Al-Adalah: Jurnal Hukum dan Politik Islam
https://jurnal.iain-bone.ac.id/index.php/aladalah
E-ISSN 2685-550X | P-ISSN X2406-8802
Vol.12, No.1, January, 2027, pp. 1-17
https: Prefix 10.35673
aladalah@iain-bone.ac.id

The Transformation of Electronic System Trade Operators' Obligations Regarding Personal Data Protection in Indonesia and Singapore

Fariz Hassan Maulana[a,1], Nadia Carolina Weley[b,2*], Rufinus Hotmaulana Hutauruk[c,3]

[a,b,c] Universitas Internasional Batam, Kota Batam, Kepulauan Riau, Indonesia
[1]2351085.fariz@uib.edu; [2] nadia.carolina@uib.ac.id*; [3] rufinus.hotmaulana@uib.ac.id

* corresponding author

ARTICLE INFO

Article history
Received : 27 August 2026
Revised : 3 November 2026
Accepted : 10 November 2026

Keywords
Personal data protection;
Electronic commerce;
Electronic system trade operators;
Indonesia;
Singapore

ABSTRACT

The rapid growth of electronic commerce has increased the volume of consumers' personal data processed by Electronic System Trade Operators (PPMSE), thereby creating a need for a robust legal protection framework. This study examines and compares how Indonesia and Singapore regulate and operationalise PPMSE obligations concerning personal data protection. It adopts a normative or doctrinal legal research design using statutory, conceptual, and comparative approaches. The analysis identifies significant differences in how the two jurisdictions institutionalise and operationalise personal data protection rules. Indonesia has established a statutory foundation through Law No. 27 of 2022 on Personal Data Protection and Government Regulation No. 80 of 2019 on Electronic System Trading; however, the effectiveness of implementation remains constrained by incomplete institutional arrangements and the absence of sufficiently detailed technical compliance standards. Singapore, by contrast, has developed a more operational framework under the Personal Data Protection Act 2012, supported by the Personal Data Protection Commission (PDPC), particularly in relation to Data Protection Officer requirements, data breach notification, and administrative sanctions. The study concludes that strengthening personal data governance in Indonesia requires the effective operationalisation of an independent supervisory authority, clearer and proportionate compliance obligations, and technical standards adapted to the characteristics of digital commerce.

This is an open access article under the CC–BY-SA 4.0 license.

1. Introduction

The growth of electronic commerce has made consumers' personal data an increasingly important asset processed by Electronic System Trade Operators (PPMSE), ranging from basic personal data—such as full name, religion, nationality, and gender—to specially categorised personal data and information concerning consumers' shopping preferences.[1] As digital commerce expands, consumers are increasingly required to provide personal data through electronic platforms. In Indonesia, the value of e-commerce transactions in 2024 was estimated to reach IDR 487.01 trillion. This figure reflects sustained year-on-year growth, while the domestic online-shopping user base was projected to reach 189.6 million people in the same year.[2] Meanwhile, Singapore has established a personal data protection regime through the Personal Data Protection Act 2012 (PDPA), which regulates organisations' obligations concerning the collection, use, disclosure, security, retention, and notification of data breaches to the relevant authorities within specified time limits. This comparison is particularly relevant because Indonesia is undergoing a significant regulatory transition following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), whereas Singapore has already developed a more mature institutional and compliance framework through the Personal Data Protection Commission (PDPC).[3]

In Indonesia, the regulation of PPMSE obligations concerning personal data protection is reflected, among other provisions, in Article 16(2)(e) of the PDP Law, which requires personal data controllers to maintain data security and prevent unauthorised access.[4] This obligation is fundamentally grounded in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which guarantees every person's right to protection of their person, family, honour, dignity, and property.[5] However, the reported leakage of 91 million Tokopedia user accounts in 2020, as reported by TEMPO Media, illustrates the limitations of PPMSE compliance prior to the enactment of the PDP Law.[6] Singapore adopts a different approach. Section 24 of the PDPA imposes legal and operational responsibilities on organisations to implement reasonable security measures. The practical enforcement of these obligations can be illustrated by the case of E-

[1] Nadia Carolina Weley and Hari Sutra Disemadi, "Implikasi Hukum Pemasangan CCTV Di Tempat Umum Secara Tersembunyi Terhadap Perlindungan Data Pribadi," *Amnesti: Jurnal Hukum* 4, no. 2 (2022): 79–93, https://doi.org/10.37729/amnesti.v4i2.2151.

[2] Puput Leni Jayanti, "Pengaruh Daya Tarik Host , Atribut Anchor Dan Diskon Terhadap Minat Beli Produk Dahion Muslim Pada Live Streaming Shopee," *Nucl. Phys.* 13, no. 1 (2026): 104–16.

[3] Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital : Perlindungan Data Pribadi Di Indonesia," no. 1 (2023): 132–46, https://doi.org/https://doi.org/10.38043/jah.v6i1.4484.

[4] Kadek Nova Adistiya et al., "Perlindungan Hukum Bagi Konsumen Terhadap Kebocoran Data Pribadi Berdasarkan Pasal 16 Ayat 2 Huruf E Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *MyGovernment* 4, no. 1 (2024): 1–13, https://doi.org/https://doi.org/10.23887/jih.v4i3.5034.

[5] "Undang -Undang Dasar Negara Republik Indonesia Tahun 1945" (1945).

[6] Annisya Diandra et al., "Polemik Data Pribadi: 5 Kasus Kebocoran Data Di Indonesia Selama 2023-2024," *Tempo*, 2025.

Commerce Enablers Pte. Ltd.[7] in which the PDPC imposed a fine of S$74,400 for a breach of data protection obligations. These differences provide a basis for examining the transformation of PPMSE obligations concerning personal data protection in Indonesia and Singapore.

Previous studies on personal data protection in Indonesia can generally be grouped into three areas. First, studies have examined legal awareness and the scope of data subjects' rights, including research on the importance of personal data literacy in promoting preventive behaviour.[8] The literature also examines civil claims based on unlawful acts and criminal enforcement for data violations under the Electronic Information and Transactions Law and the Indonesian Civil Code.[9] Second, studies have addressed regulatory adaptation and law enforcement in the digital era, including the flexibility of the PDP Law in emerging digital ecosystems and the role of supervisory institutions in addressing cybercrime, such as phishing.[10] Third, post-PDP Law studies have identified four principal obstacles in Indonesia: the absence of implementing technical regulations, limited cybersecurity infrastructure, weak inter-agency coordination, and a relatively low culture of personal data protection.[11] International comparative scholarship reinforces this gap. Comparative studies have already examined Indonesia alongside Singapore and other ASEAN jurisdictions, but they tend to focus on sector-specific regulation or broad data-protection frameworks rather than the institutional and operational obligations of electronic system trade operators. This study therefore shifts the comparison from the mere existence of legal rules to the way those rules are institutionalised, operationalised, and enforced in the digital-commerce environment.[12]

Although the existing literature has mapped important normative and practical dimensions of personal data protection in Indonesia, most studies remain focused on

---

[7] Personal Data Protection Commission, Personal Data Protection Commission [2023] SGPDPC 6 (2023).

[8] Della Delia, David Tan, and Shenti Agustini, "Regulasi Hukum Ekonomi Digital : Implikasi Undang-Undang Nomor 1 Tahun 2024 Terhadap E-Commerce Dan Start-Up Di Indonesia," *Unes Journal of Swara Justisia* 10, no. 1 (2026): 41–54, https://doi.org/https://doi.org/10.31933/d1hpnz59.

[9] Muhammad Fikri and Shelvi Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia" 5, no. 1 (2023): 39–57, https://doi.org/https://doi.org/10.23887/glr.v5i1.2237.

[10] Ananta Fadli Sutarli and Shelly Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *INNOVATIVE: Journal Of Social Science Research* 3 (2023): 4208–21.

[11] Yulianto Wibowo, Ida Aryati Dpw, and Iismiyanto, "Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi," *Jurnal Serambi Hukum* 18, no. 01 (2025): 1–6, https://doi.org/https://doi.org/10.59582/sh.v18i01.1216.

[12] Dona Budi Kharisma and Alvalerie Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare* 17, no. 2 (September 6, 2022): 157–69, https://doi.org/10.1108/IJHRH-04-2022-0035; Putu Aryan Darma Sukerta and Andri Sutrisno, "Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks," *Constitutional Law Review* 3, no. 2 (2024): 133–47; Muhayar, Fitra Deni, and Zulfadli Barus, "Cyber PPAT and Legal Certainty in Indonesia ' s Electronic Land Certification System," *Al-Adalah : Jurnal Hukum Dan Politik Islam* 10, no. 1 (2025): 201–17, https://doi.org/doi.org/10.30863/ajmpi.v10i1.8473.

domestic legal issues and general questions concerning data subjects. Against this background, this study comparatively examines the legal frameworks and regulatory arrangements governing personal data protection in Indonesia and Singapore. The comparative analysis identifies similarities, differences, and regulatory gaps in the two jurisdictions, with particular attention to institutional design, compliance mechanisms, and enforcement. The analysis therefore provides a basis for considering how Indonesia's personal data protection framework may be strengthened through context-sensitive regulatory reform.[13] The research gap is consequently not the absence of comparative scholarship, but the limited functional comparison of PPMSE obligations across the two jurisdictions. The analysis focuses on four linked regulatory functions: allocation of supervisory authority, organisational accountability through DPO arrangements, incident and breach notification, and enforcement and remedies. [14]

The study further identifies regulatory practices in Singapore that may provide useful comparative lessons for Indonesia, while recognising differences in legal systems, institutional capacity, and economic structure. The resulting recommendations are intended to assist policymakers in formulating or revising implementing regulations, guide PPMSE in strengthening compliance standards, and enhance consumer protection and public trust in Indonesia's digital commerce ecosystem. Rather than treating Singapore as a model for direct transplantation, the study uses Singapore as a comparative reference point from which Indonesia may identify institutionally feasible and proportionate reforms. This approach is particularly important because regulatory effectiveness depends on institutional capacity, supervisory accountability, and the ability of regulators to translate broad statutory principles into operational compliance requirements.

2. Legal Material and Methods

This study adopts a normative or doctrinal legal research design. The analysis focuses on primary, secondary, and tertiary legal materials. Primary legal materials comprise Law No. 27 of 2022 on Personal Data Protection (PDP Law), Government Regulation No. 80 of 2019 on Electronic System Trading (PMSE), and Singapore's Personal Data Protection Act 2012 (PDPA). Secondary legal materials include legal scholarship, textbooks, journal articles, research findings, papers, and expert opinions interpreting the relevant primary legal sources. Tertiary legal materials include legal dictionaries and Indonesian- and English-language reference dictionaries. For comparative purposes, the study also draws on international scholarship concerning data-protection governance, regulatory enforcement, supervisory independence, and risk-based

[13] Lu Sudirman and Hari Sutra Disemadi, "Titik Lemah Industri Keuangan Fintech Di Indonesia : Kajian Perbandingan Hukum" 4 (2022), https://doi.org/https://doi.org/10.14710/jphi.v4i3.471-493.

[14] I Gusti Ngurah Parikesit Widiatedja and Neha Mishra, "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective," *International Review of Law, Computers & Technology* 37, no. 3 (September 2, 2023): 252–73, https://doi.org/10.1080/13600869.2022.2155793.

compliance. These materials are used not as substitutes for the primary legal sources but as analytical authorities for interpreting the institutional and operational dimensions of the two regimes.[15]

The legal materials were collected through doctrinal desk research and library research and analysed using comparative legal and descriptive qualitative methods. The comparative analysis examines the personal data protection regimes of Indonesia and Singapore, particularly the institutionalisation of supervisory authorities, operational compliance mechanisms, and the nature of sanctions. The statutory approach is used to assess the structure and consistency of relevant regulations, while the conceptual approach is applied to examine the doctrines and principles underlying personal data protection. The findings are then synthesised into systematic and argumentative conclusions.[16] The comparative method is applied functionally: equivalent regulatory functions are compared across Indonesia and Singapore rather than comparing statutory provisions in isolation. This enables the analysis to distinguish formal legal similarity from differences in institutional capacity, compliance design, enforcement practice, and remedial accessibility.

3. Results and Discussion

3.1. Regulation of PPMSE Obligations Concerning Personal Data Protection in Indonesia and Singapore

Personal data protection in the context of Electronic System Trade Operators (PPMSE) is grounded in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which guarantees every person's right to protection of their person, family, honour, dignity, and property.[17] Under Philipus M. Hadjon's theory of legal protection, legal protection seeks to preserve human dignity and prevent arbitrary action through two principal mechanisms: preventive and repressive protection. In the context of electronic commerce, this framework requires the law to ensure that the constitutional rights associated with personal data are effectively safeguarded amid the rapid expansion of digital transactions.[18]

[15] Karen Yeung and Lee A Bygrave, "Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship," *Regulation & Governance* 16, no. 1 (January 1, 2022): 137–55, https://doi.org/https://doi.org/10.1111/rego.12401.

[16] Haikal Narendra Sudjudiman and Fatma Ulfatun Najicha, "Pengaturan Pemutusan Hubungan Kerja (Phk) Di Indonesia Dan Singapura (Studi Perbandingan Hukum Indonesia Dan Hukum Singapura)" 4, no. 2 (2020): 40–50, https://doi.org/doi.org/10.25299/uirlrev.2020.vol4(2).6767.

[17] Sudjudiman and Najicha.

[18] Muhammad Maulana Abdullah Ulil ALBAB, "Batasan Keterlibatan Non-Pihak Dalam Pemeriksaan Persiapan Sengketa Tata Usaha Negara Berdasarkan Teori Perlindungan Hukum Philipus M.Hadjon Dan Sadd Adz-Dzariah: Studi Di Pengadilan Tata Usaha Negara" (Universitas Islam Negeri Maulana Malik Ibrahin Malang, 2025).

From a normative perspective, Indonesia's legal framework comprises the PDP Law No. 27 of 2022, the Electronic Information and Transactions Law, and the PMSE Government Regulation. Singapore, by contrast, regulates electronic transactions primarily through the Electronic Transactions Act 2010 (ETA 2010), while personal data protection is governed specifically by the Personal Data Protection Act 2012 (PDPA 2012). From a preventive perspective, Article 59 of the PMSE Government Regulation and Articles 20 and 21 of the PDP Law establish requirements concerning standards, transparency, and consent-based processing.[19] However, the two jurisdictions differ significantly in the degree of legal certainty and operational uniformity provided by these rules. Singapore adopts a more universal approach through Sections 11(3) and 12 of the PDPA 2012, which require organisations to appoint a Data Protection Officer (DPO) and establish complaint-handling procedures and internal policies, irrespective of business scale. By contrast, Article 53 of Indonesia's PDP Law requires the appointment of a DPO only in specified circumstances, including public-service processing, core activities involving regular and systematic large-scale monitoring, or the processing of specific or high-risk personal data. The absence of clearly defined quantitative criteria for "large scale" and "high risk" may create legal uncertainty, produce inconsistent compliance standards among PPMSE, and complicate the exercise of data subjects' rights.[20]

Singapore may provide a useful comparative reference in the field of personal data protection because its regulatory framework combines relatively detailed statutory obligations with an established supervisory institution. The PDPC plays a central role in promoting compliance and enforcing personal data protection requirements, including through sanctions against organisations that violate the PDPA.[21] This combination of regulatory clarity, institutional capacity, and enforcement contributes to greater predictability for businesses and stronger protection for data subjects. Singapore's experience may therefore offer useful lessons for Indonesia, although any regulatory adaptation must take account of Indonesia's distinct legal, institutional, social, and economic conditions.[22] International scholarship cautions, however, against treating

[19] "Government Regulation of the Republic of Indonesia Number 80 of 2019 Concerning Trading Through Electronic Systems (Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik)" (2019).

[20] "Law Number 27 of 2022 Concerning Personal Data Protection (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi)," 2022; Benjamin Wong YongQuan, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012," *International Data Privacy Law* 7, no. 4 (November 1, 2017): 287–302, https://doi.org/10.1093/idpl/ipx016.

[21] Annisa Putri AzizulRahmah Rahmah, Putri Olivia Anggraini, and Muhammad Hasbi, "Perlindungan Data Pribadi Sebagai Hak Asasi Manusia Di Era Digital : Analisis Dan Perbandingan Indonesia Dan Singapura," 2026, 3242–49, https://doi.org/https://doi.org/10.61104/alz.v4i3.5839.

[22] Azza Fitrahul Faizah et al., "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," 2023, https://doi.org/https://doi.org/10.51903/hakim.v1i3.1222.

institutional maturity as synonymous with institutional independence.[23] Singapore's PDPC offers an established supervisory structure, but comparative scholarship on Asian data-protection regimes shows that the independence and accountability of supervisory authorities remain important criteria for assessing regulatory effectiveness. Singapore is therefore used here as a reference point for operationalisation, not as an unqualified institutional benchmark.

Repressive legal protection concerns remedies and enforcement after a person's rights have been violated. According to Philipus M. Hadjon, repressive protection serves to enforce the law, impose sanctions, and restore the rights of persons whose interests have been adversely affected by a violation. In Indonesia, Article 46(1) of the PDP Law requires PPMSE that experience a personal data protection failure to notify data subjects and the competent authority in writing within a maximum period of 3 × 24 hours. Articles 57(1)–(3) of the PDP Law and Article 80 of the PMSE Government Regulation provide for administrative fines of up to 2% of the annual revenue of the relevant personal data controller.[24] The PDP Law also provides criminal sanctions, including imprisonment and fines, under Articles 67–73 for specified unlawful acts involving personal data. Singapore adopts a comparatively developed enforcement framework under the PDPA and the supervision of the PDPC. Under Part 6A, Section 26D, organisations must notify the PDPC of notifiable data breaches within a maximum of three calendar days.[25] Section 48J(3) authorises the PDPC to impose financial penalties of up to S$1 million, or up to 10% of a company's annual turnover where its turnover exceeds S$10 million.[26] In addition, Section 48O provides a right of private action in specified circumstances, allowing individuals who suffer loss or damage to pursue civil remedies. These differences are summarised in the following table:

Table 1. Comparison of Personal Data Protection Law in Electronic Commerce in Indonesia and Singapore

Classification	Indonesian Law	Singaporean Law
Applicable law	Law No. 27 of 2022 on Personal Data Protection and Government	*Personal Data Protection Act* 2012

[23] Graham Greenleaf, "The New Data Protection Convention 108+ and Its Importance for Asia," *International Journal of Law and Information Technology* 34 (January 1, 2026): eaaf024, https://doi.org/10.1093/ijlit/eaaf024.

[24] Muhammad Fadel Adhyputra, Thoriq Ahmadi, and Mohammad Rifqi, "Gagasan Perlindungan Data Pribadi Oleh LPPDP Indonesia: Sebuah Studi Perbandingan Dengan Otoritas Pelindungan Data Pribadi Singapura," *Jurnal LeDHaK Fakultas Hukum Unhas* 2, no. 2 (2024): 304–21.

[25] Heilynn et al., "Perbandingan Penyelesaian Hukum Perkara Penyebaran Data Pribadi Di Media Massa Antar Indonesia Dan Singapura," *Almufi Jurnal Sosial Dan Humaniora* 2, no. 3 (2025), https://doi.org/https://doi.org/10.63821/ash.v2i3.574.

[26] Lailatul Badria, Dwiyanto Indiahono, and Sukarso, "Akuntabilitas Dalam Kebijakan Perlindungan Data Pribadi Di Indonesia Belajar Dari Korea Selatan Dan Singapura," *Manntra Pembaruan: Jurnal Inovasi Kebijakan* Vol. 8, no. No. 2 (2024): Hal. 89-102, https://doi.org/https://doi.org/10.21787/mp.8.2.2024.89-102.

	Regulation No. 80 of 2019 on Electronic System Trading	
Data Protection Officer	Articles 53(1)–(3) of the PDP Law: dependent on scale	Section 11(3) of the PDPA 2012: mandatory
Data breach notification	Article 46(1) of the PDP Law: 3 × 24 hours from the data protection failure.	*Section 26D of the PDPA 2012: obligation to report suspected data breaches within a maximum of three calendar days to the PDPC.*
Administrative sanctions	Articles 57(1)–(3) of the PDP Law and the PMSE Government Regulation: administrative sanctions in the form of fines of up to 2% of the annual revenue of the personal data controller	*Section 48J(3) of the PDPA 2012: financial fines imposed by the PDPC of up to S$1 million, or 10% of the company's annual turnover where turnover exceeds S$10 million*
Legal remedies	Article 64 of the PDP Law: litigation and non-litigation remedies	*Section 48H(1) of the PDPA 2012: legal remedies through complaints submitted to the PDPC*
Institution	Article 58 of the PDP Law: an independent institution to be established by presidential regulation; however, its implementation has not yet been fully established and remains in the formation process	*Sections 5(1) and (2) of the PDPA 2012: a dedicated personal data protection authority, namely the Personal Data Protection Commission (PDPC)*

Source: Authors' analysis

The significance of sanctions should likewise be assessed in terms of enforcement strategy rather than nominal penalty levels alone. Comparative evidence from data-protection enforcement indicates that the deterrent value of sanctions depends on how supervisory authorities identify violations, prioritise cases, and deploy enforcement powers. The relevant comparison is therefore between the overall enforcement architecture of Indonesia and Singapore, rather than simply between their maximum statutory fines.[27]

The comparative table demonstrates that both Indonesia and Singapore recognise personal data protection as a fundamental component of electronic commerce, but the two jurisdictions structure their regulatory mechanisms differently. Indonesia has established a comprehensive statutory foundation through Law No. 27 of 2022 and Government Regulation No. 80 of 2019. Nevertheless, the Indonesian framework continues to face legal and institutional weaknesses, particularly because several operational requirements depend

[27] Maciej Pichlak and Klaudia Gaczoł, "Simple and Advanced Reflexivity in GDPR Enforcement: Empirical Evidence from DPA Activity," *International Data Privacy Law* 13, no. 4 (November 1, 2023): 267–83, https://doi.org/10.1093/idpl/ipad018; Jukka Ruohonen and Kalle Hjerppe, "The GDPR Enforcement Fines at Glance," *Information Systems* 106 (2022): 101876, https://doi.org/https://doi.org/10.1016/j.is.2021.101876.

on implementing regulations. For example, Article 53 of the PDP Law limits the obligation to appoint a DPO to specified forms of processing, including "large scale" and "high risk" processing. Because these criteria have not been accompanied by sufficiently clear operational benchmarks, PPMSE may face uncertainty regarding the circumstances in which a DPO is mandatory.[28] This uncertainty is compounded by the incomplete operationalisation of the personal data protection authority contemplated by Article 58 of the PDP Law and by limited public digital legal literacy, which may increase vulnerability to cybercrime.[29] From this perspective, the Indonesian problem is not merely the absence of rules but the incomplete institutionalisation of rules that already exist. The challenge is to translate statutory obligations into predictable organisational duties, measurable compliance benchmarks, and effective supervisory oversight.

The comparative assessment of Singapore is based on three principal legal and institutional indicators. First, Section 11(3) of the PDPA establishes a uniform requirement for organisations to appoint a DPO, regardless of business scale. Second, Part 6A, Section 26D establishes a clear threshold for notifiable data breaches and requires notification to the PDPC within a maximum of three calendar days. Third, the PDPA provides significant administrative sanctions under Section 48J(3) and, in specified circumstances, a right of private action under Section 48O. Together with the institutional role of the PDPC, these features contribute to a comparatively clear framework for compliance and enforcement. The comparison therefore suggests that Singapore provides a useful institutional and regulatory reference point, rather than a model that should be adopted wholesale in Indonesia. At the same time, the Singaporean framework should be read critically. The existence of a dedicated authority and clearer organisational obligations improves operational certainty, but effective supervision also requires institutional accountability and sufficient independence. This qualification prevents the comparison from becoming a simple assumption that the Singaporean model is inherently superior.[30]

Viewed through Philipus M. Hadjon's theory of legal protection, personal data protection cannot remain confined to formal statutory recognition; it must operate through effective preventive and repressive mechanisms, including enforcement and the restoration of rights. In this respect, Singapore provides a more operationally developed framework because its obligations are supported by established institutional mechanisms and

[28] Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital" 7, no. 1 (2024): 333–47, https://doi.org/https://doi.org/10.26623/julr.v7i1.8705.

[29] Rufinus Hotmaulana Hutauruk et al., "Meningkatkan Literasi Keuangan Digital Masyarakat Melalui Pemahaman Hukum Di Sektor Fintech," *Abdurrauf Journal of Community Service* 1, no. 2 (2024): 107–19, https://doi.org/10.70742/ajcos.v1i2.115.

[30] Bart Custers et al., "Quis Custodiet Ipsos Custodes? Data Protection in the Judiciary in EU and EEA Member States," *International Data Privacy Law* 12, no. 2 (May 1, 2022): 93–112, https://doi.org/10.1093/idpl/ipac002.

enforceable compliance procedures.[31] Indonesia, by contrast, continues to face limitations arising from incomplete implementing guidance and institutional arrangements. The comparison therefore indicates that effective personal data protection depends not only on the existence of legislation, but also on regulatory clarity, institutional readiness, and accessible enforcement and remedial mechanisms. The comparison therefore supports a more precise proposition: legal protection becomes effective when statutory rights are connected to organisational accountability, supervisory capacity, risk-based compliance mechanisms, and accessible enforcement. This proposition provides a stronger analytical bridge between Hadjon's preventive–repressive framework and contemporary data-protection governance.

3.2. Best Practices in Singapore and Their Potential Adaptation to Indonesia

Singapore provides a useful comparative reference in personal data protection not only because of the content of its statutory framework, but also because of the institutional mechanisms supporting implementation. Under the Personal Data Protection Act (PDPA) 2012, the PDPC plays a central supervisory role and provides practical guidance through its Advisory Guidelines and published enforcement decisions. Administrative penalties may also have a deterrent effect because they are linked to the financial position of regulated organisations. At the same time, the framework governing Data Protection Officers (DPOs) provides a clear institutional point of responsibility within organisations. These features make Singapore's experience potentially instructive for Indonesia, subject to appropriate contextual adaptation. The Singapore experience is particularly instructive in showing that compliance is not exhausted by the existence of a DPO or a statutory notification period. Contemporary data-protection governance increasingly relies on risk-based accountability, impact assessment, documented internal controls, and continuing regulatory learning. These dimensions are relevant to PPMSE because digital-commerce operations routinely involve profiling, large-scale processing, third-party service providers, and cross-border data flows.[32]

Within the digital commerce ecosystem, Electronic System Trade Operators (PPMSE) play a central role in collecting, managing, and storing users' personal data. Weaknesses in regulatory or supervisory arrangements may therefore have systemic implications for privacy and economic security. The complexity of digital supply chains, including infrastructure providers, logistics services, and third-party payment providers, further increases the risk of data breaches where compliance standards and enforcement mechanisms are not adequately coordinated. Singapore's regulatory and institutional

[31] Pardamean Harahap and Novita B R Simamora, "Legal Protection of Users ' Personal Data on E-Commerce Platforms Perlindungan Hukum Terhadap Data Pribadi Pengguna Di Platform E- Commerce" 11, no. 2 (2025): 345–52, https://doi.org/https://doi.org/10.37676/jhs.v11i2.9140.

[32] Margot E Kaminski and Gianclaudio Malgieri, "Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations," *International Data Privacy Law* 11, no. 2 (2021): 125–44, https://doi.org/10.1093/idpl/ipaa020.

experience is therefore relevant as a comparative reference for strengthening Indonesia's governance framework. The risk profile of digital commerce also means that compliance should extend beyond contractual assurances between PPMSE and third-party providers. Where processing involves significant risks to individuals, impact-assessment mechanisms and transparent accountability arrangements can provide an additional preventive layer. Cross-border processing also requires attention to the legal conditions governing international data transfers.[33]

This assessment rests on three principal legal and institutional indicators. First, institutional certainty and operational effectiveness: Sections 5(1) and 5(2) of the PDPA establish the institutional basis for the PDPC to perform its supervisory functions, including enforcement and the issuance of guidance. Second, compliance standardisation: Section 11(3) requires organisations to appoint a Data Protection Officer (DPO), thereby establishing a clear internal locus of responsibility for data protection. Third, sanction enforcement: Section 48J(3) provides for substantial financial penalties, including penalties linked to annual turnover in specified circumstances. Together, these features strengthen the predictability of compliance obligations and create economic incentives for organisations to invest in data security.[34]

The comparative analysis identifies three principal weaknesses in the Indonesian framework that warrant policy adaptation: institutional fragmentation, the uncertainty surrounding the scope of DPO obligations, and comparatively limited administrative fines under Article 57 of the PDP Law. Nevertheless, Indonesia should not adopt Singapore's framework directly. Any reform should instead be adapted to Indonesia's legal system, institutional capacity, and economic structure, particularly the significant role of micro, small, and medium enterprises (MSMEs). Accordingly, three reforms should be distinguished: institutionalisation of an accountable supervisory authority; clarification of proportionate, risk-based DPO and compliance duties; and strengthening of enforcement capacity. The objective is not to maximise regulatory burdens or fines, but to establish a credible compliance system in which obligations are predictable, proportionate, and capable of being enforced.

The findings further indicate that Indonesia's normative reforms have not yet been fully matched by effective implementation. Data breach cases involving digital infrastructure suggest that, although the rights of data subjects are recognised in law, their practical realisation remains dependent on the capacity of data controllers, sector-specific conditions, and the availability of effective enforcement mechanisms. The existence of

[33] Massimo Marelli, "Transferring Personal Data to International Organizations under the GDPR: An Analysis of the Transfer Mechanisms," *International Data Privacy Law* 14, no. 1 (February 1, 2024): 19–36, https://doi.org/10.1093/idpl/ipad022; Claes G Granmar, "Global Applicability of the GDPR in Context," *International Data Privacy Law* 11, no. 3 (August 1, 2021): 225–44, https://doi.org/10.1093/idpl/ipab012.

[34] Javan Setyagraha Pamungkas, Abdul Aziz Pamungkas,Yulianto Agustian, Sumarno, and Moch. Eko Setiyo B.U, "Pertanggungjawaban Pidana Atas Pelanggaran Data Pribadi Berbasis Kecerdasan Buatan Dalam Perspektif Perbandingan Hukum Pidana (Indonesia, Uni Eropa Dan Singapura)" 10, no. 2 (2026): 341–51, https://doi.org/https://doi.org/10.24127/mlr.v10i2.5438.

statutory rights under the PDP Law therefore does not, by itself, guarantee their effective enjoyment in practice. [35]

Tabel 2. Comparison of Compliance Principles in Indonesia and Singapore

Classification	Indonesia	Singapura
Data Protection Officer	Articles 53(1)–(3) of the PDP Law: dependent on scale. The provision should be clarified through measurable, proportionate, risk-based criteria; Singapore's mandatory organisational accountability provides a useful reference, but direct transplantation should be avoided.	Section 11(3) of the PDPA 2012: mandatory
Administrative sanctions	Articles 57(1)–(3) of the PDP Law and the PMSE Government Regulation: administrative sanctions in the form of fines of up to 2% of annual revenue; Indonesia should strengthen financial penalties against negligent or abusive PPMSE to create a deterrent effect.	*Section 48J(3) of the PDPA 2012: financial fines imposed by the PDPC of up to S$1 million, or 10% of the company's annual turnover where turnover exceeds S$10 million*
Institution	Article 58 of the PDP Law: establishment of an independent institution	*Sections 5(1) and (2) of the PDPA 2012: Singapore has a dedicated personal data protection authority, namely the Personal Data Protection Commission (PDPC)* *The PDPC provides an established supervisory structure; however, comparative scholarship emphasises that supervisory effectiveness should also be assessed through independence and accountability safeguards.*

Source: Authors' analysis

Overall, legal reform in Indonesia should strengthen personal data protection while preserving legal certainty and regulatory proportionality. In addition to strengthening the

[35] Mikael Purba, Suyud Margono, and Mas Agus Priyambodo, "Analisis Yuridis Perlindungan Data Pribadi Sebagai Hak Keperdataan Berdasarkan UU No 27 Tahun 2022 Tentang PDP," 2026, 16966–80, https://doi.org/https://doi.org/10.61104/alz.v4i4.11243.

independent supervisory authority and clarifying DPO obligations, the implementing regulations of the PDP Law should establish more detailed preventive requirements. These requirements could include a Personal Data Protection Impact Assessment before high-risk processing, records of processing activities, minimum technical and organisational security standards, and timely data breach notification in accordance with Article 46 of the PDP Law. An integrated framework combining independent supervision, proportionate sanctions, and preventive compliance standards would strengthen accountability and contribute to a more trustworthy digital commerce ecosystem.[36]

Institutional reform and stronger sanctions should be accompanied by clear preventive obligations. PPMSE should be required to conduct personal data impact assessments before undertaking processing activities that may pose significant risks to data subjects. They should also maintain records of processing activities, implement appropriate security measures—including encryption for data at rest and in transit—and report qualifying data breaches promptly while taking appropriate remedial action. [37] The supervisory authority should be empowered to issue technical guidance, conduct education and compliance programmes, and impose proportionate sanctions, including financial penalties and orders requiring system remediation. Effective supervision and enforcement can encourage digital businesses to strengthen data security, improve operational practices, and provide stronger protection for consumer privacy while supporting a secure and sustainable digital economy. [38]

Singapore's regulatory framework should not simply be transplanted into Indonesia. Adaptation must reflect Indonesia's legal conditions, institutional capacity, and business structure. Implementing regulations under the Personal Data Protection Law should clearly define the authority of the Personal Data Protection Authority and provide practical compliance guidance. The government should also engage digital industry associations and PPMSE in the development of implementation standards. DPO obligations should be proportionate and risk-based so that compliance requirements reflect the capacity and risk profile of different businesses, particularly MSMEs. A further safeguard is needed: the supervisory authority should itself be subject to transparent accountability mechanisms. Comparative scholarship on supervisory governance demonstrates that the question is not only who regulates private organisations, but also who oversees the regulator. Indonesia's institutional design should therefore combine

[36] Mohamad Gery Alfaaiz, "Perbandingan Regulasi Perlindungan Data Pribadi Antara Indonesia Dan Singapura Dalam Kinteks Kasus Worldcoin," *Journal Equitable* 8, no. 1 (2023): 95–110, https://doi.org/https://doi.org/10.37859/jeq.v10i3.9241.

[37] Sudjudiman and Najicha, "Pengaturan Pemutusan Hubungan Kerja (Phk) Di Indonesia Dan Singapura (Studi Perbandingan Hukum Indonesia Dan Hukum Singapura)."

[38] Fairuz Zahirah Zihni Hamdan et al., "Kebijakan Hukum Berperspektif Dampak Terhadap Data Pribadi: Indonesia Dan Singapore Dalam Asean Framework," 2024, 211–23.

operational independence with procedural accountability, reporting duties, and accessible review mechanisms.

4. Conclusion

Based on Philipus M. Hadjon's theory of legal protection, the comparison demonstrates that Indonesia has established a constitutional and statutory foundation for protecting personal data through Article 28G(1) of the 1945 Constitution, Law No. 27 of 2022 (PDP Law), and Government Regulation No. 80 of 2019 (PMSE Government Regulation). However, the effectiveness of preventive and repressive protection remains constrained by dependence on implementing regulations, the incomplete operationalisation of the personal data protection authority under Article 58 of the PDP Law, and the conditional scope of DPO obligations under Article 53. Singapore, by contrast, has developed a more operational framework through the PDPA and the PDPC, supported by clearer DPO requirements, data breach notification procedures, administrative sanctions, and specified avenues for private action. Indonesia should therefore pursue contextual adaptation rather than direct transplantation of the Singaporean model. Priority should be given to operationalising an independent supervisory authority, clarifying proportionate and MSME-sensitive DPO obligations, strengthening data breach notification and compliance standards, and ensuring that administrative sanctions are effective and proportionate. These measures would contribute to a safer, more accountable, and sustainable digital commerce ecosystem. The principal lesson is therefore institutional rather than transplant-oriented. Indonesia should strengthen the operational independence and accountability of its supervisory authority, clarify proportionate DPO obligations through measurable risk criteria, develop risk-based impact and compliance assessment for high-risk processing, strengthen breach-notification and security standards, and ensure that sanctions are proportionate but credible. These reforms would move the Indonesian framework from formal legal recognition toward a more operational system of preventive and repressive protection.

5. CRediT authorship contribution statement

Fariz Hassan Maulana: Conceptualization, Methodology, Investigation, Formal analysis, Writing – Original Draft, Writing – Review & Editing.

Nadia Carolina Weley: Conceptualization, Methodology, Supervision, Writing – Review & Editing, Project administration.

Rufinus Hotmaulana: Conceptualization, Validation, Supervision, Writing – Review & Editing.

6. References

Adhyputra, Muhammad Fadel, Thoriq Ahmadi, and Mohammad Rifqi. "Gagasan Perlindungan Data Pribadi Oleh LPPDP Indonesia: Sebuah Studi Perbandingan

Dengan Otoritas Pelindungan Data Pribadi Singapura." *Jurnal LeDHaK Fakultas Hukum Unhas* 2, no. 2 (2024): 304–21.

ALBAB, Muhammad Maulana Abdullah Ulil. "Batasan Keterlibatan Non-Pihak Dalam Pemeriksaan Persiapan Sengketa Tata Usaha Negara Berdasarkan Teori Perlindungan Hukum Philipus M.Hadjon Dan Sadd Adz-Dzariah: Studi Di Pengadilan Tata Usaha Negara." Universitas Islam Negeri Maulana Malik Ibrahin Malang, 2025.

Alfaaiz, Mohamad Gery. "Perbandingan Regulasi Perlindungan Data Pribadi Antara Indonesia Dan Singapura Dalam Kinteks Kasus Worldcoin." *Journal Equitable* 8, no. 1 (2023): 95–110. https://doi.org/https://doi.org/10.37859/jeq.v10i3.9241.

Badria, Lailatul, Dwiyanto Indiahono, and Sukarso. "Akuntabilitas Dalam Kebijakan Perlindungan Data Pribadi Di Indonesia Belajar Dari Korea Selatan Dan Singapura." *Manntra Pembaruan: Jurnal Inovasi Kebijakan* Vol. 8, no. No. 2 (2024): Hal. 89-102. https://doi.org/https://doi.org/10.21787/mp.8.2.2024.89-102.

Commission, Personal Data Protection. Personal Data Protection Commission [2023] SGPDPC 6 (2023).

Custers, Bart, Linda Louis, Maria Spinelli, and Kalliopi Terzidou. "Quis Custodiet Ipsos Custodes? Data Protection in the Judiciary in EU and EEA Member States." *International Data Privacy Law* 12, no. 2 (May 1, 2022): 93–112. https://doi.org/10.1093/idpl/ipac002.

Delia, Della, David Tan, and Shenti Agustini. "Regulasi Hukum Ekonomi Digital : Implikasi Undang-Undang Nomor 1 Tahun 2024 Terhadap E-Commerce Dan Start-Up Di Indonesia." *Unes Journal of Swara Justisia* 10, no. 1 (2026): 41–54. https://doi.org/https://doi.org/10.31933/d1hpnz59.

Diandra, Annisya, Mohammad Muarabagja Hatta, Sukma Kanthi Nurani, Adinda Alya Izdihar, and Novali Panji Nugroho. "Polemik Data Pribadi: 5 Kasus Kebocoran Data Di Indonesia Selama 2023-2024." *Tempo*, 2025.

Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia" 5, no. 1 (2023): 39–57. https://doi.org/https://doi.org/10.23887/glr.v5i1.2237.

Fitrahul Faizah, Azza, Sinta Dewi Rosadi, Garry Gumelar Pratama, and Ananda Fersa Dharmawan. "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," 2023. https://doi.org/https://doi.org/10.51903/hakim.v1i3.1222.

Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trading Through Electronic Systems (Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik) (2019).

Granmar, Claes G. "Global Applicability of the GDPR in Context." *International Data Privacy Law* 11, no. 3 (August 1, 2021): 225–44. https://doi.org/10.1093/idpl/ipab012.

Greenleaf, Graham. "The New Data Protection Convention 108+ and Its Importance for Asia." *International Journal of Law and Information Technology* 34 (January 1, 2026): eaaf024. https://doi.org/10.1093/ijlit/eaaf024.

Hamdan, Fairuz Zahirah Zihni, Rosa Ristawati, Mardianta Putra Anggara, and Nabilah Ghassani Hamdan. "Kebijakan Hukum Berperspektif Dampak Terhadap Data Pribadi: Indonesia Dan Singapore Dalam Asean Framework," 2024, 211–23.

Harahap, Pardamean, and Novita B R Simamora. "Legal Protection of Users ' Personal Data on E-Commerce Platforms Perlindungan Hukum Terhadap Data Pribadi Pengguna Di Platform E- Commerce" 11, no. 2 (2025): 345–52.

https://doi.org/https://doi.org/10.37676/jhs.v11i2.9140.

Heilynn, Markoni, I Made Kantikha, and Dyah Permata Budi Asri. "Perbandingan Penyelesaian Hukum Perkara Penyebaran Data Pribadi Di Media Massa Antar Indonesia Dan Singapura." *Almufi Jurnal Sosial Dan Humaniora* 2, no. 3 (2025). https://doi.org/https://doi.org/10.63821/ash.v2i3.574.

Hutauruk, Rufinus Hotmaulana, Emiliya Febriyani, Hari Sutra Disemadi, Lu Sudirman, Rahmi Ayunda, and Agustianto. "Meningkatkan Literasi Keuangan Digital Masyarakat Melalui Pemahaman Hukum Di Sektor Fintech." *Abdurrauf Journal of Community Service* 1, no. 2 (2024): 107–19. https://doi.org/10.70742/ajcos.v1i2.115.

Jayanti, Puput Leni. "Pengaruh Daya Tarik Host , Atribut Anchor Dan Diskon Terhadap Minat Beli Produk Dahion Muslim Pada Live Streaming Shopee." *Nucl. Phys.* 13, no. 1 (2026): 104–16.

Kaminski, Margot E, and Gianclaudio Malgieri. "Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations." *International Data Privacy Law* 11, no. 2 (2021): 125–44. https://doi.org/10.1093/idpl/ipaa020.

Kharisma, Dona Budi, and Alvalerie Diakanza. "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union." *International Journal of Human Rights in Healthcare* 17, no. 2 (September 6, 2022): 157–69. https://doi.org/10.1108/IJHRH-04-2022-0035.

"Law Number 27 of 2022 Concerning Personal Data Protection (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi)," 2022.

Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital" 7, no. 1 (2024): 333–47. https://doi.org/https://doi.org/10.26623/julr.v7i1.8705.

Marelli, Massimo. "Transferring Personal Data to International Organizations under the GDPR: An Analysis of the Transfer Mechanisms." *International Data Privacy Law* 14, no. 1 (February 1, 2024): 19–36. https://doi.org/10.1093/idpl/ipad022.

Muhayar, Fitra Deni, and Zulfadli Barus. "Cyber PPAT and Legal Certainty in Indonesia ' s Electronic Land Certification System." *Al-Adalah : Jurnal Hukum Dan Politik Islam* 10, no. 1 (2025): 201–17. https://doi.org/doi.org/10.30863/ajmpi.v10i1.8473.

Nova Adistiya, Kadek, Si Ngurah Ardhya, Putu Riski Ananda Kusuma, and Muhamad Jodi Setianto. "Perlindungan Hukum Bagi Konsumen Terhadap Kebocoran Data Pribadi Berdasarkan Pasal 16 Ayat 2 Huruf E Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *MyGovernment* 4, no. 1 (2024): 1–13. https://doi.org/https://doi.org/10.23887/jih.v4i3.5034.

Pamungkas, Abdul Aziz Pamungkas,Yulianto Agustian, Javan Setyagraha, Sumarno, and Moch. Eko Setiyo B.U. "Pertanggungjawaban Pidana Atas Pelanggaran Data Pribadi Berbasis Kecerdasan Buatan Dalam Perspektif Perbandingan Hukum Pidana (Indonesia, Uni Eropa Dan Singapura)" 10, no. 2 (2026): 341–51. https://doi.org/https://doi.org/10.24127/mlr.v10i2.5438.

Pichlak, Maciej, and Klaudia Gaczoł. "Simple and Advanced Reflexivity in GDPR Enforcement: Empirical Evidence from DPA Activity." *International Data Privacy Law* 13, no. 4 (November 1, 2023): 267–83. https://doi.org/10.1093/idpl/ipad018.

Purba, Mikael, Suyud Margono, and Mas Agus Priyambodo. "Analisis Yuridis Perlindungan Data Pribadi Sebagai Hak Keperdataan Berdasarkan UU No 27 Tahun 2022 Tentang PDP," 2026, 16966–80.

https://doi.org/https://doi.org/10.61104/alz.v4i4.11243.

Rahmah, Annisa Putri AzizulRahmah, Putri Olivia Anggraini, and Muhammad Hasbi. "Perlindungan Data Pribadi Sebagai Hak Asasi Manusia Di Era Digital : Analisis Dan Perbandingan Indonesia Dan Singapura," 2026, 3242–49. https://doi.org/https://doi.org/10.61104/alz.v4i3.5839.

Ruohonen, Jukka, and Kalle Hjerppe. "The GDPR Enforcement Fines at Glance." *Information Systems* 106 (2022): 101876. https://doi.org/https://doi.org/10.1016/j.is.2021.101876.

Suari, Kadek Rima Anggen, and I Made Sarjana. "Menjaga Privasi Di Era Digital : Perlindungan Data Pribadi Di Indonesia," no. 1 (2023): 132–46. https://doi.org/https://doi.org/10.38043/jah.v6i1.4484.

Sudirman, Lu, and Hari Sutra Disemadi. "Titik Lemah Industri Keuangan Fintech Di Indonesia : Kajian Perbandingan Hukum" 4 (2022). https://doi.org/https://doi.org/10.14710/jphi.v4i3.471-493.

Sudjudiman, Haikal Narendra, and Fatma Ulfatun Najicha. "Pengaturan Pemutusan Hubungan Kerja (Phk) Di Indonesia Dan Singapura (Studi Perbandingan Hukum Indonesia Dan Hukum Singapura)" 4, no. 2 (2020): 40–50. https://doi.org/doi.org/10.25299/uirlrev.2020.vol4(2).6767.

Sukerta, Putu Aryan Darma, and Andri Sutrisno. "Personal Data Protection in ASEAN: A Critical Comparison between Indonesia's and Malaysia's Legal Frameworks." *Constitutional Law Review* 3, no. 2 (2024): 133–47.

Sutarli, Ananta Fadli, and Shelly Kurniawan. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia." *INNOVATIVE: Journal Of Social Science Research* 3 (2023): 4208–21.

Undang -Undang Dasar Negara Republik Indonesia Tahun 1945 (1945).

Weley, Nadia Carolina, and Hari Sutra Disemadi. "Implikasi Hukum Pemasangan CCTV Di Tempat Umum Secara Tersembunyi Terhadap Perlindungan Data Pribadi." *Amnesti: Jurnal Hukum* 4, no. 2 (2022): 79–93. https://doi.org/10.37729/amnesti.v4i2.2151.

Wibowo, Yulianto, Ida Aryati Dpw, and Iismiyanto. "Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi." *Jurnal Serambi Hukum* 18, no. 01 (2025): 1–6. https://doi.org/https://doi.org/10.59582/sh.v18i01.1216.

Widiatedja, I Gusti Ngurah Parikesit, and Neha Mishra. "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective." *International Review of Law, Computers & Technology* 37, no. 3 (September 2, 2023): 252–73. https://doi.org/10.1080/13600869.2022.2155793.

Wong YongQuan, Benjamin. "Data Privacy Law in Singapore: The Personal Data Protection Act 2012." *International Data Privacy Law* 7, no. 4 (November 1, 2017): 287–302. https://doi.org/10.1093/idpl/ipx016.

Yeung, Karen, and Lee A Bygrave. "Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship." *Regulation & Governance* 16, no. 1 (January 1, 2022): 137–55. https://doi.org/https://doi.org/10.1111/rego.12401.