Jurnal IUS Kajian Hukum dan Keadilan
Volume 13 Issue 3, December 2025, E-ISSN 2477-815X, P-ISSN 2303-3827
Indexing: Scopus, DOAJ, Sinta 1, open access at : https://jurnalius.ac.id/

Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification

Muhamad Amirulloh[1]* Eman Suparman[2], Helitha Novianty Muchtar[3], Hetty Hassanah[4]
[1] Universitas Padjadjaran, Indonesia, email: muhamad.amirulloh@unpad.ac.id
[2] Universitas Padjadjaran, Indonesia, email: Eman@unpad.ac.id
[3] Universitas Padjadjaran, Indonesia, email: helitha.novianty@unpad.ac.id
[4] Universitas Komputer Indonesia, Indonesia, email: hetty.hassanah@email.unikom.ac.id

Abstract

There is a disharmony between PBI PKBI and PADG PKBI with the PDP Law, P2SK Law, SPK Law and PBSSN Common Criteria in terms of regulating the obligation to use privacy reliability certificates by financial sector business actors under BI, so that there are many cases of customer personal data breaches. By using normative and empirical juridical methods, this study analyzes efforts to harmonize the regulations related to privacy certification obligations in the financial sector under BI. The results of the study show that with grammatical, systematic, and teleological legal interpretation, PBI PKBI and PADG PKBI can be harmonized regarding the privacy reliability certificate as the legal object in question and the nature of the regulatory norms, but it is not harmonized regarding the status of the privacy reliability certificate as a mandatory SNI, because both PBI PKBI and PADG PKBI as technical regulations in the perspective of the SPK Law have not stipulated SNI ISO 15408-2, 15408-3, or 15408-5 as the referenced standard.

Keywords: bank, compulsory, personal data protection, privacy reliability certification.

1. INTRODUCTION

There is a legal disharmony related to the privacy reliability certificate between the Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and the Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) on the one hand and the Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law) on the other. The norms referred to in the ITE Law and PP PSTE are only "regulating" or "aanvullend recht", while in the PDP Law it is "obligating" or "dwingend recht".[1] Article 10 paragraph (1) of the ITE Law stipulates that "Any business actor who conducts Electronic Transactions may be certified by Trustworthiness Certification Bodies". Article 42 paragraph (2) of the PP PSTE stipulates that, "The implementation of Electronic Transactions may use a Certificate of Reliability". Article 39 of the PDP Law stipulates that, "(1) The Personal Data Controller is obliged to prevent Personal Data from being accessed unlawfully. (2) Prevention as intended in paragraph (1) is carried out with a security system for Personal Data that is processed and/or processes

[1] Dimas Sulistio, Eman Suparman, and Muhamad Amirulloh, "Information Security Management System : Electronic Apostille System Security to Ensure Legal Certainty across National Borders," *International Journal of Data and Network Science* 9, no. 4 (2025): 881–90, https://doi.org/10.5267/j.ijdns.2025.1.004.

 DOI: http://dx.doi.org/10.29303/ius.v13i3.1777

Personal Data in an electronic system in a reliable, secure, and responsible manner. (3) Prevention as intended in paragraph (2) shall be carried out in accordance with the provisions of laws and regulations. Meanwhile, Article 239 of the P2SK Law stipulates that, "(1) PUSK is obliged to maintain the confidentiality and security of Consumer data and/or information. (2) The obligations of PUSK as intended in paragraph (1) are carried out by applying the basic principles of personal data protection processing as stipulated in the provisions of laws and regulations regarding personal data protection. This makes the public, especially business actors in the banking sector, confused about whether to implement a privacy reliability certificate or not.

In fact, cases of misuse of personal data are increasingly occurring. Misuse of personal data protection is becoming more prevalent. This impacts both individuals and corporations [2]. For individual, identity theft for fraud or bank account breaches is common case nowadays. For corporations, leading to a decline in company reputation, significant recovery costs, and fines in accordance with applicable regulations [3]. Banking activities are closely linked to the utilization of customers' personal data and there are identity theft for fraud or bank account breaches case in Indonesia[4]. Safeguarding customer data serves as a form of consumer protection in banking, which is an essential facet of financial inclusion (i.e., responsible finance through financial education and consumer protection, along with providing suitable service facilities and appropriate products)[5].

Consumer protection in the digital age is a multifaceted issue that requires a dynamic and adaptive legal framework to address the unique challenges posed by online transactions. The rapid evolution of digital technology has necessitated the development of preventive and repressive legal protections to ensure consumer safety and confidence in e-commerce. Preventive measures focus on establishing standards and regulations to prevent harm before a transaction occurs, while repressive measures provide mechanisms to address post-transaction offences.[6]. The digital environment generates vast amounts of data, raising concerns about data protection and consumer privacy. Ensuring the confidentiality and integrity of consumer data is critical to maintaining trust in digital transactions [7].

To aligns with the digital transformation, Bank Indonesia as the central bank needs to advancing towards Central Bank 4.0 in the Fourth Industrial Revolution era and as one of the Financial Sector Authority[8] by promptly harmonized it's regulation with laws on personal data protection as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The aforementioned legal harmonization, in particular,

[2] Ninuk Triyanti et al., "Legal Gaps in Personal Data Protection : Reforming Indonesia ' s Population Administration Law," *Hasanuddin Law Review* 11, no. 1 (2025): 132–47, https://doi.org/10.20956/halrev.v11i1.6177.

[3] Ari Wibowo and Widya Alawiyah, "The Importance of Personal Data Protection in Indonesia ' s Economic Development," *Cogent Social Sciences* 10, no. 1 (2024), https://doi.org/10.1080/23311886.2024.2306751.

[4] Wardah Yuspin et al., "Personal Data Protection Law in Digital Banking Governance in Indonesia," *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130, https://doi.org/10.17951/sil.2023.32.1.99-130

[5] Bank Indonesia, "Keuangan Inklusif," Bank Indonesia, 2020, https://www.bi.go.id/id/fungsi-utama/stabilitas-sistem-keuangan/keuangan-inklusif/Default.aspx#floating-3.

[6] Abdul Risal, "Jurnal Hukum Bisnis Bonum Commune Legal Protection for Debtors in Online Transactions : Evaluating Safeguards in E-Commerce" 7, no. 1 (2024): 176–87, https://doi.org/10.30996/jhbbc.v7i2.11656; Achmad Zulfa Andikatama and Bambang Eko Turisno, "Consumer Protection Law in the Digital Era," *International Journal of Social Science and Human Research* 7, no. 07 (2024), https://doi.org/10.47191/ijsshr/v7-i07-03.

[7] Cristina Mihaela, "Consumer Protection in The New Digital Decade," *SALCĂ ROTARU* 1, no. 1 (2024), https://doi.org/10.69971/x5yf2150.

[8] See Art. 244 P2SK Law.

should involve setting obligations for Reliability Certification as a technological instrument aimed at ensuring consumer protection. Accelerating the adoption of privacy reliability certificates as SNI Strategic steps in improving personal data protection and legal certainty for Electronic System Operator. This article will discuss the issue of whether Bank Indonesia has a strong legal basis regarding the obligation to implement the Privacy Reliability Certificate to protect consumers' personal data in harmony with the relevant laws and regulations, and whether a privacy reliability certificate is a legal obligation that must be applied by business actors in the banking sector.

This research employs a combination of normative and empirical legal approaches to examine the concept and implementation of the obligation of banking sector business actors to have a privacy reliability certificate. Normatively, the harmonization and applicability of legal norms regarding privacy reliability certificates between the cyber law regime and personal data protection law and banking sector law based on legal principles and theories are examined. Empirically, this study investigates the fact of the use of privacy reliability certificates by business actors in the banking sector.

2. ANALYSIS AND DISCUSSION

2.1. Harmonization on Legal Regulations of Bank Indonesia related to Privacy Reliability Certificate Obligations

In Hans Kelsen's theory of pure law, the "closed logical system of norms" refers to the view that law is a hierarchically and logically arranged system of norms, in which each norm derives its validity from a higher norm, culminating in a basic norm (Grundnorm). Kelsen emphasized that the legal system must be logically consistent, so that any norm that contradicts the higher norm is considered invalid. This system is also deductive, in which lower norms are derived from higher norms through logical processes.[9] In relation to the protection of personal data, it can be said that the PDP Law and the P2SK Law have their validity based on the Indonesian constitution, namely the 1945 Constitution of the fourth amendment. From a constitutional perspective, personal data receives legal protection based on Article 28G (1) of the 1945 Constitution, which states, "Every person shall have the right to the protection of self, family, honor, dignity, and property, and has the right to security and protection from threats of fear to exercise or not to exercise their fundamental rights."[10] Likewise, the constitutional basis for personal data protection is found in Article 28H paragraph (1) of the 1945 Constitution, which states, "Every person has the right to own personal property, and such property may not be arbitrarily deprived by anyone." Thus, based on this theory, it can be said that the applicable provisions related to the protection of personal data by using a security system for personal data are the P2SK Law and the PDP Law, not the provisions of the ITE Law and PP PSTE, because the P2SK Law and the PDP Law have the basis for their validity based on Article 28 H paragraph (1) of the 1945 Constitution of the fourth amendment.

[9] A Kraevsky, "Validity and Efficacy of International Law According to the Pure Theory of Law," *Vestnik of Saint Petersburg University. Law*, 2021, https://doi.org/10.21638/spbu14.2021.113; Cahya Iradi Arimba, "Hans Kelsen's Nomostatics and Nomodinamics Legal Theory," *Justice Voice*, 2024, https://doi.org/10.37893/jv.v2i2.773.

[10] Tina Amelia, Nunung Rahmania, and Aftab Haider, "Legal Protection of Personal Data as Listed in Court Decision : A Discourse Renewal," *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 3 (2024).

Hans Kelsen's theory of pure law greatly influenced the way of interpreting law, especially in limiting interpretation to the normative and internal aspects of the legal system. Kelsen emphasized that the interpretation of law is a mental process that occurs in the application and formation of law, and must remain within the framework of an autonomous legal system.[11] Systematic interpretation is very much in line with the theory of pure law. Kelsen views law as a hierarchical and structured system of norms, in which each norm derives its validity from a higher norm (stufenbau). According to Kelsen, legal interpretation must be carried out by paying attention to the position and relationship between norms in the legal system, not separately.[12] Systematic interpretation places a legal norm in the context of the legal system as a whole. Norms are not understood in isolation, but rather are associated with other norms, legal principles, and broader regulatory structures. This method helps uncover the meaning of norms by looking at their relationships and consistency in the legal system.[13] Based on a systematic legal interpretation, the applicable regulations related to privacy reliability certificates are those contained in the PDP Law and the P2SK Law, not the ITE Law and PP PSTE. This is considering that the purpose of the ITE Law as stipulated in Article 4 letter e is, "to provide a sense of security, justice, and legal certainty for IT Users & Operators". That sense of security can only be fulfilled if an electronic system is equipped with a privacy reliability certificate so that personal data is truly protected. The regulations related to the privacy reliability certificate in the PDP Law and the P2SK Law can be said to be more capable of realizing the intended goals.

The purpose as referred to in Article 4 letter e of the ITE Law can be said to be a goal within the scope of cyber law, so that it is in line with Hans Kelsen's intention to systematically create legal integration. This purpose is not an extrajudicial purpose, so it can also be said that a teleological interpretation that is limited to a legal purpose can be done. Teleological (or purposive) interpretation seeks to reveal the purpose or intent of the formation of a legal norm. Interpreters look for what the lawmakers want to achieve through these norms, so that the application of the law can be aligned with the social goals, justice, or values that they want to realize. [14]

Grammatical interpretation focuses on the meaning of words, terms, and sentence structures in legal texts. This method emphasizes understanding the literal meaning of the words used by lawmakers, paying attention to grammar and syntax. The goal is to find the clear and explicit meaning of the legal text without adding or detracting from the meaning.[15] In the context of Article 39 paragraph (2) of the Personal Data Protection Law (PDP Law), the key phrases that need to be interpreted grammatically

[11] Ícaro Fellipe Alves Ferreira De Brito, "INTERPRETATION OF LAW AND THE KELSENIAN INTERPRETIVE FRAMEWORK," ARACÊ, 2024, https://doi.org/10.56238/arev6n3-138; Ahmad Fanani and Muhammad Sulthon Zulkarnain, "Understanding John Austin's Legal Positivism Theory and Hans Kelsen's Pure Legal Theory," Peradaban Journal of Law and Society, 2022, https://doi.org/10.59001/pjls.v1i2.41.

[12] O. Bogdan V. Seredyuk, "Neo-Kantian Epistemological Basis of Hans Kelsen's Pure Theory of Law," *Scientific Bulletin of Uzhhorod National University. Series: Law* 4, no. 8 (2025): 177–84, https://doi.org/https://doi.org/10.24144/2307-3322.2025.88.4.27.V. Seredyuk.V. Seredyuk; Divya Bisht, "Kelsen's Pure Theory of Law: An Overview," *International Journal for Research in Applied Science and Engineering Technology*, 2023, https://doi.org/10.22214/ijraset.2023.49679.

[13] Merdova Olha et al., "Interpretation of Legal Norms in Modern Jurisprudence," *Cuestiones Políticas* 41, no. 77 (2023): 298–308, https://doi.org/https://doi.org/10.46398/cuestpol.4177.20.

[14] Merdova Olha et al.

[15] V. Leheza, Y., Reznykova, M., Korniakova, T., Lytvyn, O., & Komashko, "Understanding the Interpretation of Legal Standards: Theoretical, Administrative, Criminal, Financial Aspects.," *Revista Do Curso de Direito Do UNIFOR.*, 2023, https://doi.org/https://doi.org/10.24862/rcdu.v14i2.1828.

are: "security system for Personal Data that processes and/or processes Personal Data in electronic systems in a reliable, secure, and responsible manner." The relationship with the Privacy Reliability Certificate (Article 76 paragraph (1) letter c PP PSTE) is that the Privacy Reliability Certificate is formal proof that an electronic system has met certain reliability and security standards. Grammatically speaking, the phrase "security system for Personal Data that is processed and/or processes Personal Data in an electronic system in a reliable, secure, and responsible manner" in Article 39 paragraph (2) can be interpreted as the requirement of electronic systems to have verifiable reliability, one of which is through certification. The grammatical interpretation directs that "the security system for personal data... reliably" in Article 39 paragraph (2) of the PDP Law textually opens up space for the existence of a Privacy Reliability Certificate as one of the instruments to prove the reliability of electronic systems as stipulated in Article 76 paragraph (1) letter c of PP PSTE. The grammatical interpretation of Article 39 paragraph (2) of the PDP Law emphasizes that the personal data security system must be reliable, secure, and responsible. This reliability can be textually proven through the Privacy Reliability Certificate as stipulated in the PP PSTE, so that the two provisions complement each other normatively.

The regulatory disharmony on privacy reliability certificate obligations can also be examined through legal principles related to conflict of norms. A conflict of norms occurs when there are two legal rules that govern the same thing, but give conflicting orders, prohibitions, or permits. In this situation, the application of one of the norms will lead to a violation of the other norm. Conflicts can occur between prescriptive (commanding/prohibiting) and permissive (allowing) norms, or between two conflicting prescriptive norms.[16] There are 3 (three) main legal principles to resolve conflicts of norms in the legal system. First, Lex superior derogat legi inferiori: If there is a conflict between laws and regulations of different levels (e.g., laws vs government regulations), then the higher degree of regulation will apply.[17] The P2SK Law applies to set aside PBI PKBI and PADG PKBI based on this principle. The P2SK Law is higher in rank than PBI PKBI and PADG PKBI. Similarly, the PP PSTE was sidelined because it was in a lower position compared to the PDP Law and the P2SK Law.

Second, Lex specialis derogat legi generali: If there are two rules of the same level, but one of them is more specific, then a specific rule is applied.[18] The PDP Law and the P2SK Law apply to set aside the ITE Law based on this principle. The PDP Law is more specialized in the protection of personal data, and the P2SK Law is more specialized in the financial sector compared to the ITE Law. Similarly, PP PSTE is ruled out because it is more common compared to PBI PKBI. The P2SK Law sets aside the Consumer Protection Law Number 8 of 1999, because it is based on Article 248 of the P2SK Law.

Third, Lex posterior derogat legi priori: If two rules are of the same level and of the same nature, then the newer rule applies.[19] PBI PKBI Number 3 of 2023 sets aside PBI

[16] E. Vranes, "The Definition of 'Norm Conflict' in International Law and Legal Theory.," *European Journal of International Law.* 17, no. 2 (2006): 395–418, https://doi.org/https://doi.org/10.1093/ejil/chl002.

[17] Mesa Indra Naiborhu and Wagiman, "THE FUNDAMENTAL POSITION OF LEX POSTERIOR DEROGAT LEGI PRIORI IN THE CONFLICT OF NORMS AGAINST THE RIGHTS OF HOLDERS OF THE RIGHT TO JUSTICE," *Jurnal Indonesia Sosial Teknologi* 5, no. 2 (2024): 659–71, https://doi.org/10.59141/jist.v5i2.906.

[18] I. Bernazuk, "APPLICATION OF THE LEX SPECIALIS PRINCIPLE TO SOLVING CONFLICTS IN LEGISLATION: ANALYSIS OF COURT PRACTICE.," *Slovo of the National School of Judges of Ukraine.* 38–39, no. 1–2 (2022): 69–82, https://doi.org/https://doi.org/10.37566/2707-6849-2022-1-2(38-39)-7.

[19] Muh. Afdal Yanuar, "Laundering of Proceeds Forest Destruction and Narcotics Crimes: A Resolution of The Conflict Norms," *Mulawarman Law Review* 8, no. 1 (2023): 1–20, https://doi.org/https://doi.org/10.30872/mulrev.

PKBI Number 22 of 2020, and PADG PKBI Number 23 of 2023 sets aside PADG PKBI Number 23 of 2021.

In an effort to provide consumer protection, including the protection of consumers' personal data, currently, Bank Indonesia has Bank Indonesia Regulation No. 3 of 2023 concerning Consumer Protection of Bank Indonesia (PBI PKBI), and Regulation of Members of the Board of Governors No. 20 of 2023 concerning Procedures for the Implementation of Bank Indonesia Consumer Protection (PADG PKBI), which was made based on the provisions of the P2SK Law.[20] In relation to consumer protection, including the protection of consumer personal data, both the P2SK Law and PBI PKBI have determined the need to harmonize with the PDP Law and other related regulations.

Article 7 paragraph (1) letter f of PBI PKBI also states that one of the principles of consumer protection is the protection of consumer data and/or information. The explanation for this provision is that the protection of consumer data and/or information is carried out by the financial service providers, among other things, by maintaining the confidentiality and security of such data and/or information, and only using this data and/or information according to the interests and purposes approved by the Consumer. The principle of protecting consumer data and/or information is further implemented in the norms found in Article 32 of the said PBI PKBI.

Provisions directly related to the use of electronic systems in protecting consumer data and/or information are found in Article 32. Paragraph (1) stated that, "The Organizer is obliged to maintain the confidentiality and security of Consumer data and/or information". This provision is a basic provision that places an obligation for financial sector business actors to maintain the confidentiality and security of consumer data. With the nature of the obligating or coercive norm, in line with the norms in the P2SK Law and the PDP Law. This is strengthened by the regulation of paragraph (2) which reads: (2) The obligation to maintain the confidentiality and security of Consumer data and/or information as intended in paragraph (1) in accordance with the provisions of laws and regulations. In addition to the P2SK Law and the PDP Law, regulations related to privacy reliability certificates include Law Number 20 of 2014 concerning Standardization and Conformity Assessment (SPK Law), Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure (Perpres PIIV), and Regulation of the State Cyber and Cryptography Agency Number 7 of 2024 concerning Implementation of Conformity Assessment of General Criteria for The Evaluation of Indonesian Information Technology Security (Indonesia Common Criteria For Information Technology Security Evaluation) (PBSSN Common Criteria).

Very specific provisions in the PBI PKBI related to privacy reliability certificates are contained in Article 32 paragraph (3) letter b which stipulates that, "to maintain the confidentiality and security of data and/or Consumer information as intended in paragraph (1), The organizer must have:

a. Functions responsible for protection Consumer data and/or information;
b. Reliable information and cyber resilience systems to support data protection implementation and/or Consumer information; and

v8i1.1044.al

[20] The Dictum Considering the letter a of PBI PKBI states that "with the enactment of Law Number 4 Year 2023 on Sector Development and Strengthening Finance has strengthened Bank Indonesia's authority to perform setup and supervision Consumer Protection in the Financial Sector".

c. mechanisms and procedures regarding data protection and/or Consumer information."

By interpreting it grammatically and systematically, and teleologically, Article 32 paragraph (3) b is interpreted as the basis for the obligation for financial sector business actors to have a privacy reliability certificate as referred to in the PDP Law, P2SK Law and PP PSTE. Financial sector business actors who do not carry out these obligations will be subject to administrative sanctions in the form of written warning to revocation of business license, based on the paragraph (4).

Thus, it can be said that PBI PKBI has laid the legal basis for the obligation to use a privacy reliability certificate for financial sector Business actors regulated and supervised by Bank Indonesia.

According to Article 37 of PBI PKBI, it is stated that further provisions regarding the implementation of the principles of consumer data and/or information protection as well as procedures for imposing administrative sanctions are regulated in the Board of Governors Regulation (Peraturan Anggota Dewan Gubernur - PADG). Currently, there is already a Regulation of Members of the Board of Governors Nmor 20 of 2023 on the Procedures for the Implementation of Consumer Protection of Bank Indonesia (PADG PKBI). Article 16 (1) PADG PKBI stipulate that "The Organizer is obliged to maintain confidentiality and security Consumer data and/or information". This provision has the same meaning as Article 32 paragraph (1) of the PBI PKBI.

Furthermore, in Article 16 paragraph (3) of the PADG PKBI, it is stipulated that the obligation to maintain data confidentiality and security and/or Consumer information as intended in paragraph (1) is carried out in accordance with the provisions of the Laws and Regulations. This provision also has the same meaning as Article 32 paragraph (2) of the PBI PKBI. While the provisions regarding the mechanism and procedures for the protection of consumer data and/or information, Article 19 of the PADG PKBI is essentially only about the use of consumer data and/or information, which is carried out by pouring it into the the Operator's internal provisions regarding the use of data and/or Consumer Information.

Unfortunately, in this PADG PKBI there is no provision that further implements Article 32 paragraph (3) of the PBI PKBI, especially related to the obligation to use a privacy reliability certificate. Thus, it can be said that the PADG PKBI as a technical regulation that is expected to establish technical standards that refer to the privacy reliability certificate is anticlimactic.

In an effort to create information system security and cyber resilience, BI has made PBI Number 2 of 2024 (PBI KKS). Article 28 of the PBI KKS stipulates that in the context of prevention, security and protection of data and/or information shall be carried out by means of Ensure compliance with personal data protection in accordance with the provisions of laws and regulations. Following up on the PBI KKS, PADG KKS Number 24 of 2024 was made. Regarding personal data protection, Article 24 of the PADG KKS also stipulates that the prevention and protection of personal data is carried out by ensuring compliance with the protection of personal data in accordance with the provisions of laws and regulations. Thus, even in the scope of information system security and cyber resilience, both in PBI KKS and PADG KKS there are no provisions at all regarding privacy reliability certification and the technical standards they use.

Meanwhile, the PADG for the implementation of KKS according to the Classification of Financial Sector Business Operators until now (December 2025) does not exist.

2.2. Compliance of Banks and Financing Technology Business Actors with the Obligation to Implement the Privacy Reliability Certificate.

In practice, it has been observed that the sum of 13 subjects, including 3 government bank, 1 local government bank, and 1 private bank, also 9 payment gateways, do not have the Privacy Reliability Certificate yet (until 2023). Based on the regulatory analysis in section 2.1., this happens because there is no provision in PBI PKBI and PADG PKBI also PBI KKS and PADG KKS, that sets certain standards to be used as a standard for the implementation of privacy reliability certificates in the financial services sector, especially under Bank Indonesia.

Table 1. PUSK BI Implemented Privacy Reliability Certificate (Per 2023)

Name (Data Kept Confidential, by request)	Implemented	
	Information Security Management Certif.	Privacy Information Management Certifi.
Gov Bank A	**Process**	**X**
Gov Bank B	**Process**	**X**
Gov Bank C	√	**X**
Local Gov Bank D	√	**X**
Private Bank E	√	**X**
Payment Gateway E	n.a.	**X**
Payment Gateway F	n.a.	**X**
Payment Gateway G	√	**X**
Payment Gateway H	√	**X**
Payment Gateway I	√	**X**
Payment Gateway J	√	**X**
Payment Gateway K	√	**X**
Payment Gateway L	√	**X**

In addition, the lack of the formation of the Personal Data Protection Institution as stipulated in the PDP Law is also one of the obstacles regarding the authority of its regulatory institutions. Based on the SPK Law, PBI PKBI and PADG PKBI with the absence of technical regulations regulating privacy reliability certificates is also one of the causes of weak implementation. This is because with the non-establishment of the referred technical standards, the obligation to certify privacy reliability has not become mandatory SNI. In detail, Article 24 of the SPK Law stipulates as follows: (1) In matters related to the interests of safety, security, health, or preservation of environmental functions, non-ministerial ministries/government agencies are authorized to determine

the mandatory implementation of SNI by Ministerial Regulation or Regulation of the Head of Non-Ministerial Government Institutions. (2) Business Actors, ministries/ non-ministerial government institutions, and/or Regional Governments are obliged to implement Ministerial Regulations or Regulations of Heads of Non-Ministerial Government Institutions regarding the mandatory implementation of SNI.

The latest development shows that the State Cyber and Cryptography Agency Regulation Number 7 of 2024 has stipulated that for cybersecurity and privacy protection for electronic systems that include vital information infrastructure, there is an obligation to implement SNI ISO/IEC 15408-2, 15408-3, and 15408-5. Meanwhile, based on Article 4 paragraph (1) letter d of Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure and Article 99 paragraph (2) letter d of PP PSTE, the financial sector is one of the sectors included in the Vital Information Infrastructure. Based on Article 1 point 35 PP PSTE, State Organizing Agencies, hereinafter referred to as Agencies, are legislative, executive, and judicial institutions at the central and regional levels and other agencies established by laws and regulations. Thus Bank Indonesia is other agencies established by laws and regulations as financial sector agency referred to in Article 99 paragraph (2) letter d PP PSTE. The existing PBI PKBI and PADG PKBI are not at all in accordance with the SPK Law and BSSN Regulation or the Presidential Regulation in question, because in particular, PADG PKBI has not set SNI ISO 15408-2, 15408-3, or 15408-5 as the referred technical standard.

In relation to the obligation to implement cybersecurity standards, Article 9 of the PIIV Presidential Regulation stipulates that, "IIV operators must carry out IIV protection reliably and safely and be responsible for the operation of IIV as appropriate. In the protection of IIV as intended in paragraph (1), IIV Operators are obliged to implement information security standards and/or other security standards set by the Ministry or Institutions and/or Agencies." Based on this provision, in order to protect personal data and implement privacy reliability certificates, financial sector authorities are obliged to harmonize with the provisions made by the State Cyber and Cryptography Agency (BSSN).

In creating a financial sector ecosystem compliant with the Personal Data Protection Law (PDP Law) that safeguards personal data and the EIT Law that requires reliability and security of electronic systems—both of which aim to protect consumers and society—the financial sector authority should view and treat reliability certification as a "minimum standard". This is considering that the financial sector has a "strategic" or at least "high" vulnerability or susceptibility to cybercrime. Consequently, financial supervisory and regulatory authorities should take harmonious steps aligned with efforts to provide higher-level personal data protection in Indonesia, as a manifestation of consumer protection. Such steps can be taken by establishing regulations and supervising the use of privacy reliability certificates for Public Electronic System Organizers[21].

The implementation of the SNI ISO/IEC 15408-2, 15408-3, and 15408-5 Privacy Reliability Certificate can be viewed as an investment in efforts to protect public and

[21] Artur Strzelecki and Mariia Rizun, "Consumers' Security and Trust for Online Shopping after GDPR: Examples from Poland and Ukraine," *Digital Policy, Regulation and Governance* 22, no. 4 (2020): 289–305, https://doi.org/10.1108/DPRG-06-2019-0044.

consumers' personal data. Thus, even though it requires significant costs, this should be seen as relatively cheaper compared to the costs of recovery from personal data breaches and/or costs that may arise from continued misuse of breached personal data. This aligns with Richard A. Posner's economic analysis of law theory. Misuse of personal data resulting from data breaches includes various malicious purposes such as fraud, theft, bank account breaches, unsolicited product promotions, and privacy violations[22].

One such case occurred on 5 October 2020, where the Indonesian National Police identified 10 suspects who hacked into 3,070 customer accounts across various banks and Grab user accounts (an online transportation platform), amassing around US$1.5 million or approximately Rp21 billion from compromised accounts. The most intriguing fact was that the data from the compromised accounts was gathered from the official Financial Information Services System of the Financial Services Authority (OJK)[23]. It is evident that the 21 billion Rupiah from this personal data crime (and potentially more with ongoing misuse) is incomparable to the investment costs businesses would incur for implementing privacy reliability certification and/or electronic system security reliability certification, ranging between 75 million to 350 million Rupiah. Moreover, the strategic choice of implementing privacy reliability certification requires detailed and thorough calculations to maximize efficiency in funds and other resources expended by Public Electronic System Organizers. The costs and processes of SNI ISO/IEC 15408-2, 15408-3, and 15408-5 certification can vary based on company size, consultant or auditor qualifications, and the duration of the certification process[24]. The cost of the risk of personal data breaches should also consider the expenses to be paid to plaintiffs or customers or consumers or the public who file compensation claims due to the leakage of their personal data managed by Financial Sector Business Actors.

A model for protecting personal data is to use Privacy Information Management with the ISO 27701 standard [25]. ISO 27701 is an international standard that extends ISO/IEC 27001 and 27002 for privacy information management, providing a framework for managing personal data and ensuring compliance with privacy regulations. It is particularly relevant in the context of data protection laws such as the GDPR and the Brazilian LGPD[26]. The standard outlines the requirements and guidelines for establishing, implementing, maintaining and continuously improving a Privacy Information Management System (PIMS). This makes it a valuable tool for organisations aiming to improve their data protection practices and achieve compliance with international privacy standards. ISO 27701 provides a structured approach to managing personal data, integrating privacy management into existing information security management

[22] Joris van Hoboken and R. Fathaigh, "Smartphone Platforms as Privacy Regulators," *Computer Law and Security Review* 41 (2021), https://doi.org/10.1016/j.clsr.2021.105557.

[23] Sheshadri Chatterjee and Demetris Vrontis, "Usage of Smartphone for Fi Nancial Transactions : From the Consumer Privacy Perspective" 2, no. September 2021 (2023): 193–208, https://doi.org/10.1108/JCM-03-2021-4526.

[24] Huairong Huo et al., "An Accelerated Method for Protecting Data Privacy in Financial Scenarios Based on Linear Operation," *Applied Sciences (Switzerland)* 13, no. 3 (2023), https://doi.org/10.3390/app13031764.

[25] Adinda Denisa, Muhamad Amirulloh, and Helitha Novianty Muchtar, "Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik," *Rechtsvinding* 12, no. 2 (2023): 167–84; Zandra Azelia Savitri, Muhamad Amirulloh, and Mei Susanto, "Urgensi Sertifikat Keandalan Privasi Dalam Menghadapi Kebocoran Data Pribadi The Urgency of Reliability Certificates in the Face of Personal Data Leaks," *Jurnal USM Law Review* 8, no. 1 (2025): 235–53.

[26] Almeida. Cícero, José, Albano., P., "Lei Geral de Proteção de Dados: Uma Análise Da ISO 27701 Como Ferramenta de Controle Para LGPD," *Revista Ifes Ciência*, 2024, https://doi.org/10.36524/ric.v10i1.2445;

systems (ISMS) based on ISO/IEC 27001 and 27002.[27]. ISO 27701 certification is carried out by private conformity assessment bodies, offering a competitive alternative to other certification schemes such as GDPR Article 42/43 certification. The adoption of ISO 27701 could affect the data protection certification market, potentially prompting regulatory bodies to clarify their stance on ISO standards[28].

3. CONCLUSION

PBI PKBI and PADG PKBI has harmonized with the PDP Law, the P2SK Law and SPK Law because it has regulated the obligation to use a personal data security system, with grammatical, systematic and teleological legal interpretation of the provisions of the privacy reliability certificate contained in the ITE Law and PP PSTE. However, the existing PADG PKBI has not at all in accordance with the SPK Law and PBSSN Common Criteria, because in particular, has not set SNI ISO 15408-2, 15408-3, or 15408-5 as the referred technical standard. Based on regulatory harmonization said above, the obligation of privacy certification is mandatory for the financial sector.

The PKBI PADG must be revised to be more in line with the PDP Law, the P2SK Law, the SPK Law and PBSSN Common Criteria by stipulating SNI ISO 15408-2, 15408-3, or 15408-5 as the technical reference standard, so that financial sector business actors under BI can implement it. Financial sector business actors under BI should apply a privacy reliability certificate as regulated by PBSSN Common Criteria or other standards based on best practices in securing personal data so that they are categorized as business actors with good faith and can be protected by law from excessive liability and free from criminal sanctions in the SPK Law.

ACKNOWLEDGEMENTS (OPTIONAL)

We would like to express our gratitude to Bank Indonesia and Bank Indonesia Institute for providing the costs for this research. We also express our thanks to the Financial Sector Business Actors who have been informants in interviews and FGDs, and the Chancellor of Universitas Padjadjaran who has given us permission to carry out research.

REFERENCES

Afdal Yanuar, Muh. "Laundering of Proceeds Forest Destruction and Narcotics Crimes: A Resolution of The Conflict Norms." *Mulawarman Law Review* 8, no. 1 (2023): 1–20. https://doi.org/https://doi.org/10.30872/mulrev.v8i1.1044.

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 (2022): 323–52. https://doi.org/10.21098/jcli.v1i2.19.

Amelia, Tina, Nunung Rahmania, and Aftab Haider. "Legal Protection of Personal Data

[27] Fal. O., M., "Documentation in the ISO/IEC 27701 Standard.," *Cybernetics and Systems Analysis* 57, no. 5 (2021): 796–80, https://doi.org/10.1007/S10559-021-00404-3; Svetlana A. Grishaeva, "Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019," 2021, 198–200, https://doi.org/10.1109/itqmis53292.2021.9642925.

[28] Eric, Lachaud., 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification.', *European Data Protection Law Review*, 6.2 (2020), 194–210 < https://doi.org/10.21552/EDPL/2020/2/7 >

as Listed in Court Decision : A Discourse Renewal." *Jurnal IUS Kajian Hukum Dan Keadilan* 12, no. 3 (2024).

Andikatama, Achmad Zulfa, and Bambang Eko Turisno. "Consumer Protection Law in the Digital Era." *International Journal of Social Science and Human Research* 7, no. 07 (2024). https://doi.org/10.47191/ijsshr/v7-i07-03.

Arimba, Cahya Iradi. "Hans Kelsen's Nomostatics and Nomodinamics Legal Theory." *Justice Voice*, 2024. https://doi.org/10.37893/jv.v2i2.773.

Bernazuk, I. "APPLICATION OF THE LEX SPECIALIS PRINCIPLE TO SOLVING CONFLICTS IN LEGISLATION: ANALYSIS OF COURT PRACTICE." *Slovo of the National School of Judges of Ukraine.* 38–39, no. 1–2 (2022): 69–82. https://doi.org/https://doi.org/10.37566/2707-6849-2022-1-2(38-39)-7.

Bisht, Divya. "Kelsen's Pure Theory of Law: An Overview." *International Journal for Research in Applied Science and Engineering Technology*, 2023. https://doi.org/10.22214/ijraset.2023.49679.

Brito, Ícaro Fellipe Alves Ferreira De. "INTERPRETATION OF LAW AND THE KELSENIAN INTERPRETIVE FRAMEWORK." *ARACÊ*, 2024. https://doi.org/10.56238/arev6n3-138.

Chatterjee, Sheshadri, and Demetris Vrontis. "Usage of Smartphone for Fi Nancial Transactions : From the Consumer Privacy Perspective" 2, no. September 2021 (2023): 193–208. https://doi.org/10.1108/JCM-03-2021-4526.

Cícero, José, Albano., P., Almeida. "Lei Geral de Proteção de Dados: Uma Análise Da ISO 27701 Como Ferramenta de Controle Para LGPD." *Revista Ifes Ciência*, 2024. https://doi.org/10.36524/ric.v10i1.2445.

Denisa, Adinda, Muhamad Amirulloh, and Helitha Novianty Muchtar. "Sertifikat Keandalan Privasi Sebagai Salah Satu Bentuk Pelindungan Konsumen Di Bidang Informasi Dan Transaksi Elektronik." *Rechtsvinding* 12, no. 2 (2023): 167–84.

Eric, Lachaud. "ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification." *European Data Protection Law Review* 6, no. 2 (2020): 194–210. https://doi.org/10.21552/EDPL/2020/2/7.

Fanani, Ahmad, and Muhammad Sulthon Zulkarnain. "Understanding John Austin's Legal Positivism Theory and Hans Kelsen's Pure Legal Theory." *Peradaban Journal of Law and Society*, 2022. https://doi.org/10.59001/pjls.v1i2.41.

Grishaeva, Svetlana A. "Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019," 198–200, 2021. https://doi.org/10.1109/itqmis53292.2021.9642925.

Hoboken, Joris van, and R. Fathaigh. "Smartphone Platforms as Privacy Regulators." *Computer Law and Security Review* 41 (2021). https://doi.org/10.1016/j.clsr.2021.105557.

Huo, Huairong, Jiangyi Guo, Xinze Yang, Xinai Lu, Xiaotong Wu, Zongrui Li, Manzhou Li, and Jinzheng Ren. "An Accelerated Method for Protecting Data Privacy in Financial Scenarios Based on Linear Operation." *Applied Sciences (Switzerland)* 13, no. 3 (2023). https://doi.org/10.3390/app13031764.

Indonesia, Bank. "Keuangan Inklusif." Bank Indonesia, 2020. https://www.bi.go.id/id/fungsi-utama/stabilitas-sistem-keuangan/keuangan-inklusif/Default.aspx#floating-3.

Kraevsky, A. "Validity and Efficacy of International Law According to the Pure Theory of Law." *Vestnik of Saint Petersburg University. Law*, 2021. https://doi.org/10.21638/spbu14.2021.113.

Leheza, Y., Reznykova, M., Korniakova, T., Lytvyn, O., & Komashko, V. "Understanding the Interpretation of Legal Standards: Theoretical, Administrative, Criminal, Financial Aspects." *Revista Do Curso de Direito Do UNIFOR.*, 2023. https://doi.org/https://doi.org/10.24862/rcdu.v14i2.1828.

Mihaela, Cristina. "Consumer Protection in The New Digital Decade." *SALCĂ ROTARU* 1, no. 1 (2024). https://doi.org/10.69971/x5yf2150.

Naiborhu, Mesa Indra, and Wagiman. "THE FUNDAMENTAL POSITION OF LEX POSTERIOR DEROGAT LEGI PRIORI IN THE CONFLICT OF NORMS AGAINST THE RIGHTS OF HOLDERS OF THE RIGHT TO JUSTICE." *Jurnal Indonesia Sosial Teknologi* 5, no. 2 (2024): 659–71. https://doi.org/10.59141/jist.v5i2.906.

O., M., Fal. "Documentation in the ISO/IEC 27701 Standard." *Cybernetics and Systems Analysis* 57, no. 5 (2021): 796–80. https://doi.org/10.1007/S10559-021-00404-3.

Olha, Merdova, Estudios Pol, Humberto J La Roche, and Ciencias Jur. "Interpretation of Legal Norms in Modern Jurisprudence." *Cuestiones Políticas* 41, no. 77 (2023): 298–308. https://doi.org/https://doi.org/10.46398/cuestpol.4177.20.

Risal, Abdul. "Jurnal Hukum Bisnis Bonum Commune Legal Protection for Debtors in Online Transactions : Evaluating Safeguards in E-Commerce" 7, no. 1 (2024): 176–87. https://doi.org/10.30996/jhbbc.v7i2.11656.

Savitri, Zandra Azelia, Muhamad Amirulloh, and Mei Susanto. "Urgensi Sertifikat Keandalan Privasi Dalam Menghadapi Kebocoran Data Pribadi The Urgency of Reliability Certificates in the Face of Personal Data Leaks." *Jurnal USM Law Review* 8, no. 1 (2025): 235–53.

Seredyuk, O. Bogdan V. "Neo-Kantian Epistemological Basis of Hans Kelsen's Pure Theory of Law." *Scientific Bulletin of Uzhhorod National University. Series: Law* 4, no. 8 (2025): 177–84. https://doi.org/https://doi.org/10.24144/2307-3322.2025.88.4.27.

Strzelecki, Artur, and Mariia Rizun. "Consumers' Security and Trust for Online Shopping after GDPR: Examples from Poland and Ukraine." *Digital Policy, Regulation and Governance* 22, no. 4 (2020): 289–305. https://doi.org/10.1108/DPRG-06-2019-0044.

Sulistio, Dimas, Eman Suparman, and Muhamad Amirulloh. "Information Security Management System : Electronic Apostille System Security to Ensure Legal Certainty across National Borders." *International Journal of Data and Network Science* 9, no. 4 (2025): 881–90. https://doi.org/10.5267/j.ijdns.2025.1.004.

Triyanti, Ninuk, I Gusti Ayu, Ketut Rachmi, and Lego Karjoko. "Legal Gaps in Personal Data Protection : Reforming Indonesia ' s Population Administration Law." *Hasanuddin Law Review* 11, no. 1 (2025): 132–47. https://doi.org/10.20956/halrev.v11i1.6177.

Vasquez, Jaime Damian. "Iso/Iec 27000." *HT, High Tech Engineering Journal*, 2023, 80–84. https://doi.org/https://doi.org/10.46363/high-tech.v3i2.3.

Vranes, E. "The Definition of 'Norm Conflict' in International Law and Legal Theory." *European Journal of International Law.* 17, no. 2 (2006): 395–418. https://doi.org/https://doi.org/10.1093/ejil/chl002.

Wibowo, Ari, and Widya Alawiyah. "The Importance of Personal Data Protection in Indonesia ' s Economic Development." *Cogent Social Sciences* 10, no. 1 (2024). https://doi.org/10.1080/23311886.2024.2306751.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130.