Vol. 7, No. 4, April 2026
E-ISSN:2723 – 6692 P-ISSN:2723– 6595
http://jiss.publikasiindonesia.id/

Personal Data Protection in the Banking Sector from the Perspective of Contextual Integrity: An Analysis on the Privacy Policies of State-Owned Banks

Arbain*, Dimas Fiancheto, Romadhon, Jane Latifarah Sriadi
Universitas Al-Azhar Indonesia, Indonesia
Email: arbain.2012@gmail.com*, difiancheto@gmail.com, janelatifarah2102@gmail.com, romaromadhon47@gmail.com

Keywords:
Personal Data Protection; Banking Sector; Contextual Integrity; Privacy Policy.

Abstract

The banking sector is structurally dependent on the continuous collection and processing of personal data, making data governance an inherent component of banking operations rather than a discretionary practice. This study examines personal data protection in the Indonesian banking sector by applying Helen Nissenbaum's theory of Contextual Integrity as a normative analytical framework. Using a normative juridical approach and qualitative textual analysis, the research analyzes the privacy policies of four state-owned banks Bank Mandiri, BRI, BTN, and BNI to assess how norms governing information flows are articulated at the policy level. The analysis focuses on five core elements of Contextual Integrity: social context, actors and social relations, data attributes, transmission principles (purposes), and the integrity of contextual boundaries across data uses. The findings show that privacy policies in state-owned banks largely function as instruments of formal legal compliance rather than as normative statements clarifying the appropriateness of information flows within the banking context. While purposes of data processing are relatively explicit, multiple processing contexts such as core banking services, digital platforms, and marketing activities are often aggregated without clear normative boundaries. This weakens the articulation of trust-based norms and increases the risk of context collapse, particularly in relation to secondary uses of customer data.

INTRODUCTION

The banking sector is one of the most intensive sectors in the collection, processing, and exchange of personal data. From the beginning, banking functions cannot be separated from the management of customer data, ranging from identities, financial transactions, risk profiles, to financial behavior patterns. The development of information technology and the digitalization of financial services has significantly expanded banks' capacity to collect, process, and integrate data at scale, across systems (Abubakar et al., 2024). This transformation is part of a broader social change, where information technology is changing the structure and dynamics of information flows in modern life.

The personal data protection framework that has developed so far generally relies on two main approaches, namely privacy as *secrecy* and privacy as individual control over personal data (*control-based privacy*) (Gstrein & Beaulieu, 2022). Such an approach assumes that privacy protection can be guaranteed through restrictions on access to data or through the consent of the data subject. However, in a social practice characterized by complex and interconnected information systems, this approach is increasingly difficult to explain why

certain data processing practices arouse public resistance even though they are legally and procedurally feasible.

In the banking sector, the limitations of this approach are very real. The processing of personal data in banking is structural and not entirely optional, as the financial system cannot function without continuous data processing. Therefore, individual consent often loses its substantive meaning as the primary instrument of privacy protection. As an institution that has systemic risks and a strategic role in the economy, banks operate in a distinctive social context. The relationship between banks and customers is not only contractual, but also contains a *high level of trust-based relationship* and due diligence (Lappeman et al., 2023).

In addition, banks play an important role in maintaining the stability of the financial system and protecting the interests of the broader public (Boissay et al., 2021). In this context, the legitimacy of the processing of personal data is determined not solely by formal compliance with the law, but also by the conformity of the practice with the social norms inherent in the banking context. The *contextual integrity* theory developed by Helen Nissenbaum offers a relevant conceptual framework for understanding such tensions. Instead of defining privacy as the absence of information flow, this theory understands privacy as guarding the appropriate *flow of information* in a given social context (Nissenbaum, 2019). In this framework, a data flow is considered legitimate or invalid not solely based on consent or a formal legal basis, but based on its conformity with the norms of the social context that govern who can know what, under what conditions, and for what purpose.

For the banking sector, this perspective is very important because the banking context is characterized by strong and relatively stable norms. These norms reflect what Nissenbaum calls *informational norms*, which are normative expectations that determine the appropriateness of the flow of information in a social context (Malkin et al., 2023). This understanding is in line with the view that privacy is a relational and social phenomenon, not merely an individual right that stands alone. In the context of banking, this norm serves as a barrier against the tendency to treat personal data as an economic commodity that can be exploited across contexts.

The relevance of *contextual integrity theory* is increasing in the era of banking collaboration with third parties, *fintech*, and the broader digital ecosystem (Wang et al., 2020). System integration and service outsourcing increase the risk of shifting data processing contexts that are not always detected through formal legal compliance tests. In this situation, public trust in banks is highly dependent on the institution's ability to demonstrate that its data governance is not only law-abiding, but also maintains the integrity of the banking social context.

Thus, the banking sector needs to understand *contextual integrity* theory not just as a philosophical discourse, but as a normative perspective that bridges personal data protection laws, institutional governance, and public expectations. This perspective allows banks to develop privacy policies and data management practices that are not only legally valid, but also socially legitimate, because they are rooted in contextual norms that are the basis of public trust in the banking system itself.

In the last five years, research on personal data protection in the banking sector has mainly developed within the framework of legal compliance and digital risk governance (Hornuf et al., 2023). A number of studies explicitly examine the application of personal data protection principles in digital banking and *open banking*, especially related to *lawful basis*, the division of roles *of data controllers* and *data* processors, and customer data protection obligations in the

banking data sharing ecosystem (Briones de Araluze & Cassinello Plaza, 2022). Other research links the protection of personal data to customer trust and the sustainability of digital banking businesses, but tends to position privacy as an instrument of reputation and regulatory compliance, rather than as an autonomous social norm (Martínez-Navalón et al., 2023). In addition, studies on banks' collaboration with fintech's highlight the increased risk of data leaks and the complexity of cross-actor legal liability, but generally still limit analysis to *cybersecurity* and technical accountability issues. Different from the previous research, the novelty of this journal lies in the use of *contextual integrity* theory as a framework to assess (Shvartzshnaider et al., 2019) *privacy policy* in the banking sector. Based on this background, this research is focused on two problem formulations, namely what are the problems of *privacy policy* in the banking sector (case study of SOE Banks) and how to improve *privacy policy* in the banking sector from the perspective of *contextual integrity theory*.

The purpose of this research is to examine personal data protection in the Indonesian banking sector by applying Helen Nissenbaum's theory of Contextual Integrity as a normative analytical framework. The specific objectives are: (1) to identify problems in privacy policies of state-owned banks using the five CI core elements; (2) to assess the quality of normative statements in privacy policies regarding information flow propriety; (3) to compare articulation levels across four state-owned banks; and (4) to formulate recommendations for improving privacy policies from a contextual integrity perspective. The contribution of this research is to provide a theoretically grounded and operationally applicable framework for assessing banking privacy policies beyond formal compliance. The benefits of this research extend to banks (guidance for improving privacy policies), regulators (evaluative framework for assessing compliance substance), legal scholars (application of CI theory to banking context), and customers (understanding of what constitutes appropriate data protection norms).

METHOD

This study used a normative juridical approach with the character of qualitative-descriptive analysis, which places banking privacy policy as the main object of study. This approach was chosen because the focus of the research is not directed at empirical testing of the factual practices of personal data processing, but rather at a normative assessment of how the flow of information and the protection of personal data is formulated in official banking policy documents (Zimmer, 2018), particularly in the perspective of *Contextual Integrity theory*.

This type of research is *library research*, with primary materials in the form *of privacy policies* of four state-owned banks, namely Bank Mandiri, Bank Rakyat Indonesia (BRI), Bank Tabungan Negara (BTN), and Bank Negara Indonesia (BNI) which are announced on the websites of each bank. In addition, there are also laws and regulations related to personal data protection and the banking sector, as well as secondary legal materials in the form of doctrine, academic literature, and scientific works relevant to privacy theory.

The analysis approach used is normative-textual analysis, by placing *the privacy policy* as a policy text that contains normative statements regarding the processing of personal data. Within this framework, the study does not assess the effectiveness of policy implementation, factual compliance levels, or data breach incidents, but rather analyzes the extent to which the

privacy policy explicitly and coherently reflects the norms of information flow propriety in the social context of banking.

For this purpose, this study uses the *theory of Contextual Integrity* developed by Helen Nissenbaum as the main analytical framework. This theory is operationalized through five core elements, namely: (1) the social context of data processing, (2) actors and social relations, (3) attributes or types of personal data, (4) the principle of transmission or purpose of processing, and (5) the integrity of the context. These five elements are used as analytical indicators to assess the quality of normative statements in (Shaffer, 2021) *privacy policies*, not as an instrument for legal compliance audits or technical evaluations of data management systems.

RESULTS AND DISCUSSIONS

1. The Problem of Personal Data Protection in the Banking Sector on the Aspect of Privacy Policy (Case Study of State-Owned Banks)

Based on the ***Contextual Integrity*** framework above, the author conducted a comparative analysis of the privacy policies of four state-owned banks to identify general patterns, differences in articulation levels, and institutional tendencies in formulating personal data protection. With this approach, the discussion is not directed at assessing factual compliance or implementation effectiveness, but rather at the quality of the normative statement of the privacy policy in reflecting the social context of data processing as referred to in *the theory of Contextual Integrity*.

Analysis of the privacy policies of four state-owned banks shows that in general, privacy policies have functioned as an instrument of legal compliance and institutional communication, but the level of articulation of information flow norms as referred to in the (Degutis et al., 2023) ***Contextual Integrity theory*** still varies between banks and between elements. The difference does not lie in the presence or absence of formal legal arrangements, but in the extent to which the privacy policy explicitly and coherently states the social context of the data processing, the actors involved, the type of data processed, the purpose of the information flow, and the normative boundaries between processing contexts.

In the social context element, most banks tend to formulate (Ameen et al., 2021) *privacy policies* within one grand narrative framework of banking services without a firm separation between the core banking context, digital services, and marketing activities. This condition causes the context of data processing to often be expressed in general and aggregate. Among the four banks, BTN is relatively more explicit in linking data processing to certain banking functions such as *know your customer* (KYC), credit, and fraud prevention, while Bank Mandiri shows the least articulation of context.

In the element of actors and relationships, there is a stronger tendency to mention the parties involved in data processing, including subsidiaries, affiliates, regulators, and third parties. BRI and BNI are relatively more detailed in stating the relationship between actors, especially in the context of business groups and regulatory obligations, while Mandiri and BTN still tend to use general formulations such as "third party" or "related party" without an in-depth relational explanation.

The data attribute elements of the four banks are generally presented in the form of a broad and detailed list of data categories. However, from the perspective of *Contextual Integrity*, the completeness of the list is not always directly proportional to the normative power.

BRI and BNI show a higher level of clarity because they group data in categories that are relatively stable and consistent with the purpose of processing, while Mandiri and BTN still display a list of data that is descriptive and less associated with a particular context of use.

In the transmission principle element or processing destination, the entire bank is relatively stronger than the other element. The purposes of processing are generally explicitly stated, including banking services, regulatory compliance, risk management, and marketing. Nevertheless, differences arise at the level of destination specifications. BRI, BTN, and BNI tend to be more systematic in detailing processing purposes, while Mandiri still uses broad and cross-contextual objectives.

Meanwhile, the element of context integrity is the weakest element in general. While all banks acknowledge the possibility of cross-party and cross-functional data transfers or disclosures, there is little normative explanation for the limitations of data flows between processing contexts. In other words, privacy policies state more *that data* can be streamed, but have not consistently explained *within normative limits what* the transfer of context is justified.

Based on these findings, it can be concluded that the main difference between banks does not lie in formal compliance with personal data protection regulations, but in the quality of articulation of contextual norms in privacy policies.

To facilitate comparison and summarize the results of the analysis that have been described narratively, the following table presents the comparative assessment of the four state-owned banks based on the five core elements *of Contextual Integrity* on a scale of 1–3.

Table 1: Comparative Assessment of State-Owned Banks Based on the Five Elements *of Contextual Integrity*

CI Elements	Self-Sufficient	BRI	BTN	BNI
1. Social Context	1	2	3	2
2. Actors & Relationships	2	3	2	3
3. Data Attributes	2	3	2	3
4. Transmission Principle (Purpose)	2	3	3	3
5. Context Integrity	1	2	2	2

Brief Explanation per Bank (concise & defensible)

a) Bank Mandiri

Mandiri tends to use one large narrative of "Bank Mandiri's products and/or services" without a firm separation between contexts (core banking, digital, marketing), so that the social context and the integrity of the context are weak (value 1). Actors, data, and objectives are indeed mentioned, but they are still aggregate and cross-contextual, so most elements are at the level of "generally stated".

b) Bank BRI

BRI shows the most systematic level of articulation. BRI's privacy notice document explicitly distinguishes between data sources, objectives, actors (including BRI Group and regulators), and profiling mechanisms, so that it is strong on actors & relationships, data attributes, and processing objectives (value 3). However, the boundaries of data flow between contexts are still generally stated, so the integrity of the context is not yet fully normative.

c) Bank BTN

BTN explicitly states the purpose of processing based on banking functions (KYC, credit, fraud, services, marketing), so that the social context and transmission principle are relatively clear (value 3). However, actors, data attributes, and cross-contextual boundaries are still presented descriptively and broadly, so they are at a sufficient level (2).

d) Bank BNI

BNI has a neat and legalistic privacy notice structure, with detailed explanations of actors, business groups, data, objectives, and legal basis, so that it is strong on actors & relationships, data attributes, and processing purposes (value 3). However, like BRI and BTN, normative boundaries between contexts (e.g. from services to marketing or profiling) are still generally stated.

2. Improving Personal Data Protection in the Banking Sector in the Perspective of *Contextual Integrity Theory*

Analysis of banking privacy policies shows that *privacy policies* are generally still positioned as formal compliance instruments with personal data protection laws and regulations (Degeling et al., 2019). This approach emphasizes the legality of the processing and consent of the data subject, but has not fully made a privacy policy a normative statement about the propriety of the flow of information in a given social context. In the perspective of *Contextual Integrity* (CI) theory, privacy is not determined solely by confidentiality or consent, but rather by the conformity of the flow of information with the contextual norms inherent in a social practice.

Improving the banking *privacy policy* needs to start from the affirmation of the social context of personal data processing. In CI theory, every social practice including banking has its own purpose, role, and normative expectations that shape the context of data processing. However, many banking privacy policies still use a single common narrative of "banking services" or "products and/or services", without distinguishing between the core banking context (such as KYC and transactions), digital services, and marketing activities. This ambiguity has the potential to blur the boundaries of the appropriateness of the information flow because the norms that apply in one context are not necessarily valid when applied in another.

In addition to context, improvements are also needed in the aspect of actors and data processing relationships. CI emphasizes that information flows always involve specific social roles senders, receivers, and data subjects each of which carries different normative expectations. In the banking *privacy policy*, actors such as subsidiaries, affiliates, partners, and third parties are often referred to in an aggregate manner, without a clear explanation of the relationship and the limits of authority. As a result, it is difficult for data subjects to understand to whom the data flows and in what social relations the transfer is considered appropriate.

The next aspect is the personal data attribute. Many banking privacy policies list very broad and general categories of data. From CI's point of view, the privacy issue does not lie in the amount of data collected, but in the suitability of the type of data with the context and purpose of the processing. Therefore, the improvement of *the privacy policy* requires the formulation of data attributes in a more contextual and proportional manner, not just an inventory of personal data.

In terms of the principle element of transmission or processing purposes, *the banking privacy policy* is relatively more explicit, but still tends to formulate objectives broadly and across contexts. In CI, the principle of transmission serves as a normative justification for the flow of information, not just a formal legal basis. Without a clear link between purpose and social context, the purpose of the processing has the potential to expand (Lom et al., 2024; *purpose creep*) and substantially weaken privacy protections.

The most crucial improvement has to do with the integrity of the context. CI asserts that privacy breaches often occur not because data is collected unlawfully, but because data flows into other contexts without adequate normative justification. In many banking *privacy policies*, the possibility of data disclosure or transfer is acknowledged, but the normative boundaries between contexts are rarely explicitly stated. As a result, the privacy policy fails to provide clarity as to when and within what extent the transfer of the context of data processing can be justified.

Thus, it is not enough to improve *privacy policy* in the banking sector through the addition of legal clauses or the expansion of the processing basis. What is needed is a shift in approach from formal compliance to a clearer articulation of contextual norms. The *Contextual Integrity* perspective provides a conceptual framework for pushing *privacy policy* into a normative transparency instrument, enabling data subjects to understand and assess the appropriateness of information flows in modern banking practices.

CONCLUSION

Based on the analysis of the privacy policies of four state-owned banks using the perspective of *Contextual Integrity theory*, it can be concluded that privacy policies in the Indonesian banking sector in general have functioned as an instrument of formal compliance with personal data protection regulations. However, the privacy policy has not fully functioned as a normative statement that clearly and coherently articulates the appropriateness of the flow of information in the social context of banking. Most privacy policies are still structured in an aggregate and legalistic manner, with a tendency to obscure the differences in the context of data processing, relationships between actors, and normative boundaries between banking, digital services, and marketing functions. The findings of the study show that the difference in the quality of privacy policies between state-owned banks does not lie in the existence or absence of the legal basis for data processing, but in the level of clarity of contextual statements regarding the flow of information. The element of the processing purpose is relatively more explicit than the other, while the element of contextual integrity i.e., the limitation of the flow of data between contexts is the weakest aspect in general (Sanfilippo et al., 2020). This condition indicates that the approach to personal data protection in the banking sector is still oriented towards minimal normative compliance, not fully adopting a substantive approach that places privacy as a matter of social propriety. Thus, this study confirms that *the theory of Contextual Integrity* is relevant and operational to assess privacy policy as a policy text, while revealing the limitations of the personal data protection approach that relies too much on formal consent and legality. Privacy policies that do not clearly state the social context and boundaries of information flow risk undermining data subjects' understanding of how and in what context their personal data is processed.

REFERENCE

Abubakar, M., Hasan, R., & Abubakar, M. H. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 144*, 103560. https://doi.org/10.1016/j.cose.2024.103560

Aldboush, H. H., & Ferdous, M. (2023). Building trust in FinTech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies, 11*(3), 90. https://doi.org/10.3390/ijfs11030090

Ameen, N., Tarhini, A., Reppel, A., & Anand, A. (2021). Customer experiences in the age of artificial intelligence. *Computers in Human Behavior, 114*, 106548. https://doi.org/10.1016/j.chb.2020.106548

Boissay, F., Ehlers, T., Gambacorta, L., & Shin, H. S. (2021). Big techs in finance: On the new nexus between data privacy and competition. In D. Zetzsche, R. Buckley, & D. Arner (Eds.), *FinTech Handbook* (pp. 855–875). Springer. https://doi.org/10.1007/978-3-030-65117-6_31

Borges, André, dan Fernando Laurindo. (2022). Privacy and data protection in digital banking: Impacts on customer trust. *International Journal of Bank Marketing, 40*(6), 1231–1250.

Briones de Araluze, I., & Cassinello Plaza, N. (2022). Open banking: A bibliometric analysis-driven definition. *Heliyon, 8*(10), e10641. https://doi.org/10.1016/j.heliyon.2022.e10641

Cohen, Julie E. (2013). What privacy is for. *Harvard Law Review, 126*, 1904–1933.

Cohen, Julie E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy… now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2019)*. Internet Society. https://doi.org/10.14722/ndss.2019.23378

Degutis, M., Urbanavičius, S., Hollebeek, L. D., & Anselmsson, J. (2023). Consumers' willingness to disclose their personal data in e-commerce: A reciprocity-based social exchange perspective. *Journal of Retailing and Consumer Services, 74*, 103385. https://doi.org/10.1016/j.jretconser.2023.103385

Gillis, Tommaso, dan Colin McInnes. (2020). Data protection and open banking: Regulatory challenges and compliance strategies. *Computer Law & Security Review, 36*, 105392.

Gillis, Tommaso, et al. (2021). Data governance and accountability in FinTech–Bank partnerships. *Journal of Banking Regulation, 22*(4), 321–336.

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology, 35*(1), 1–38. https://doi.org/10.1007/s13347-022-00497-4

Hornuf, L., Momtaz, P. P., Nam, R., & Bhatt, D. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets, 33*(1), 33. https://doi.org/10.1007/s12525-023-00622-x

Lappeman, J., Marlie, S., Johnson, T., & Patel, T. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing, 28*, 337–357. https://doi.org/10.1057/s41264-022-00154-z

Lom, H. S., Thoo, A. C., Lim, W. M., & Koay, K. Y. (2024). Advertising value and privacy concerns in mobile advertising: The case of SMS advertising in banking. *Journal of Financial Services Marketing, 29*(3), 1135–1153. https://doi.org/10.1057/s41264-023-00240-6

Malkin, N., Wijesekera, P., Egelman, S., & Wagner, D. (2023). Contextual integrity, explained. *IEEE Security & Privacy, 21*(1), 28–38. https://doi.org/10.1109/MSEC.2022.3218081

Martínez-Navalón, J.-G., Fernández-Fernández, M., & Pedrosa Alberto, F. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? *International Entrepreneurship and Management Journal, 19*(2), 781–803. https://doi.org/10.1007/s11365-023-00839-4

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law, 20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology, 71*(9), 1002–1013. https://doi.org/10.1002/asi.24327

Shaffer, G. (2021). Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy, 11*, 222–265. https://doi.org/10.5325/jinfopoli.11.2021.0222

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis. *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing, 7*(1), 162–170.

Wang, H., Ma, S., Dai, H.-N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with nudge theory in open banking. *Future Generation Computer Systems, 110*, 812–823. https://doi.org/10.1016/j.future.2019.09.010

World Bank. (2021). *Financial consumer protection and data governance*. Washington, DC: World Bank.

Zimmer, M. (2018). Addressing conceptual gaps in big data research ethics: An application of contextual integrity. *Social Media + Society, 4*(2), 1–12. https://doi.org/10.1177/2056305118787083