a telephone number on a piece of paper is data. It is different if on the piece of paper, a telephone number, and the name of the owner of the phone number are written, then the data is personal data. The phone number on a blank piece of paper is not personal data because the data cannot be used to identify the owner, while the data on the telephone number and the name of the owner can be used to identify the owner of the data, therefore it can be referred to as personal data.[27] In the context of personal data protection, the terms that are often used are "personal information" and "personal data." The term used in the United States is personal information (personally identifiable information), whereas the term used in Europe is 'personal data.' Currently in Indonesia, the terminology used is 'personal data,' as referred to under the Law on Information and Electronic Transactions.[28]

OJK Circular Letter (SEOJK) No.14/2014 has laid out several guidelines for banks regarding protecting consumer data and or personal information, namely:

---

[25] Agus Yudha Hernoko, Hukum Perjanjian: Asas Proporsionalitas Dalam Kontrak Komersial (Yogyakarta: Laksbang Mediatama, 2008), 110-112.

[26] Harry Purwanto, "Keberadaan Asas Pacta Sunt Servanda Dalam Perjanjian Internasional," Mimbar Hukum 21, no. 1 (2009): 155–70, 162, https://doi.org/10.22146/jmh.16252.

[27] Sinta Dewi Rosadi and Garry Gumelar Pratama, "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia," Veritas et Justitia 4, no. 1 (2018): 88–110, 94, https://doi.org/10.25123/vej.2916.

[28] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," Business Economic, Communication, and Social Sciences (BECOSS) Journal 1, no. 1 (2019): 147–54, 150, https://doi.org/10.21512/becossjournal.v1i1.6030.

1. If the consumer gives written consent, the bank can provide Consumer Personal Data and/or Information with the obligation to ensure that the third party does not provide and/or use Consumer Personal Data and/or Information for purposes other than those agreed between the bank and the third party.
2. The procedure to obtain a Consumer's written approval can be stated in the form of:
   a. Choice to agree or disagree; or
   b. Providing a sign of approval

   in documentation and/or product and/or service agreements.
3. If a bank obtains personal data and/or information of a person and/or group of people from another party and the bank will use such data and/or information to carry out its activities, the bank is required to have a written statement that the other party has obtained written approval from that person and/or a group of people to provide the said personal data and/or information to any party including banks.
4. Banks are required to establish written policies and procedures regarding the use of Consumer Personal Data and/or Information which at least contains:
   a. Written and/or oral explanation to the Consumer regarding the objectives and consequences of granting written consent and providing and/or disseminating Consumer Personal Data and/or Information.
   b. Request for written approval from the Consumer if the bank is to provide and/or disseminate Consumer Personal Data and/or Information to third parties for any purpose unless otherwise stipulated in the applicable laws and regulations.
5. Written policies and procedures must be stated in standard operating procedures regarding the use of Consumer Personal Data and/or Information.

As stated under number 4 point (a) above, banks must explain in writing and/or orally to consumers regarding the purpose and consequences of granting written consent and providing and/or disseminating Consumer Personal Data and/or Information. It is a crucial thing that needs to be done by banks if it is related to consumer rights which are explicitly stated in Article 4 point (e) of the Law No. 8 of 1999 on Consumer Protection, that consumers are entitled to obtain proper advocacy, protection, and settlement in any consumer protection dispute. Likewise, under Article 7 paragraph (1) of the Bank Indonesia Regulation No. 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection, one of the principles of consumer protection is the principle of disclosure and transparency. The term "disclosure and transparency" means

the provision of information by the Operator to Consumers both orally and in writing, including clear and complete information through electronic means, in plain language. Article 31 of the POJK 1/2013 also explicitly states that Financial Service Providers are prohibited in any way from providing data and/or information regarding their consumers to third parties unless the consumer gives written consent, and/or such disclosure is required by laws or regulations. In addition, Article 26 of Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, establishes that the use of any information through electronic media concerning a person's personal data must be carried out only with the consent of the person concerned and the person who was harmed have the right to file a claim for damages if their rights are violated.

The 2025 SPI Blueprint also provides guidelines for banks, namely the existence of contractual standards for Open API collaboration between banks and third-party service providers including financial technology (fintech) as outlined in the form of guiding principles which include the rules for giving consent for data disclosure, procedures for accessing and modifying data and risk management. This aims to protect consumer data and/or personal information from data misuse. Violations or misuse of personal data can also result in criminal sanctions, as stated by Situmeang, that:[29]

> Misuse of personal data is an action that fulfills the elements of criminal acts such as elements of criminal acts of theft and elements of criminal acts of fraud and other criminal acts including both the objective and subjective elements. Misuse of personal data is an act that fulfills the elements of a criminal act such as the element of the criminal act of theft and the element of a criminal act of fraud and other criminal acts both in terms of objective elements and subjective elements. With the fulfillment of these elements, administrative sanctions, civil sanctions, and criminal sanctions are not sufficient to accommodate the criminal act of misuse of personal data which is a perfect form of crime.

IV. THE PRINCIPLE OF *AMANAH*

In addition to the precautionary principle, the confidentiality principle, and the fiduciary principle, there is one principle that is also important in protecting consumer data and/or information, namely the principle of *amanah*. In the Sharia Economic Law Compilation (*Kompilasi Hukum Ekonomi Syariah*,

[29] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," Sasi 27, no. 1 (2021): 38–52, 39, https://doi.org/10.47268/sasi.v27i1.394.

"KHES") the principle of *amanah* means that every contract must be carried out by the parties in accordance with the agreement determined by the person concerned and at the same time avoiding breach of contract. Therefore, according to Septarina Budiwati, the principle of *amanah* means that each party tries to have good intentions, or "good faith" in transacting with other parties and it is not allowed for one party to exploit the ignorance of the other party.[30]

Etymologically, *amanah* means *al-wafa* (fulfilling/delivering) and *wadi'ah* (entrusted), while based on its terminology, *amanah* means fulfilment of what is conveyed to him and entrusted to him so that peace of mind arises, dispelling any concerns. This can be seen in the word of Allah in Surah Al Baqarah verse 283 that:

> [i]f you are on a journey (and do *muamalah*, not in cash) and cannot find a scribe, then a mortgage (deposit) must be handed over; Hence, if one party has given *amanah* the other, the one who is receives the *amanah* shall return the object to him due to fear of Allah, his Lord; and do not hide his testimony; and if one hides it, his heart is sinful from within; and Allah knows what you do.[31]

In Islam, everything that is entrusted to man is called "amanah." As QS al-Anfal/8:27: 27: "O you who believe, do not betray Allah and the Messenger (Muhammad) and (also) do not betray the commissions entrusted to you, while you know."[32] The principle of *amanah* in the context of a contract is that contracting parties shall exercise good faith in the transaction and is not permissible for one party to betray another party. Betrayal or trespass means denying responsibility, being unfaithful, or breaking a promise he has made. Furthermore, trespass also means denying the responsibility that has been entrusted to him.

Amanah has the same meaning as the word faith, so that people do not practice *amanah* means not believing and not providing a sense of security for either themselves or other people. It can then be concluded that *amanah* conveys any right to the owner, not taking anything beyond his rights and not infringing on the rights of others. *Amanah* also has to do with the right of

---

[30] Septarina Budiwati, "Akad Sebagai Bingkai Transaksi Bisnis Syariah," Jurnal Jurisprudence 7, no. 2 (2018): 152–59, 158, https://doi.org/10.23917/jurisprudence.v7i2.4095.

[31] Muhammad Harfin Zuhdi, "Prinsip-Prinsip Akad Dalam Transaksi Ekonomi Islam," IqtIshaduna Jurnal Ekonomi Syariah 8, no. 1 (2017): 77–115, 100, https://journal.uinmataram.ac.id/index.php/iqtishaduna/article/view/403/167.

[32] Saddan Husain and Wahyuddin Abdullah, "Metafora Amanah Pengelolaan Dana Pihak Ketiga (DPK) Sebagai Penopang Asset Perbankan Syariah Ditinjau Dari Aspek Trilogi Akuntabilitas (Studi Kasus Pada PT. Bank BNI Syariah Cabang Makassar)," Jurnal Iqtisaduna 1, no. 2 (2015): 40–64, 41.

others to fulfill their obligations. In the business world, *amanah* and honesty are characteristics that must be shown, because *amanah* is the core of peaceful conditions and stabile society. In addition, *amanah* is also a moral and ethical foundation of peace and social interaction.[33]

According to several people, the principle of *amanah* is the same as the principle of good faith or fiduciary duty. This principle can be concluded from Article 1338 paragraph (3) BW that "Agreements must be implemented in good faith." This principle implies that the parties to an agreement must carry out the substance of the contract or obligation based on the principle of *amanah* or confidence and the good faith of the parties in order to achieve the objectives of the agreement.[34] It is emphasised that the character of *amanah* or being trustworthy is the most important characteristic that must exist in the person who will accept, maintain, and carry out an obligation in any form. *Amanah* is everything, both material and immaterial, which is entrusted by the giver to the recipient to always be maintained and fulfilled to the best degree possible.[35]

M. Isnaeni explained that the principle of good faith is in line with business ethics that are always enforced by the parties. Nuances of cooperation underlie the entire business process when the parties act in good faith. Therefore, the principle of good faith must exist at all stages of contracting, i.e., both during contract formation, until the close of the termination of the contract and on the performance of the contract.[36] It is also stated by Kevin Bork and Manfred Wandt regarding the importance of good faith in the civil law system:[37]

> Likewise, similar is the important task of the Civil Law judge when applying the law. Not only is he entitled to determine the content of norms by the recognised methods of interpretation (such as wording, systematics, *telos* and history) but also requested to apply fairness to the individual case. Probably the most important instrument for complying with this request is the principle of good faith. It serves to prevent injustice that can arise through the mere application of a provision and constitutes a necessary correction for the weaknesses of statutory law.

---

[33] Siti Salehah Madjid, "Prinsip-Prinsip (Asas-Asas) Muamalah," Jurnal Hukum Ekonomi Syariah 2, no. 1 (2018): 14–28, 24, https://doi.org/10.26618/j-hes.v2i1.1353.

[34] Ubaidullah Muayyad, "Asas-Asas Perjanjian Dalam Hukum Perjanjian Syariah," 'Anil Islam 8, no. 1 (2015): 1–24, 14, https://ejournal.inzah.ac.id/index.php/assyariah/article/view/256.

[35] Abdul Halim, Zulhedi, and Sobhan, "Karakteristik Pemegang Amanah Dalam Al-Qur'an," Mashdar: Jurnal Studi Al-Qur'an Dan Hadis 1, no. 2 (2019): 185–98, 198.

[36] M. Isnaeni, Selintas Pintas Hukum Perikatan (Surabaya: Revka Petra Media, 2017), 48.

[37] Kevin Bork and Manfred Wandt, "'Utmost' Good Faith in German Contract Law," Zeitschrift Fur Die Gesamte Versicherungswissenschaft 109, no. 2–4 (2020): 243–54, 243, https://doi.org/10.1007/s12297-020-00478-6.

Therefore, based on such meaning, the principle of *amanah* should become the fundamental principle for banks in implementing their service agreements regarding an open access system on consumers' data which shall uphold good faith between banks and consumers in order to manage consumers' data and/or information; neither party is allowed to exploit the ignorance of their contracting partners, and that the banks are to maintain the *amanah* that has been given by consumers in the form of granted consent/approval. Samuel D. Warren and Louis D. Bradeis also emphasised:[38]

> That an individual shall have full protection in person and in property is a principle as old as the common law, but it has been found necessary from time to time to define anew the exact nature and extent of such protection.

It is also emphasised by Marijana Petrovic that:[39]

> Regulatory open banking allows companies to provide more accurate personal financial guidance to customers, tailored to their circumstances and delivered securely and confidentially.

V. CONCLUDING REMARKS

One of the initiatives of the Indonesian 2025 SPI Blueprint is open banking to support banking digitisation. Open Banking is defined as an approach that allows banks to disclose their consumer financial data and information to third parties (fintech). As it is known that banks as financial services business actors are generally prohibited in any way from providing data and/or information about their customers to third parties. However, this prohibition is waived if the customer gives written consent or disclosure is required by laws or regulations. Therefore, with the customer's approval, a bank's legal action in providing data and/or customer information to a third party does not violate the principle of confidentiality. Even so, the provision of customer data by banks to any third party must be based on the fiduciary principle, precautionary principle, and the principle of *amanah*, as any misuse of customer's data by banks and third parties can lead to administrative sanctions, criminal sanctions, and civil sanctions on the basis of tort.

---

[38] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review 4, no. 5 (1890): 193–220, 193.

[39] Marijana Petrović, "PSD2 Influence on Digital Banking Transformation: Banks' Perspective," Journal of Process Management.: New Technologies 8, no. 4 (2020): 1–14, 2, https://doi.org/10.5937/jouproman8-28153.

REFERENCES

Abdullah, Samahir. "The Bank's Duty of Confidentiality, Disclosure Versus Credit Reference Agencies; Further Steps for Consumer Protection: 'Approval Model.'" *European Journal of Current Legal Issues* 19, no. 4 (2013). https://webjcli.org/index.php/webjcli/article/view/296/405.

Bank Indonesia. *Bank Indonesia : Menavigasi Sistem Pembayaran Nasional Di Era Digital BANK INDONESIA*. Jakarta: Bank Indonesia, 2019.

Bork, Kevin, and Manfred Wandt. "'Utmost' Good Faith in German Contract Law." *Zeitschrift Fur Die Gesamte Versicherungswissenschaft* 109, no. 2–4 (2020): 243–54. https://doi.org/10.1007/s12297-020-00478-6.

Budiwati, Septarina. "Akad Sebagai Bingkai Transaksi Bisnis Syariah." *Jurnal Jurisprudence* 7, no. 2 (2018): 152–59. https://doi.org/10.23917/jurisprudence.v7i2.4095.

Greenleaf, Graham, and Alan Tyree. "Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons." In *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres around the World*, edited by Dora Neo and Sandra Booysen, 31–61. Cambridge: Cambridge University Press, 2017. https://doi.org/DOI: 10.1017/9781316535219.003.

Hadad, Shahrazad. "Challenges for Banking Services in the Knowledge Economy." *Management Dynamics in the Knowledge Economy* 7, no. 3 (2019): 337–52. https://doi.org/10.25019/mdke/7.3.04.

Halim, Abdul, Zulhedi, and Sobhan. "Karakteristik Pemegang Amanah Dalam Al-Qur'an." *Mashdar: Jurnal Studi Al-Qur'an Dan Hadis* 1, no. 2 (2019): 185–98.

Hernoko, Agus Yudha. *Hukum Perjanjian: Asas Proporsionalitas Dalam Kontrak Komersial*. Yogyakarta: Laksbang Mediatama, 2008.

Husain, Saddan, and Wahyuddin Abdullah. "Metafora Amanah Pengelolaan Dana Pihak Ketiga (DPK) Sebagai Penopang Asset Perbankan Syariah Ditinjau Dari Aspek Trilogi Akuntabilitas (Studi Kasus Pada PT. Bank BNI Syariah Cabang Makassar)." *Jurnal Iqtisaduna* 1, no. 2 (2015): 40–64.

Iryna, Basysta, Shepitko Iryna, and Shutova Olga. "Protection and Risks of Illegal Divulgation of Banking Secrecy in Ukrainian Criminal Proceeding*." *Access to Justice in Eastern Europe* 4, no. 8 (2020): 298–305. https://doi.org/10.33327/AJEE-18-3.4-n000042.

Isnaeni, M. *Selintas Pintas Hukum Perikatan*. Surabaya: Revka Petra Media, 2017.

Laplante, Phil, and Nir Kshetri. "Open Banking: Definition and Description." *Computer* 54, no. 10 (2021): 122–28. https://doi.org/10.1109/MC.2021.3055909.

Madjid, Siti Salehah. "Prinsip-Prinsip (Asas-Asas) Muamalah." *Jurnal Hukum Ekonomi Syariah* 2, no. 1 (2018): 14–28. https://doi.org/10.26618/j-hes.v2i1.1353.

Muayyad, Ubaidullah. "Asas-Asas Perjanjian Dalam Hukum Perjanjian Syariah." *'Anil Islam* 8, no. 1 (2015): 1–24. https://ejournal.inzah.ac.id/index.php/assyariah/article/view/256.

Muqorobin, Masculine Muhammad, Ayu Anggraini, Ayu Dewi Rahmawati, Diana Yohanes, and Faricha Ifkarina. "Pengaruh Open Banking Berbasis Open API Terhadap Eksistensi Perbankan." *MAKSIMUM* 11, no. 2 (2021): 75–84. https://jurnal.unimus.ac.id/index.php/MAX/article/view/7877.

Omarini, Anna Eugenia. "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future." *International Business Research* 11, no. 9 (2018): 23–36. https://doi.org/10.5539/ibr.v11n9p23.

Petrović, Marijana. "PSD2 Influence on Digital Banking Transformation: Banks' Perspective." *Journal of Process Management.: New Technologies* 8, no. 4 (2020): 1–14. https://doi.org/10.5937/jouproman8-28153.

Prayogo, Sedyo. "Penerapan Batas-Batas Wanprestasi Dan Perbuatan Melawan Hukum Dalam Perjanjian." *Jurnal Pembaharuan Hukum* 3, no. 2 (2016): 280–87. https://doi.org/10.26532/jph.v3i2.1453.

Purwanto, Harry. "Keberadaan Asas Pacta Sunt Servanda Dalam Perjanjian Internasional." *Mimbar Hukum* 21, no. 1 (2009): 155–70. https://doi.org/10.22146/jmh.16252.

Rani, Marnia. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank." *Jurnal Selat* 2, no. 1 (2014): 168–81.

Revathy, P., and G. Belshia Jebamalar. "A Review Based on Secure Banking Application against Server Attacks." In *Smart Intelligent Computing and Communication Technology*, edited by V.D. Ambeth Kumar, S. Malathi, V.E. Balas, M. Favorskaya, and T. Perumal, 38:241–45. Amsterdam: IOS Press, 2021. https://doi.org/10.3233/APC210044.

Rizal, Muhammad Saiful. "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malaysia." *Jurnal Cakrawala Hukum* 10, no. 2 (2019): 218–27. https://doi.org/10.26905/idjch.v10i2.3349.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. "Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (2018): 88–110. https://doi.org/10.25123/vej.2916.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Sasi* 27, no. 1 (2021): 38–52. https://doi.org/10.47268/sasi.v27i1.394.

Stranieri, Andrew, Angelique N. McInnes, Mustafa Hashmi, and Tony Sahama. "Open Banking and Electronic Health Records." In *ACSW '21: 2021 Australasian Computer Science Week*, 1–4. Association for Computing Machinery, 2021. https://doi.org/https://doi.org/10.1145/3437378.3437397.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220.

Yasin, Akhmad. "Keterkaitan Kerahasiaan Bank Dan Pajak: Antara Kepentingan Negara Dan Pribadi." *Jurnal Konstitusi* 16, no. 2 (2019): 212–34. https://doi.org/10.31078/jk1621.

Yunanto, Yunanto. "Hakikat Asas Pacta Sunt Servanda Dalam Sengketa Yang Dilandasi Perjanjian." *Law, Development and Justice Review* 2, no. 1 (2019): 33–49. https://doi.org/10.14710/ldjr.v2i1.5000.

Yuniarti, Siti. "Perlindungan Hukum Data Pribadi Di Indonesia." *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (2019): 147–54. https://doi.org/10.21512/becossjournal.v1i1.6030.

Zatika, Dinda Anna. "Pembukaan Prinsip Kerahasiaan Bank Sebagai Perbuatan Melawan Hukum (Studi Kasus Bank BCA)." *Sasi* 26, no. 4 (2020): 500–513. https://doi.org/10.47268/sasi.v26i4.238.

Zuhdi, Muhammad Harfin. "Prinsip-Prinsip Akad Dalam Transaksi Ekonomi Islam." *IqtIshaduna Jurnal Ekonomi Syariah* 8, no. 1 (2017): 77–115. https://journal.uinmataram.ac.id/index.php/iqtishaduna/article/view/403/167.

This page is intentionally left blank