Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022
ISSN: 2747-2604
Volume 7 No. 3, September 2025, (450-459)

Implementation of the Principles of Necessity and Proportionality in the Sharing of Customer Data by Banks with Vendors

Nandani Bayu Prasanti[1)] & Ariawan Gunadi[2)]
[1)]Faculty of Law, Universitas Tarumanagara, E-mail: Indonesia, nandani.207241020@stu.untar.ac.id
[2)] Faculty of Law, Universitas Tarumanagara, Indonesia, E-mail: ariawang@fh.untar.ac.id

Abstract. *In the era of digital transformation in the banking sector, there has been an increasing practice of sharing customer data with third parties, such as service providers or vendors. This practice poses legal challenges, particularly concerning the fulfillment of the principles of necessity and proportionality in the protection of personal data. This study aims to analyze the implementation of these two principles in the collaborative practices between banks and vendors regarding the protection of customers' personal data. This normative juridical research employs a conceptual and statutory approach, using legal materials obtained from national and international regulations, academic journals, and best practices in the banking sector. The findings indicate the need for clear and comprehensive internal bank policies on personal data protection in third-party data processing, serving as a guideline to ensure compliance with personal data protection principles.*

Keywords: *Bank; Data; Necessity; Personal; Protection.*

1. Introduction

Human beings are dynamic creatures who continuously strive to survive from one era to another (Marius, 2006). Each period is generally marked by innovations that bring significant changes to human ways of working. When humans utilize tools and their cognitive abilities to simplify life, it is known as technology (Al, 2023). A radical transformation in how humans produce goods and services driven by technological advancement is referred to as the Industrial Revolution (Fernando & Fahruddin, 2023).

Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022
ISSN: 2747-2604
Volume 7 No. 3, September 2025, (450-459)

At present, humanity has experienced four stages of the Industrial Revolution. The Fourth Industrial Revolution is characterized by the emergence of the Internet of Things (IoT), Artificial Intelligence (AI), Big Data, and Cloud Computing. The Internet of Things refers to the ability of surrounding devices or electronic tools to be continuously connected to the internet and exchange data in real time (Hardiyanti, 2024). This continuous connectivity generates large, fast, and diverse data sets known as big data.

Initially, data only served as a record or historical archive for companies. However, today, data has become a valuable asset. In principle, data represents both value and risk. When data is well managed, producing high-quality information, it becomes valuable to a company supporting more effective policy or business strategies and improving operational efficiency (Prasad, 2024). Conversely, when data is poorly managed, leading to uncontrolled dissemination or loss of exclusivity, it poses risks such as data breaches, which can cause both financial and legal harm to companies (Ridho et al., 2024).

As institutions that are actively undergoing digital transformation, banks are required to establish proper data governance, including comprehensive data policies, and to ensure access control and data security (Rannie B, 2023). Although banks have legitimate interests in processing customer data as part of fulfilling their contractual relationships, such processing must be based on lawful and relevant purposes and conducted fairly. This is essential because personal data protection forms part of the constitutional right to privacy (Suwondo, 2022). Furthermore, banks may engage third parties (vendors) as data processors, making the supervision of compliance and data security even more critical.

Excessive justification for customer data usage must be avoided, as illustrated by the Data Retention Directive case in the European Union, where governments mandated the mass retention of communication data to prevent terrorism (Meškić & Samardžić, 2017). Although the policy had legitimate aims, it created a conflict between national security interests and the fundamental right to data protection. Therefore, it is necessary to further examine the extent to which the principles of necessity and proportionality have been implemented in the policies and practices of customer data management by banks in Indonesia.

2. Research Methods

This study employs a normative juridical method with a theoretical research approach, aiming to explore the legal theories and principles underlying regulations and practices of personal data protection in the management of customer data by banks (Gunardi, 2022). The approaches used in this study include: Conceptual approach, which seeks to understand the fundamental principles and theories of personal data protection: Statutory approach, which

examines the legal norms contained within the applicable positive laws; and Comparative approach, which analyzes and compares existing regulatory frameworks across different legal systems (Marzuki, 2017). The legal materials utilized consist of primary legal materials, namely statutory regulations, and secondary legal materials, including academic journals, books, and legal doctrines collected through library research. These are further supported by best practice interviews with data privacy experts in the banking sector.

3. Results and Discussion

3.1. The Application of the Principles of Necessity and Proportionality in Indonesia's Personal Data Protection Law

In principle, the protection of personal data constitutes a fundamental human right guaranteed by the Constitution (Iswandari, 2022). Article 28G of the Constitution of the Republic of Indonesia of 1945 (hereinafter referred to as the 1945 Constitution) states that:

"Every person shall have the right to protection of their personal self, family, honor, dignity, and property under their control, and shall have the right to feel secure and to be protected from the threat of fear to do or not to do something that is their right."

This article implicitly encompasses the right to privacy, which includes the right to personal data protection (right to personal data protection). Furthermore, the elucidation of Article 26 of Law No. 19 of 2016 concerning the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) stipulates that the protection of personal data forms part of privacy rights (Anggraeni, 2018). The right to privacy means that every individual has the right to be free from fear or insecurity due to unjustified interference (Tantimin et al., 2023). In the context of personal data protection, this right is understood as the right to informational self-determination, meaning that each individual has the right to know, control, and determine how their data is used (Wulansari, 2020).

When a data subject establishes a legal relationship with an institution or company and provides their personal data for processing within an information system, the control over such data no longer entirely rests with the data owner (Agusta, 2020). Consequently, a limitation arises over the fundamental right of the data subject to personal data protection. Therefore, the processing of personal data must adhere to the principles of necessity and proportionality to ensure that the processing is limited, lawful, and reasonable—not excessive (European Data Protection Supervisor, 2019).

The principle of necessity requires that the data being processed is genuinely needed to achieve a specific, legitimate purpose. Meanwhile, the principle of proportionality ensures and justifies that any limitation imposed on the right is balanced against the intended processing purpose, is not excessive, and does not infringe upon the rights of the data subject (DPO Centre, 2025). Hence, the rights of data subjects remain optimally protected, while the interests of data controllers are fulfilled in a reasonable and proportionate manner.

Article 52 of the Charter of Fundamental Rights of the European Union (CFR) provides that any limitation on the exercise of rights and freedoms recognized by the Charter must comply with the principle of proportionality, be necessary, and genuinely pursue objectives of general interest recognized by the European Union or the protection of the rights and freedoms of others. Article 52 of the CFR thus ensures that any restriction of privacy or personal data protection rights must pass the proportionality test, in which the necessity principle serves as a key parameter to determine that such limitation is carried out only to the extent required to achieve a legitimate purpose.

In the practice of the Court of Justice of the European Union (CJEU), the necessity test forms an inherent component of the proportionality test, which consists of several stages: legitimate objective, appropriateness, necessity, and reasonableness (Meškić & Samardžić, 2017). Within this test, the term “necessary” is not interpreted as the only means to achieve the processing objective, but rather as a proportionate means to achieve a legitimate goal (Black & Stevens, 2013). Therefore, personal data processing may be deemed “necessary” if it is genuinely required to achieve the agreed purpose and if no less intrusive alternative exists to accomplish that purpose (Black & Stevens, 2013).

The European Union serves as a pioneer in the field of personal data protection, as evidenced by the enforcement of the General Data Protection Regulation (GDPR) a comprehensive regulation governing personal data protection across the EU. Indonesia has also established its own legal framework for personal data protection through the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). The following section presents a comparison between the principles of necessity and proportionality as regulated under the PDP Law and the GDPR.

Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022
ISSN: 2747-2604
Volume 7 No. 3, September 2025, (450-459)

Table 1. Comparison of the Principles of Necessity and Proportionality under Indonesia's PDP Law and the EU GDPR

Aspect / Principle	Indonesia's Personal Data Protection Law (Law No. 27 of 2022)	General Data Protection Regulation (GDPR)	Analysis
Lawfulness, fairness, and transparency	**Article 16(2)(a)**: The collection of personal data shall be conducted in a limited and specific manner, lawfully, and transparently.	**Article 5(1)(a)**: Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.	Both provisions emphasize the **principle of proportionality**, in which data collection and processing must be limited, specific, and adequate. The main parameters of this principle are **suitability** and **reasonableness** (Ellis, 1999).
Purpose limitation	**Article 16(2)(b)**: The processing of personal data shall be carried out in accordance with its specified purpose.	**Article 5(1)(b)**: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.	Both provisions emphasize the **principle of purpose limitation**, which requires that personal data be collected for **specific and legitimate purposes** (Data Protection Commission, 2019). This principle reflects the application of **necessity**, as data may only be used when required for a legitimate purpose, while **proportionality** ensures that such purposes are not excessive.
Data minimization	**Article 21(1)**: In cases where data processing is based on consent, the data controller must provide information regarding: (a) the legality of the processing; (b) the purpose of processing; and (c) the type and relevance of personal data to be processed, etc.	**Article 5(1)(c)**: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (*data minimization*).	Substantively, both provisions reflect the **principle of data minimization**, emphasizing that data controllers may only collect **the minimum amount of data necessary**, and must not collect irrelevant data. Relevant data must be directly and reasonably related to the processing purpose and must not be excessive. This principle embodies **necessity**—data collection is limited to the agreed purposes—and **proportionality**, by protecting data subjects from excessive data collection, thus maintaining a balance between processing needs and privacy intrusion.
Storage limitation	**Article 16(2)(g)**: Personal data shall be destroyed and/or deleted after the retention period expires or upon the request of the data subject.	**Article 5(1)(e)**: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	Both provisions reflect the **principle of necessity**, as the duration of data retention is limited to the period necessary to achieve the processing purposes.
Integrity and confidentiality (security)	**Article 16(2)(e)**: The processing of personal data must ensure protection against	**Article 5(1)(f)**: Personal data shall be processed in a manner that ensures appropriate security,	Both provisions embody the **principle of proportionality**, as the level of protection must be **commensurate with the risks**

Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022
ISSN: 2747-2604
Volume 7 No. 3, September 2025, (450-459)

Aspect / Principle	Indonesia's Personal Data Protection Law (Law No. 27 of 2022)	General Data Protection Regulation (GDPR)	Analysis
	unauthorized access, disclosure, alteration, destruction, and/or loss of personal data.	including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (*integrity and confidentiality*).	associated with data processing. This principle ensures that data processing does not impose greater harm to the rights of data subjects than the benefits derived from such processing.

3.2. The Application of the Principles of Necessity and Proportionality in the Sharing of Customer Data by Banks with Vendors

In principle, the relationship between a bank and its customers is founded upon a fiduciary relationship based on trust (Usanti & Shomad, 2016). Since customers have entrusted their personal data to be processed by the bank, maintaining confidentiality is a fundamental obligation of the bank. However, in processing customer data, banks often face limitations in terms of expertise or infrastructure. Consequently, banks may involve third parties or vendors to support the implementation of banking services. These vendors may provide information technology services, cloud or server-based data storage, or skilled manpower, including data management support.

Referring to Article 51 paragraph (1) of the Personal Data Protection Act (UU PDP), a bank, as a personal data controller, may appoint a personal data processor such as a vendor to carry out personal data processing activities in accordance with the instructions of the controller. According to Article 1 point 5 of the Act, a personal data processor is defined as any individual, public body, or international organization acting independently or jointly in processing personal data on behalf of the personal data controller. As stated on the official website of Bank BTN, certain customer personal data may be managed, processed, and stored by third parties in cooperation with BTN for the provision of banking services, while maintaining compliance with access obligations and effectiveness as regulated by applicable laws and regulations (BTN, 2025).

Furthermore, the processing of personal data by affiliated companies and third parties is carried out in compliance with data protection requirements and only after the signing of cooperation and confidentiality agreements, in accordance with prevailing regulations and legislation (BTN, 2025). The necessity of a written contract or cooperation agreement as the legal basis for customer data processing aligns with Article 28(3) of the GDPR, which stipulates that data processing by a

processor must be governed by a valid contract that defines and binds the legal relationship between the data controller and the data processor.

Although the requirement for a written contract between data controllers and processors is not explicitly stated in the Personal Data Protection Act, the Act implicitly demands a legal instrument as the basis for processing activities. This can be inferred from Article 51 paragraph (1) of the PDP Act, which stipulates that a personal data processor must carry out data processing based on the instructions of the controller. This indicates the existence of a binding legal relationship, wherein the processor acts not independently, but under the lawful direction of the controller. To ensure such instructions are valid and accountable, they must be set forth in a written legal instrument namely, a cooperation agreement.

From a legal standpoint, the cooperation agreement between a bank and its vendor in the context of a data processing agreement (DPA) may be construed under the legal framework of an agency agreement. Pursuant to Article 1792 of the Indonesian Civil Code, an agency is defined as an agreement whereby one person grants authority to another to perform certain acts on their behalf (Subekti, 1995). In this case, the vendor acts solely on the bank's instructions, meaning that the vendor receives the authority from the bank to process the customer's personal data.

Based on an interview with Mr. Andri Irwanza Humardhani, Head of the Data Privacy Department at Bank BTN, the bank has established an adequate framework for processing customer personal data that aligns with the PDP Act and supports the application of the principles of necessity and proportionality. The framework includes the following elements:

1. Appointment of a Data Protection Officer (DPO) in accordance with Article 53 paragraph (1) of the PDP Act. The DPO is responsible for overseeing compliance with data protection principles and mitigating risks of personal data breaches.
2. Third Party Risk Assessment (TPRA) is conducted before entering into any cooperation with vendors. The TPRA aims to evaluate and monitor risks related to third-party partnerships to ensure that the third party complies with prevailing standards and regulations through several assessment parameters. This procedure supports the principle of proportionality, ensuring that the risks borne by data subjects do not exceed the intended purpose of data processing.
3. In cases where vendors require access to banking data (including customer data) to perform their duties, such requests must be submitted or represented by an organic employee of Bank BTN. This ensures that all

data access remains under the supervision and responsibility of the bank as the data controller. Vendor access to customer data is limited only to information that is necessary for fulfilling the processing purpose as stipulated in the cooperation agreement, applying the need-to-know and least privilege principles to minimize risks of misuse or data leakage.

4. A data sharing protocol has been implemented to regulate the review process for every data request. This protocol ensures that each request has a valid legal basis and that the data requested is relevant to the processing purpose. The review process involves the Compliance, Risk Management, and IT Security units to ensure adherence to the principles of necessity and proportionality in personal data protection.

5. The bank has established clear policies regarding data retention and disposal for data managed by third parties. When the retention period expires, as determined by internal policies, cooperation agreements, or government regulations, third parties are required to permanently dispose of the data to prevent future access or recovery. The disposal process must be documented in a Data Disposal Report, which is then reviewed by internal BTN staff. This mechanism aligns with the principles of storage limitation and necessity, ensuring that data is retained only for as long as it has a lawful processing basis and remains necessary to achieve the intended purpose.

4. Conclusion

Both the Indonesian Personal Data Protection Act (PDP Law) and the General Data Protection Regulation (GDPR) are rooted in the same paradigm that personal data processing must be conducted only to the extent necessary to achieve the intended purpose (necessity) and in a manner that is limited, balanced, and not excessive (proportionality). The principles of necessity and proportionality serving as fundamental parameters in personal data protection within the European Union originate from Article 52 of the Charter of Fundamental Rights of the European Union (CFR) and are explicitly articulated in several provisions of the GDPR, such as Article 23(1). In practice, the Court of Justice of the European Union (CJEU) applies a multi-layered proportionality test encompassing the stages of appropriateness, necessity, and reasonableness to ensure that any restriction on the right to privacy remains balanced with the legitimate objectives pursued. In contrast, the Indonesian PDP Law implicitly interprets the principle of necessity as requiring that personal data be processed strictly for its intended purpose, while the principle of proportionality is reflected in the requirement that personal data collection must be specific and limited. The phrase “specific and limited” indicates that data collection should not be excessive relative to the purpose of processing and must maintain a fair balance between corporate interests and the protection of data subjects’ rights. Unlike the European Union, where necessity and

proportionality tests have been explicitly and systematically implemented, the PDP Law does not yet provide concrete guidance on how to assess whether a given data processing activity can be considered "necessary." Consequently, the application of these two principles in Indonesia particularly within the banking sector still largely depends on the subjective interpretation of data controllers within respective institutions.

5. References

Journals:

Agusta, H. 2020. Perlindungan Data Pribadi Penerima Pinjaman dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi (Peer to Peer Lending). *Jurnal Hukum & Pembangunan*, Vol. 50, No. 4: p.795.

Anggraeni, S. F. 2018. Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi untuk Harmonisasi dan Reformasi Hukum di Indonesia. *Jurnal Hukum & Pembangunan*, Vol. 48, No. 4, Article 7: p.819.

Balya Al, M. D. 2023. Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya. Tuturan: *Jurnal Ilmu Komunikasi, Sosial, dan Humaniora,* Vol. 1, No. 3: p.275.

Black, G., & Stevens, L. 2013. Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest. *Scripted,* Vol. 10: p.93.

Hardiyanti, S. E. 2024. *Inovasi dalam Layanan Perbankan Berbasis Internet of Things (IoT): Peluang dan Tantangan di Era Digital.* Maeswara: Jurnal Riset Ilmu Manajemen dan Kewirausahaan, Vol. 2, No. 3: p.362.

Iswandari, B. A. 2022. Jaminan Keamanan Data Pribadi Warga Negara dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Government). *Dharmasisya,* Vol. 2, No. 1: p.80.

Marius, J. A. 2006. Perubahan Sosial. *Jurnal Penyuluhan,* Vol. 2, No. 2: p.125.

Meškić, Z., & Samardžić, D. 2017. The Strict Necessity Test on Data Protection by the CJEU: A Proportionality Test to Face the Challenges at the Beginning of a New Digital Era in the Midst of Security Concerns. *Croatian Yearbook of European Law & Policy,* Vol. 13, No. 1: p.133–168.

Prasad. 2024. Impact of Poor Data Quality on Business Performance: Challenges, Costs, and Solutions. *SSRN Electronic Journal.*

Rannie, B. W. 2023. Legal Protection of Customer Personal Data in the Banking Sector. *ARRUS Journal of Social Sciences and Humanities*, Vol. 3, No. 5: p.712.

Ridho, M. R., et al. 2024. Peran Big Data dalam Pengembangan Strategi Perbankan Syariah. *Jurbisman*, Vol. 2, No. 4: p.1352.

Suwondo, D. 2022. The Legal Protection of Personal Data in the Perspective of Human Rights. *Law Development Journal*, Vol. 5, No. 4: p.425.

Tan, S., Alexander, C., & Tantimin, T. 2023. An Academic Analysis of Data Privacy Frameworks in Indonesia. *Barelang Journal of Legal Studies*, Vol. 1, No. 1: p.72–89.

Wulansari, E. M. 2020. Konsep Perlindungan Data Pribadi sebagai Aspek Fundamental Norm dalam Perlindungan terhadap Hak atas Privasi Seseorang di Indonesia. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan,* Vol. 7, No. 2: p.268.

Books:

Ellis, E. (Ed.). (1999). *The principle of proportionality in the laws of Europe.* Oxford: Hart Publishing.

Gunardi. (2022). *Buku ajar metode penelitian hukum.* Jakarta: Damera Press.

Marzuki, P. M. (2017). *Penelitian hukum* (Edisi Revisi). Jakarta: Kencana.

Subekti, R. (1985). *Aneka perjanjian.* Jakarta: (penerbit tidak disebutkan).

Usanti, T. P., & Shomad, A. (2017). *Hukum perbankan.* Jakarta: Kencana.

Internet:

Data Protection Commission. "Quick Guide to the Principles of Data Protection." https://www.dataprotection.ie/, accessed on October 5th 2025.

DPO Centre. "Data Retention and the GDPR: Best Practices for Compliance." https://www.dpocentre.com/data-retention-and-the-gdpr-best-practices-for-compliance, accessed on September 25th 2025.

European Data Protection Supervisor. "Necessity & Proportionality." https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality, accessed on September 21st 2025.

PT Bank Tabungan Negara (Persero), Tbk. "Kebijakan Privasi BTN". https://www.btn.co.id/Privacy-Policy, accessed on October 4th 2025.

Regulation:

The 1945 Constitution of the Republic of Indonesia.

Law Number 27 of 2022 concerning Personal Data Protection.

European Union. (2000). Charter of Fundamental Rights of the European Union.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: General Data Protection Regulation (GDPR).

Interview:

Interview with Mr. Andri Irwanza Humardhani as Data Privacy Department Head at BTN on September, 23rd 2025.