JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i5

Juridical Construction of Data Accuracy Principles in Personal Data Protection Governance: A Comparative Analysis of Indonesia and Singapore

Seroja Rizki Amelia[1*], Sidi Ahyar Wiraguna[2]
[1]Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia
[2]Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia

[*]Corresponding Author: oja.amelia25@gmail.com

Abstract: The transformation of personal information into a strategic commodity in the digital ecosystem has elevated data quality governance from a mere administrative matter to a constitutional imperative. This study examines how the principle of accuracy is juridically constructed in Law Number 27 of 2022 concerning the Protection of Personal Data (PDP Law) and compares the construction with Singapore's Personal Data Protection Act 2012 (PDPA). Using normative-comparative legal research methods enriched with legislative, conceptual, and comparative functionalism approaches, the study evaluates whether Indonesia's regulatory framework provides adequate operational certainty for data controllers and adequate protection for data subjects. The analysis revealed that although Article 16 of the PDP Law mandates accuracy, completeness, and consistency, the provisions are declarative and lack defining precision, temporal renewal mechanisms, and clear accountability parameters. In contrast, Singapore's PDPA operates accuracy through *Accuracy Obligation* and *Correction Obligation*, which are enforced by *an independent Personal Data Protection Commission* (PDPC) with investigative and sanctioning authority. This study proposes a juridical reconstruction of Indonesia's accuracy principles through periodic data audits, effective correction protocols, calibration of risk-based governance, and the establishment of an independent supervisory authority with *quasi-judicial competence*.

Keywords: Data Accuracy, Juridical Construction, Personal Data Protection, Digital Governance, Comparative Law.

INTRODUCTION

Background

The digital revolution has transformed the characteristics of personal data from mere static identity attributes to dynamic assets that mediate individual access to public services, the financial system, and political participation (Cohen, 2019). The use of artificial intelligence, cloud computing, and predictive analytics has accelerated data collection, creating a fundamental information asymmetry between data subjects and data controllers (Solove, 2008). The main problem of personal data protection is no longer limited to information

confidentiality (*confidentiality*), but has shifted to the issue of data quality governance (*data governance*). When data becomes the basis for automated decision-making, the accuracy of information determines whether digital technologies will strengthen or even reduce the protection of individual rights. In situations where data subjects have limited ability to know, access, or correct processed data, information quality is one of the main prerequisites for algorithmic decision-making accuracy, as well as the protection of data subjects' rights.

As personal data becomes a key instrument in digital decision-making, any information inaccuracies no longer only impact administrative errors, but also potentially limit individuals' access to civil, economic, and political rights. It is in this context that the principle of data accuracy gains relevance as an instrument of legal protection against misuse and misprocessing of personal data.

Indonesia, with internet penetration exceeding 229 million users by 2026 (APJII, 2026), faces data governance disruptions that have not been matched by regulatory maturity. The incident of commercialization of BPJS Kesehatan participant data on the dark web forum, the alleged exfiltration of the database of digital platform users, and the compromise of the General Election Commission's Permanent Voter List (DPT) are not just indicators of *cybersecurity* failure. These various incidents show weak personal data governance which includes aspects of security, integrity, and data quality. These weaknesses increase the risk of inaccurate data being used in various administrative processes and automated decision-making. Defective, outdated, or unverified data not only compromises privacy, but can also lead to systemic discrimination, service access failures, and misdeterminations of legal status.

The *data accuracy principle* emerged in response to the crisis. This principle requires that data controllers guarantee that the information collected, processed, and exchanged meets the parameters of factual truth, contextual relevance, completeness of attributes, and temporal up-to-date (Rubinstein, 2013). Failure to meet this principle in a system that relies on *digital profiling* and decision-making, will automatically result in biased outputs and harm data subjects. Therefore, data accuracy has evolved from a secondary administrative obligation to a key pillar of the protection of digital privacy rights and human rights in the digital age.

Domestically, Indonesia's personal data protection regime is codified in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Article 16 of the PDP Law mandates data controllers to ensure the accuracy, completeness, and consistency of personal data. Symmetrically, Article 5 (letter d) recognizes the right of data subjects to update and correct their information. However, the normative construction in the PDP Law leaves a significant normative gap (*lacuna*), where this regulation does not define the parameters of "accuracy" and "consistency" operationally, and fails to formulate a structured data update mechanism, and fails to regulate the allocation of *burden of proof* when losses occur due to data defects.

By comparison, Singapore through the Personal Data Protection Act 2012 (PDPA) has operationalized the principle of accuracy into measurable obligations. The PDPA requires organizations to make reasonable *efforts* to ensure data accuracy, along with access and correction obligations overseen by the *Personal Data Protection Commission* (PDPC). The effectiveness of this regime can be seen from the 2018 SingHealth post-incident response, when the PDPC tightened compliance standards for data accuracy and protection obligations (PDPC, 2019; Ministry of Health Singapore, 2019). Singapore was chosen as the object of comparison because it is one of the jurisdictions in the Southeast Asian region that has operationalized the principle of data accuracy through the obligation of reasonable efforts, data correction mechanisms, and active supervision by the PDPC so as to provide a more implementable regulatory model than Indonesia.

Various studies have examined the implementation of the Personal Data Protection Law from the perspective of privacy rights, cybersecurity, and data governance, but discussions on

the principle of accuracy as a legal obligation of data controllers are still relatively limited. Studies that specifically analyze the normative parameters of data accuracy, accountability mechanisms for inaccurate data, and their comparison with Singapore's legal regime have also not been widely conducted. This gap shows the need for research that examines the principle of data accuracy as an instrument for the protection of data subject rights as well as evaluating the adequacy of its regulation in the PDP Law through a comparative legal approach.

Based on these problems, this study aims to analyze the regulation of data accuracy principles in Law Number 27 of 2022 concerning Personal Data Protection, identify normative weaknesses in its implementation, and compare it with the regulations in the Singapore Personal Data Protection Act in order to formulate recommendations for strengthening the protection of data subject rights in Indonesia.

Problem Formulation

Based on the above background, this study formulates two main questions:

1. What is the juridical construction of the principle of data accuracy in Indonesia's personal data protection regime?
2. How do the data accuracy principles compare between Indonesia and Singapore, as well as what reconstruction models can be adopted to strengthen Indonesia's PDP regime?

Research Objectives

This study aims to: (a) analyze the juridical construction of the principle of data accuracy in the Indonesian PDP Law through systemic interpretation; (b) compare the construction with Singapore's PDPA regime; and (c) formulate a normative reconstruction model that is adaptive to the dynamics of digital data governance.

Research Significance

Theoretically, this study develops a juridical construction framework of data accuracy principles that integrates the perspective of digital constitutional rights with a risk-based governance approach. Practically, the results of the research are expected to be considered for lawmakers in drafting implementing regulations for the PDP Law and realizing an independent supervisory authority.

RESEARCH METHODS

Types and Approaches to Research

This study applies normative-comparative legal research methodology enriched with a socio-legal perspective. The normative approach is used to dissect the construction of data protection norms, principles, and principles in Indonesian and Singapore regulations through grammatical, systemic, and teleological law interpretation techniques (Wiraguna, 2024).

A comparative approach is used to evaluate the effectiveness of the regulations of the two countries using the comparative *functionalism* method, which assesses how each legal system solves identical problems (data accuracy protection) through different normative and institutional instruments (Kötz & Zweigert, 1998). This approach does not simply compare regulatory texts, but rather evaluates legal outputs in data governance practices.

Legal Materials and Collection Techniques

Primary legal materials include: PDP Law No. 27 of 2022, Singapore PDPA 2012 (including 2020 amendments), ITE Law No. 11 of 2008 as amended by Law No. 19 of 2016, PP No. 71 of 2019, and PDPC's investigation report related to the SingHealth incident. Secondary legal materials include scientific literature, *international guidelines* (*OECD Privacy Framework, APEC Privacy Framework*), and empirical data related to data leak incidents in Indonesia.

Data Analysis Techniques

The analysis was carried out qualitatively through three techniques: (a) *doctrinal content analysis* to map the normative construction in the PDP Law; (b) *comparative functional analysis* to evaluate the effectiveness of the Singapore regime; and (c) *prescriptive legal argumentation* to formulate adaptive normative reconstructions. The *legal transplantation analysis approach* (Watson, 1993) was used to measure the feasibility of adopting the concept *of accountability* and *risk-based governance* from Singapore into the Indonesian legal system, taking into account institutional readiness and national legal culture.

ANALYSIS AND DISCUSSION

Juridical Construction of Data Accuracy Principles in Indonesia's PDP Regime

1. The Position of the Accuracy Principle in the Hierarchy of Data Protection Norms

The juridical construction of the principle of data accuracy in the PDP Law cannot be analyzed in isolation, but must be positioned within the overall normative hierarchy of the data protection regime. The PDP Act adopts *a principles-based regulatory approach* that mandates a set of fundamental principles in the processing of personal data. Article 4 (letter d) of the PDP Law stipulates that the processing of personal data must be carried out accurately, completely, not misleading, up-to-date, and relevant to the purpose for which it was collected. Article 15 adds that data controllers are obliged to guarantee the security of personal data from unauthorized access, use, alteration, disclosure, destruction and/or deletion. Article 16 then requires controllers to ensure the accuracy, completeness, and consistency of personal data.

This tripartite juridical construction of accuracy (Articles 4 & 16), security (Article 15), and correction (Article 5) creates *normative interdependency*, where the failure of one principle will cascade the failure of another. However, the PDP Law fails to articulate the causal and hierarchical relationship between the three principles. From the perspective *of systemic statutory interpretation*, Article 16 should be interpreted as an *operative provision* that implements the principle of Article 4 (letter d), but the absence of an operational definition makes Article 16 self-referential and juridically empty.

2. Definitional Deficits and Conceptual Emptiness

A textual analysis of Article 16 of the PDP Law reveals four fundamental juridical construction deficits:

1) First, the absence of an operational definition of "accuracy". The PDP Law does not distinguish between accuracy in the static sense (conformity of data with the subject's basic identity at the time of collection) and *accuracy* in the dynamic sense (relevance and up-to-date data as subject conditions change). In a digital ecosystem, the validity of data demands a *continuous updating obligation* or accurate data at the time of collection can become invalid if it is not updated, which in turn distorts algorithmic output (Kuner, 2013).
2) Second, the ambiguity of the "consistency" parameter. Consistency in the PDP Law can be interpreted minimally as *internal consistency* (there is no contradiction between attributes in one database) or maximalist as *external consistency* (the suitability of data between various databases owned by controllers or third parties). Without clarification, data controllers may formally meet their consistency obligations while the data is substantively obsolete or does not reflect the actual conditions of the data subject.
3) Third, the absence of rules regarding the allocation *of burden of proof*. When a data subject suffers a loss due to a data defect (e.g., denial of credit access due to outdated data in credit scoring), the PDP Act does not regulate whether the subject or controller must prove error. In the perspective of *the accountability principle* adopted by the GDPR

and international *guidelines*, the burden of proof should be placed on the data controller (*reversal burden of proof*), given the asymmetry of information and technological capacity between the subject and the controller (Voigt & von dem Bussche, 2017).

4) Fourth, the absence of *a strict liability* or *liability without fault* regime for losses due to data defects. The PDP Law regulates liability in Articles 57-66, but it is general and does not specify the consequences of violations of the principle of accuracy. Lynskey (2015) argues that data integrity must be guaranteed through an absolute liability regime, where controllers are responsible for losses due to obsolete data or failed verification, without having to wait for proof of fault. The failure to regulate this makes data protection in Indonesia trapped in a formalistic compliance paradigm that is absent from *risk-based digital governance*.

3. Juridical Construction in the Perspective of Legal Protection Theory

Based on the theory of legal protection by Philipus M. Hadjon (1987), an effective law must provide preventive and repressive instruments. In the context of data accuracy, a preventive approach is realized through the obligation to verify the accuracy of pre-processing data and periodic *audits*. Meanwhile, the perspective of Gustav Radbruch (1950) emphasizes that law must guarantee legal certainty (*Rechtssicherheit*), which in the context of personal data means certainty over the validity of data to prevent multidimensional losses.

An ideal juridical construction according to legal protection theory requires the existence of: (a) clear norms and not multi-interpretations, (b) effective supervisory mechanisms, (c) proportionate sanctions, and (d) easy access to justice. Indonesia's PDP Law only meets a small part of these criteria. Accuracy norms have been described, but they are blurred because oversight mechanisms have not yet been established (supervisory authorities are still in the process of being formed), administrative sanctions have not been regulated in detail, and access to courts is still hampered by *unregulated* burden of proof.

Comparison of Data Accuracy Principles Setting: Indonesia and Singapore

1. Normative Architecture of Singapore PDPA

Singapore through the PDPA 2012 has translated the principle of accuracy into measurable and enforceable operational obligations. Section 23 of the PDPA establishes *an Accuracy Obligation* which requires organizations to make reasonable *efforts* to ensure that the personal data used or disclosed is accurate and complete, especially if the data is the basis for decision-making that affects the individual. These obligations are not absolute, but are calibrated by reasonable *efforts standards* assessed based on the context of the processing, the sensitivity of the data, and the risk of impact on the data subject.

Section 24 of the PDPA adds *a Correction Obligation* that provides a structured corrective mechanism. If the data subject finds an error, the organization is obliged to correct it and send the corrected data to the third party that received the data within the previous year. This mechanism ensures the *propagation of accuracy* throughout the data processing chain, reducing the risk of data stale spread across multiple entities.

2. Institutional Architecture and Law Enforcement

The fundamental difference between Indonesia and Singapore lies in the institutional architecture of the supervisory system. Singapore mandates the *Personal Data Protection Commission (PDPC)* as an independent authority with investigative authority, compliance audits, the imposition of administrative sanctions, and the issuance of technical guidelines. Post-SingHealth 2018 incident, in which the personal data of 1.5 million patients including the data of Prime Minister Lee Hsien Loong was exfiltrated. The PDPC conducts a

comprehensive investigation and tightens compliance standards for *accuracy obligations and protection obligations* (PDPC, 2019; Ministry of Health Singapore, 2019).

The effectiveness of the Singapore regime lies in *the feedback loop* between incidents, investigations, and regulatory reforms. The PDPC not only imposes sanctions, but also publishes a public report detailing systemic failures and recommendations for improvement. This approach implements the principles *of accountability* and *transparency* that are essential for *trust-based digital governance.*

On the contrary, Indonesia is still grappling with the institutional design of supervisory authorities that have not been fully guaranteed independence. The PDP Law mandates the establishment of a supervisory institution (Articles 56-66), but until now its realization is still pending. Hadjon (1987) reminded that effective legal protection requires preventive and repressive instruments executed by empowered and independent institutions. Without a functioning supervisory authority, the principle of accuracy in the PDP Law will depend heavily on the *goodwill* of the data controller and the good faith of the data subject in assuming compliance.

Table 1. Comparative Juridical Construction

Dimensions	Indonesia (PDP Law)	Singapore (PDPA)
Normative Foundations	Article 4 letter d, Article 16	Part 23, Part 24
Definition of Accuracy	Undefined	*Reasonable efforts* for accuracy and completeness
Update Mechanism	Unregulated	*Correction obligation* with notification to third parties
Liability Standards	*Best effort* (implicit)	*Reasonable efforts* (explicit and calibrated)
Supervisory Authority	Not yet formed	PDPC (*independent, investigative, punitive)*
Sanctions for Accuracy Violations	Not specially set	Administrative and criminal sanctions
Burden of Proof	Unregulated	Accountability to the operator (implicit in the guidelines)

3. Reconstruction Model of Data Accuracy Principles for Indonesia

Based on the comparative analysis and juridical construction above, the reconstruction of the principle of data accuracy in the Indonesian PDP regime must be carried out through implementing regulations or amendments to the PDP Law. Ideal models include:

1) Periodic *Data Audit Obligation*
   Data controllers, especially those who process sensitive data (health, financial, biometrics) or use *automated decision-making*, are required to conduct periodic audits of the validity and relevance of data (at least annually). This audit should document: (a) the source of the data, (b) the date of collection, (c) the last date of the update, (d) the level of accuracy to the subject's actual condition, and (e) the follow-up of corrections. Audit documentation is evidence of *compliance* that can be requested by supervisory authorities or courts.
2) Effective *Correction Mechanism*
   Adopting Singapore's correction obligation with adaptation to the Indonesian context, the regulation should: (a) limit the controller's response time to a correction request (e.g. 14 working days), (b) require notification of the correction to the data subject, (c)

require the controller to forward the correction to a third party that has received the data within 12 months, and (d) provide the data subject with the right to file an *objection* if the correction is rejected.

3) Automatic *Updating Obligation*
   For high-risk sectors (health, finance, population), controllers are required to build a system that is integrated with primary data sources (e.g. Dukcapil for population data, BI OJK for financial data) to update data automatically or periodically. This obligation reduces the risk of *data stale*, which is the root of problems in *credit scoring* and public services.
4) *Risk-Based Data Governance*
   The controller's liability should be calibrated based on the level of data processing risk. Technical guidelines issued by supervisory authorities should categorize risks based on: (a) data sensitivity, (b) processing scale, (c) algorithm complexity, and (d) potential impact on data subjects. The higher the risk, the more stringent the verification, audit, and mitigation standards that must be applied.
5) Implementation *of Strict Liability* and *Reversal Burden of Proof*
   Data controllers must be held fully accountable for losses arising from data defects, unless they can prove that they have conducted periodic audits and met reasonable *efforts standards*. The burden of proving that the data has been processed accurately and lawfully should be placed on the controller, not the data subject. This approach accommodates information asymmetry and encourages controllers to invest resources in data quality governance.
6) Strengthening of the Independent Supervisory Authority
   Indonesia must immediately realize an independent personal data protection supervisory body, equivalent to the Singapore PDPC model. This authority shall have the authority to: (a) issue technical guidelines and industry standards, (b) conduct ex *officio* compliance audits or on the basis of complaints, (c) impose administrative sanctions (warnings, fines, processing restrictions), and (d) file a class *action on* behalf of the aggrieved data subject.

CONCLUSION

1. The principle of data accuracy is a fundamental pillar in the modern personal data protection ecosystem that cannot be reduced to a mere administrative obligation. An analysis of the juridical construction in the Indonesian PDP Law reveals that the provisions of Article 16 are declarative and lack definitive precision, temporal renewal mechanism, burden of proof allocation, and accountability parameters. This normative vacuum creates a space of legal uncertainty that undermines the protection of digital privacy rights and risks triggering multidimensional losses for data subjects.
2. A comparative study with Singapore proves that the effectiveness of data protection is largely determined by the operationalization of norms through measurable accuracy obligations and correction obligations, supported by independent supervisory authorities with investigative and punitive powers. Singapore's PDPC shows that an effective data protection regime does not stop at regulatory text, but rather at progressive and incidental law enforcement.
   Therefore, legal reconstruction in Indonesia must be directed to: (a) the implementation of periodic data audits with compliance documentation, (b) structured correction mechanisms with deadlines and notifications, (c) automatic renewal obligations for high-risk sectors, (d) risk-based governance calibrated by sensitivity and processing scale, (e) the implementation of strict liability with *reversal burden of proof*; and (f) strengthening independent supervisory institutions with *quasi-judicial competence*. This transformation is essential to

shift the paradigm of data protection in Indonesia from *formalistic compliance* to *risk-based digital governance* that is adaptive to artificial intelligence disruption and social data expansion.

BIBLIOGRAPHY

APJII. (2026). *Report on Indonesian internet user penetration and behavior survey 2026*. Indonesian Telecommunication Network Operators Association.

Bygrave, L. A. (2002). *Data protection law: Approaching its rationale, logic and limits*. Kluwer Law International.

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

Cohen, J. E. (2019). *Turning privacy inside out.* Theoretical Inquiries in Law, 20(1), 1–31. https://doi.org/10.1515/til-2019-0001

De Hert, P., & Papakonstantinou, V. (2016). *The new general data protection regulation: A sound instrument for the digital internal market?* Computer Law & Security Review, 32(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

Greenleaf, G. (2023*). Global data privacy laws 2023: 145 national laws, including 15 new laws, as GDPR nears its fifth anniversary*. Privacy Laws & Business International Report, 181, 10–15.

Hadjon, P. M. (1987). *Legal protection for the Indonesian people*. Build Knowledge.

Ministry of Health of Singapore. (2019)*). Public report on the SingHealth data breach*. Ministry of Health Singapore.

Kötz, H., & Zweigert, K. (1998). *An introduction to comparative law* (3rd ed.). Clarendon Press.

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

PDPC. (2019). *Guide to data protection practices for ICT systems*. Personal Data Protection Commission Singapore.

PDPC. (2019). *Public consultation on proposed amendments to the Personal Data Protection Act*. Personal Data Protection Commission Singapore.

Radbruch, G. (1950). Legal philosophy (K. Wilk, Trans.). *The legal philosophies of Lask, Radbruch, and Dabin* (pp. 43–224). Harvard University Press.

Republic of Indonesia. (2008). *Law Number 11 of 2008 concerning Information and Electronic Transactions*. Statute Book of the Republic of Indonesia of 2008 Number 58.

Republic of Indonesia. (2016). *Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions*. Statute Book of the Republic of Indonesia Year 2016 Number 59.

Republic of Indonesia. (2019). *Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions*. Statute Book of the Republic of Indonesia of 2019 Number 122.

Republic of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*. Statute Book of the Republic of Indonesia Year 2022 Number 238.

Republic of Singapore. (2012). *Personal Data Protection Act 2012* (No. 26 of 2012, as amended in 2020). Government of Singapore.

Rosadi, S. (2020). *Cyber law and privacy protection in Indonesia*. Aditama Review.

Rubinstein, I. S. (2013). *Big data: The end of privacy or a new beginning? International Data Privacy Law*, 3(2), 74–87. https://doi.org/10.1093/idpl/ipt003

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7

Warren, S. D., & Brandeis, L. D. (1890). *The right to privacy*. Harvard Law Review, 4(5), 193–220.

Watson, A. (1993). *Legal transplants: An approach to comparative law* (2nd ed.). University of Georgia Press.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Wiraguna, S. A. (2024). *Normative and empirical methods in legal research: An exploratory study in Indonesia*. Public Sphere: Journal of Socio-Politics, Government and Law, 3(3), 45–58.

Wiraguna, S. A. (2025). *Exploration of research methods with normative and empirical approaches in legal research in Indonesia*. Lex Jurnalica, 22(1), 66–72.