PALAR (Pakuan Law Review)
https://journal.unpak.ac.id/index.php/palar

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Protection of Investors' Personal Data in *Initial Public Offerings* in Indonesia and Singapore

Nywara Natriyasmara Lubis[1]; Nadia Carolina Weley[2]; Agustianto[3].

Faculty of Law, Batam International University
Email: 2351113.nywara@uib.edu, Nadia.carolina@uib.ac.id, agustianto.lec@uib.ac.id
Manuscripts received : 16/09/2026, Revision and Review : 25/09/2026, Approved 30/09/2026

Abstract

This study aims to analyze and compare the protection of investors' personal data at the stage of registration, verification, and allocation of shares in the Initial Public Offering (IPO) process, as well as the form of sanctions for the impact of data leaks in the Indonesian and Singapore capital markets. Digital transformation through the Electronic Initial Public Offering (e-IPO) system facilitates investment access but poses massive cyber risks due to the processing of sensitive financial data. The research method used is normative legal research with a statute approach. The results of the study show that there is a disharmony of norms in Indonesia between the principle of full disclosure of capital markets based on the Capital Market Law and the principle of data minimization in the Personal Data Protection Law (PDP Law), which is complicated by the obligation of due diligence of bank statements based on SEOJK Number 25/SEOJK.04/2025 without being accompanied by clear cybersecurity technical standards. In contrast, Singapore aligns exchange activities with privacy through the position of the Securities and Futures Act (SFA) and MAS Notice SFA04-N02 as lex specialis, although the security standards remain general. Analyzed through Philipus M. Hadjon's Repressive Legal Protection Theory, sanctions enforcement in Indonesia is considered less effective in fulfilling the functions of simultaneous recovery, deterrence, and legal certainty, due to the fragmentation of authority between the OJK and the Personal Data Protection Supervisory Agency (LPPDP), administrative fines that are still flat, and the criminal path of the PDP Law that is doctrinally difficult to reach negligent data controllers. Singapore applies turnover-based administrative fines of up to 10% or S$1,000,000 under Section 48J of the PDPA as well as Section 480 of the PDPA's right of personal action, although its application is still limited by institutional discretion and the requirement of proof of loss. This study recommends more operational repressive legal reforms, including revisions to administrative fine implementing regulations, OJK-LPPDP memorandums of understanding, and simple lawsuit mechanisms for investors.

Keywords: Personal Data Protection; Investors; Singapore; Indonesia.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

A. Introduction

Investment in Indonesia is growing rapidly, especially with technological advancements that allow people to invest through digital applications, online banking, and digital wallet platforms. Investors, which refer to individuals or entities who buy shares of companies with the aim of making a profit, play an important role in driving the capital market. This digital transformation has transformed the capital market landscape into a borderless, but at the same time it has created new vulnerabilities to data access by unauthorized parties in the electronic trading system [1]. Companies that do *Initial Public Offering* (IPO) is the company that first offered its shares to the public to raise funds. In this process, investors' personal data, such as names, addresses, and identity numbers, will be collected and managed. A Katadata survey showed that 52% of respondents considered investment apps vulnerable to data leaks, followed by 49% on digital banking, and 48% on digital wallets.[2] Therefore, the protection of investors' personal data in IPOs is essential to ensure public trust and protect sensitive information used in the company's stock offering process. Theoretically, trust is the main foundation of capital market integrity, where the absence of robust legal protections can trigger price distortions and declining public participation [3].

Article 6 of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) which stipulates that the collection of personal data can only be carried out with the explicit consent of the data owner, and Section 13 *Personal Data Protection Act 2012 Singapura* (PDPA) which stipulates that personal data must be collected with explicit consent, data leakage that occurs in Observe, which results in around 2.9 million user data hacked, as well as hacking Lazada which involves 1.1 million customer accounts by platformer RedMart, demonstrating the importance of strong personal data protection [4]. This cyber infrastructure failure proves that law enforcement in Indonesia still tends to be administrative and has not provided a deterrent effect equivalent to the turnover-based fine sanction model in Singapore [5]. In addition, the case Tokenize Xchange in Singapore, which ceased its operations and is under police investigation after *Monetary Authority of Singapore* (MORE) rejected its license application, adding to the concerns. A number of investors, such as George Tan, a retiree who has invested S$ 23,000, trapped in uncertainty after the platform abruptly shut down services, causing Investment Losses that cannot be

[1] Nyoman Nidia, Sari Hayati, and Sri Warjiyati, "Juridical Analysis of the Concept of Omnibus Law in the Harmonization of Laws and Regulations in Indonesia," *Journal of Justice Ocean Law* 16, no. 1 (2021): 1–18.

[2] (Catadata Databox, 2021)

[3] Hasbuddin Khalid, "Law and Investment: Aspects of Legal Protection by Financial Services Authorities for Capital Market Investors," *Unes Law Review* 6, no. 1 (2023): 737–45, https://review-unes.com/https://creativecommons.org/licenses/by/4.0/.

[4] CNN Indonesia, "2.9 Million User Data Cermati.Com Hacked," 2020, https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/9e47e8a7538de5d/survei-ini-produk-keuangan-yang-dianggap-rentan-kebocoran-data%0A https://www.cnnindonesia.com/teknologi/20201102103348-185-564812/29-juta-data-pengguna-cermaticom-diretas.

[5] Tiara Almira Raila, Sinta Dewi Rosadi, and Rika Ratna Permata, "Privacy Data Protection in Indonesia and Singapore Related to the Implementation of Digital Contact Tracing as an Effort to Prevent Covid-19 and Its Responsibilities," *Journal of Legal Certainty and Justice* 2, no. 1 (2021): 1, https://doi.org/10.32502/khdk.v2i1.3044.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

defrosted [6]. These cases underscore the importance of implementing stricter security measures and personal data protection regulations that can prevent misuse and data leakage to the detriment of all parties involved.

Previous research studies have provided a foundation for this issue, but still leave significant analytical gaps. Research by Raila (2020) compared the privacy regulations of Indonesia and Singapore with the finding that Singapore has a more integrated Public Sector Governance Act (PSGA) and PDPA framework in mitigating the risk of data misuse than Indonesia [7]. Meanwhile, Kharlie et al. (2025) emphasized that Singapore's protection model is more business-centric that provides certainty for issuers, while Indonesia still faces challenges in cross-border data protection (*cross-border)* for multinational companies [8]. Jasmine (2024) dissects the protection for minority shareholders in IPOs, but finds that information asymmetry remains a major obstacle to retail investors due to weak transparency of non-financial risks, including data risk [9].

Furthermore, Darmawan and Putri (2025) evaluated the effectiveness of the IOSCO principle in protecting investor data against cyber threats, which concluded the need for the establishment of an independent supervisory authority in Indonesia to avoid dualism of authority with the OJK [10]. Pohan et al.'s (2023) research examined the application of the principle of full disclosure and found that current regulations do not emphasize severe enough sanctions for issuers who hide material facts related to the security of their electronic systems [11]. The advantage of this research compared to previous studies is the specific focus on the IPO stage which involves verifying investor liquidity data. The novelty of this research lies in the analysis of the impact of the implementation of SEOJK Number 25 of 2025 which requires underwriters to conduct due diligence on the proof of retail investors' bank statements, which analytically has the potential to violate the right to privacy if not synchronized with the PDP Law. The scope of personal data protection in Indonesia's positive law has generally been mapped, but has not yet touched the sectoral context of the capital market [12]. The regulatory gap on data proportionality in digital banking in the ASEAN region, including Indonesia, has also been identified, showing that

[6] Fintech News Singapore, "Tokenize Xchange Shutdown Leaves Investors in Limbo," 2025, https://fintechnews.sg/116488/crypto/tokenize-xchange-shutdown-singapore-investors/.

[7] Raila, Rosadi, and Permata, "Privacy Data Protection in Indonesia and Singapore Related to the Implementation of Digital Contact Tracing as an Effort to Prevent Covid-19 and Its Responsibilities."

[8] Ahmad Tholabi Kharlie et al., "Comparative Analysis of Personal Data Protection in Indonesia and Singapore for a Sustainable Digital Future," *Towards Resilient Societies: The Synergy of Religion, Education, Health, Science, and Technology*no. Fuster 2014 (2025): 593–98, https://doi.org/10.1201/9781003645542-95.

[9] Alifia Jasmine et al., "Initial Public Offering: Legal Protection of Minority Shareholders and Their Influence on Company Performance," *Journal of Law & Development* 54, no. 1 (2024), https://doi.org/10.21143/jhp.vol54.no1.1606.

[10] Kevin Darmawan and Aninditha Sekar Putri, "Legal Protection for Investors' Personal Data Against Cybercrime Threats in Capital Market Based on IOSCO Principles," *Journal of Law, Politic and Humanities* 5, no. 4 (2025): 2293–2303, https://doi.org/10.38035/jlph.v5i4.1458.

[11] Ghiffary Akmal Alija Pohan, FX. Joko Priyono, and Ery Agus Priyono, "Application of Principle Full Disclosure and Legal Protection for Investor Due To Market Manipulation of Shareprices By Issuers in Capital Market," *Creep* 5, no. 1 (2023): 104–15, https://doi.org/10.14710/crepido.5.1.104-115.

[12] Muhammad Fikri and Shelvi Rusdiana, "The Scope of Personal Data Protection: A Study of Indonesian Positive Law," *Ganesha Law Review* 5, no. 1 (2023): 125–39, https://doi.org/https://doi.org/10.23887/glr.v5i1.2237.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

the problem of disharmony in the principle of data minimization also extends to other digital financial services sectors, not just the capital market [13]. Weak implementation of the right to be forgotten *(right to be forgotten)* in Indonesia compared to South Korea, the United States, and the European Union are also benchmarks for post-leak data subject rights restoration standards [14]

The legal issues raised in this study include the potential conflict of norms between the obligation to verify investor funds by underwriters with data minimization standards in the PDP Law, as well as the unclear form of proportionate sanctions for companies in the capital market. The disharmony of authority between the OJK as the supervisor of the financial sector and the new PDP authority can create legal uncertainty in the enforcement of sanctions for data leaks [15]. Based on this identification, the formulation of the problem in this study is how the regulation of investor personal data protection in the IPO process in Indonesia and Singapore is reviewed from the perspective of ius constitutum, as well as how the form of sanctions against companies for the impact of investor data leaks on the capital market in both countries. The purpose of this study is to analyze the synchronization of sectoral regulations with privacy laws, as well as to evaluate the effectiveness of the administrative and criminal sanctions regime to ensure legal certainty for investors.

This research uses the foundation of legal protection theory developed by Philipus M. Hadjon as the main analysis knife. Hadjon (1987) divides legal protection into two instruments, namely preventive protection which aims to prevent disputes through regulations and licensing procedures, and repressive protection which focuses on dispute resolution and sanctions enforcement [16]. In the digital realm, preventive protection is manifested through cybersecurity audits and liabilities *Data Protection Impact Assessment* (DPIA), while repressive protection includes the right of private action to claim compensation for data loss [17]. Theoretically, this research contributes to the development of information technology law in conceptualizing "personal data as an investment asset". Practically, this study provides recommendations for regulators (OJK and MAS) in harmonizing cyber data governance standards. The limitation of this research lies in the focus of analysis which is limited to the initial market phase (IPO) and only covers the jurisdiction of Indonesia and Singapore.

---

[13] Agustianto Agustianto et al., "Regulatory Gaps in Data Protection and Proportionality in Digital Banking: Legal Issues in ASEAN," *Syura: Journal of Law* 4, no. 1 (2026): 55–86, https://doi.org/https://doi.org/10.58223/syura.v4i1.811.

[14] Ampuan Situmeang et al., "International Journal of Educational Review, Law, and Social Sciences (IJERLAS)," *International Journal of Educational Review, Law, and Social Sciences (IJERLAS)* 6, no. 1 (2026): 184–94, https://doi.org/10.3390/fi17020083.13.

[15] Salwa Naya Syakirah and Haipa Nisrina Sayyidah, "The Urgency on Strengthening the Implementation of Personal Data Protection for Equity Crowdfunding Financial Services Sector Financiers in Indonesia (A Comparative Study of Malaysia) The Urgency on Strengthening Implementation of Personal Data Protection for Fins" 12 (2024): 109–22.

[16] Philipus M. Hadjon, *Legal Protection for the People in Indonesia: A Study of Its Principles, Its Handling by the Courts in the General Judiciary and the Establishment of State Administrative Courts* (Surabaya: Bina Ilmu, 1987).

[17] Azza Fitrahul Faiza et al., "Strengthening Personal Data Protection through Supervisory Authorities in Indonesia Based on a Comparison of Hong Kong and Singapore Laws," *Judge: Journal of Law and Social Sciences* 1 (2023).

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

B. Research Methods

This research uses a type of normative legal research. The approach used is a statute approach by examining all regulations related to the issue of protecting investors' personal data in the Initial Public Offering process [18]. Data collection was carried out through a literature study of secondary legal materials.

Primary legal materials in this study include Law Number 27 of 2022 concerning Personal Data Protection, Law Number 8 of 1995 concerning Capital Markets, Personal Data Protection Act 2012 Singapore, and Securities and Futures Act (SFA) Singapore. Second, secondary legal materials include Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, as well as the Financial Services Authority Regulation (POJK) and the Financial Services Authority Circular Letter (SEOJK) related to the implementation of electronic public offerings (e-IPO). Third, tertiary legal materials include the Code of Corporate Governance as well as regulations and operational guidelines from the Monetary Authority of Singapore (MAS).

The data collection technique applied in this study is library research by tracing, inventorying, and systematically examining these legal documents and laws and regulations. Finally, the type of analysis method used is the analytical descriptive method, in which all legal materials that have been collected are carefully described and critically analyzed in order to draw prescriptive legal conclusions regarding the protection of investors' personal data in the stock exchanges in Indonesia and Singapore.

C. Results and Discussion

1. Investor Personal Data Protection Arrangements in the *Initial Public Offering Process* in Indonesia and Singapore

Investor personal data protection arrangements in the process *Initial Public Offering* (IPO) is a crucial meeting point between two different legal regimes, namely personal data protection law and capital market law. Theoretically, personal data protection policies in Indonesia adopt a state-centric approach (*state-centric*), which is reflected in the strict basis for data processing as stipulated in Article 20 paragraph (2) of the PDP Law and the technical-organizational security obligations in Article 35 of the PDP Law, while Singapore uses a business-centric model (*business-centric*) which is apparent from the breadth of the consent exemption for commercial interests and sectoral compliance as set out in Part 3 of the Personal Data Protection Act 2012 (PDPA) and MAS Notice SFA04-N02 [19]. This difference in philosophical underpinnings has very significant normative implications, especially in responding to the challenges of governance of biometric data and sensitive financial information of retail financiers in the initial public offering phase [20]. These fundamental differences affect how each

[18] Silk Day is enshrined, "The Lens of Legal Research: A Descriptive Essay on Legal Research Methodology," *Journal of Judicial Review* 24, no. 2 (2022): 289–304, http://dx.doi.org/10.37253/jjr.v.

[19] Kharlie et al., "Comparative Analysis of Personal Data Protection in Indonesia and Singapore for a Sustainable Digital Future."

[20] (Alfaaiz and Gery, 2025)

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

country integrates privacy protections into its initial offering mechanisms, which are highly technical and require information disclosure.

Within Indonesia's positive legal framework, the protection of the personal data of investors participating in e-IPOs is generally controlled by the PDP Law as a lex generalis. However, because the nature of transactions in the capital market is very dynamic and full of information asymmetry, the processing of such data is also subject to sectoral regulations issued by the Financial Services Authority [21]. The use of electronic platforms in the stock exchange (e-IPO) requires investors to submit a series of sensitive data such as identity cards, collateral account numbers, and Single Investor Identification (SID) in order to meet the principles of legality and information disclosure [22]. This aims to ensure the validity of transactions in the primary market and facilitate the registration of integrated digital accounts on the official e-ipo.co.id website electronically. This registration system launches the obligation for prospective investors to upload ID card documents and connect their securities accounts to securities as part of customer validation [23].

The horizontal synchronization analysis identifies a normative tension between the data minimization principle and the disclosure requirements of capital market law, though the tension requires careful delineation. The full disclosure obligation under Article 1 number 25 in conjunction with Article 78 and Article 80 of Law Number 8 of 1995 concerning the Capital Market binds the issuer to disclose material information about its business, financial condition, and risk factors in the prospectus; it does not, on its own terms, require the public disclosure of individual investors' personal data. The actual friction lies elsewhere, in the scope and retention of the investor data that underwriters, custodians, and securities administration bureaus collect for verification purposes during the subscription process, namely identity documents, account numbers, and bank statements. Capital market regulations do not specify how long this verification data may be kept, who beyond the verification process may access it, or whether it may be reused for purposes other than allotment, which leaves room for the kind of purpose creep that the minimization principle in Article 20 paragraph (2) in conjunction with Article 35 of the PDP Law is designed to prevent (Pohan et al., 2023). The concern, in other words, is not that full disclosure pushes investors' data into the public domain, but that the administrative process built to satisfy capital market verification requirements collects and circulates sensitive investor data without a correspondingly clear limit on its later use (Suardana et al., 2020). Article 78 and Article 80 of the Capital Market Law and Article 20 paragraph (2) of the PDP Law are accordingly not in direct conflict; the absence of implementing rules connecting the two,

[21] Emir Adzan Syazali, "Legal Protection for Investors in Initial Public Offerings (IPOs): Between Das Sein and Das Sollen," *Al-Qanun: Journal of Islamic Law Thought and Reform* 28, no. 2 (2025), https://doi.org/https://doi.org/10.15642/alqanun.2025.28.2.269-283.

[22] Nidia, Hayati, and Warjiyati, "Juridical Analysis of the Concept of Omnibus Law in the Harmonization of Laws and Regulations in Indonesia."

[23] Abdul Malik, "Definition, Stages, and How to Buy It," Bareksa, 2025, https://www.bareksa.com/berita/saham/2025-12-02/e-ipo-pengertian-tahapan-dan-cara-belinya.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

however, still leaves investors exposed to an information asymmetry that data controllers could exploit in the absence of clearer purpose limitation.

This clash of legal principles became more evident after the enactment of new regulations through the Financial Services Authority Circular Letter (SEOJK) Number 25/SEOJK.04/2025 which came into effect on November 17, 2025. This circular tightens the mechanism for supervising electronic public offerings of shares by dividing the portion of centralized allotment allocation (pooling allotment) equally between retail and non-retail investors in order to create a fairer market. This regulatory step is taken by the OJK to minimize unreasonable price volatility and increase the confidence of the investor community in a sustainable manner [24]. However, this policy has the consequence of much more massive data processing at the level of securities selling agents due to the integration of administrative systems that require instant verification of customer identities.

Despite its stated aim of improving market fairness, SEOJK Number 25/SEOJK.04/2025 leaves a vacuum of technical norms concerning the cybersecurity of financiers' financial data. Section III of the circular, on the verification of interest and/or orders for Fixed Allotment, requires underwriters (*underwriter*) to conduct due diligence (*due diligence*) on Fixed Allotment investors, to be carried out, among other means, by examining the bank statement or other documents evidencing liquid asset ownership of the investor for a period of at least three months before the submission of interest and/or orders, in order to mitigate the risk of large-scale fictitious orders that often distort price discovery on the first day of listing (Setiawan Budi, 2025). This obligation is reinforced by Article 23 letter b of POJK Number 13 of 2025 concerning Internal Control and Conduct of Securities Companies Acting as Underwriters and Broker-Dealers, which separately requires the bookkeeping function of underwriters to verify that Fixed Allotment investors hold sufficient funds by examining their bank statements. Both instruments are presently in force rather than proposed reforms: SEOJK 25/2025 took effect on 17 November 2025, and POJK 13/2025, enacted on 11 June 2025, took effect on 11 December 2025, so the bank statement verification obligation this study examines rests on two overlapping regulations already binding on underwriters. Neither instrument, however, refers to the four minimum technical security parameters set out in Articles 35 to 39 of the PDP Law, namely: (1) the encryption and technical-operational obligations that protect bank statement data from unauthorized access (Article 35 of the PDP Law); (2) the obligation to periodically audit every party involved in processing the data (Article 37 of the PDP Law); (3) a limit on how long (*retention period*) the bank statement data may be kept once the verification and allocation process concludes; and (4) a restriction on access rights (*access control*) to only those officers authorized to verify liquidity (Article 39 paragraph (1) of the PDP Law). The absence of a cross-reference between the capital market rules and the PDP

[24] Yulianto Syahyu, "Legal Protection of Investor in the Indonesian Capital Market," *International Journal of Research and Review* 12, no. 11 (2025): 85–94, https://doi.org/10.52403/ijrr.20251110.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Law leaves each underwriter to set its own security standard for this highly sensitive financial data.

This practical challenge is increasingly evident because the underwriters of securities (*underwriter*) and securities companies are private entities that have varying levels of cybersecurity maturity. In the absence of uniform encryption standards and without periodic audit obligations set by the OJK, the processing of highly detailed bank statement data by securities parties is at high risk of data leakage due to cyber attacks or misuse by insiders [25]. In the absence of cybersecurity standardization, the collection of financial transaction files without qualified encryption is prone to being used by cybercriminals to launch cyberattacks targeting investors' financial accounts [26]. No clear regulation regarding storage time limits (*retention period*) and restriction of access rights to such bank statement data, securities companies may misuse investors' sensitive information for commercial purposes outside of exchange transactions [27].

Processing Policy	Terms & Practices in Indonesia	Terms & Practices in Singapore
Consent	It must be the primary basis for non-CDD activities, such as e-IPO account registration and marketing of additional investment products; must be explicit and cannot be incorporated in default approval (Article 20 paragraph (2) letter a of the PDP Law)	It remains a general basis under Part 3 of the PDPA, but is not the only basis applicable in the context of the capital market
Legal Obligation of Data Controller	Underpinning the obligation of due diligence of current accounts by underwriters in SEOJK Number 25/SEOJK.04/2025 (Article 20 paragraph (2) letter c of the PDP Law), so that normatively it does not require investor approval	Underlies the Customer Due Diligence (CDD)/Anti-Money Laundering (AML) obligations for underwriters and stockbrokers under MAS Notice SFA04-N02, which is explicitly excluded from the approval obligation
Legitimate Interest/Other Processing Policy	It has not been used explicitly by capital market players due to the lack of technical guidance	It is widely used by issuers and securities companies for risk management

[25] Darmawan and Putri, "Legal Protection for Investors' Personal Data Against Cybercrime Threats in Capital Market Based on IOSCO Principles."

[26] Indira Pratiwi, "Legal Protection for Investors in the Implementation of Stock Transactions with Online Trading System," *Dharmasisya: Journal of the Master of Law Program, Faculty of the University of Indonesia* 2, no. January (2023): 1335–37.

[27] Kurniastuti Sri Fajariah and Niru Anita Sinaga, "Legal Protection for Consumers in Buying and Selling Transactions through the Bukalapak E-Commerce Platform," *Lex Progressium* 1, no. 2 (2024): 153–69.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

(Legitimate Interest, etc.)	from the OJK and LPPDP regarding its limits	purposes and is directed through the PDPC Advisory Guidelines (Lim et al., 2025), thus providing flexibility but potentially reducing data subject control

The problem of legal implementation is further exacerbated by the confusion of understanding the basis for processing investor data in the digital e-IPO system, especially the erroneous assumption that all processing of investor data must always be based on consent. In fact, Article 20 paragraph (2) of the PDP Law expressly recognizes six legal data processing bases, namely data subject consent, fulfillment of contractual obligations, fulfillment of legal obligations of data controllers, protection of the vital interests of data subjects, implementation of public interest duties, and fulfillment of other legitimate interests. On the one hand, investment platforms often claim to have obtained consent from investors through default consent combined in a lengthy privacy policy, so that they do not meet the voluntary and explicit consent standards and violate the digital human rights of investors. On the other hand, the obligation of due diligence of current accounts in SEOJK Number 25 of 2025 is actually more appropriately categorized as data processing on the basis of the legal obligations of data controllers, not on the basis of consent, so investors should not be asked for separate consent for the process. The confusion in the use of this processing basis is what creates uncertainty, both for investors in understanding their rights, and for industry players in developing compliance policies.

To clarify the basic differences in the processing of investors' personal data that are relevant in the IPO process, the following table presents the mapping based on Article 20 paragraph (2) of the PDP Law as well as the applicable provisions in Singapore:

Horizontally, Indonesia also faces a prospective conflict of authority between the OJK and the Personal Data Protection Supervisory Institution (LPPDP) that the PDP Law mandates but that has not yet been established. Under current law, the OJK already exercises sanctioning authority over data-related violations in adjacent segments of the financial sector: Article 85 of POJK Number 57/POJK.04/2020 concerning Securities Offerings through Information Technology-Based Crowdfunding Services grants the OJK full authority to impose administrative sanctions within the securities crowdfunding segment it governs, including for conduct connected to the mishandling of investor data (Syakirah & Sayyidah, 2024). For a traditional public offering such as the IPO process this study examines, the OJK draws its general sanctioning authority instead from Article 102 of the Capital Market Law, which allows it to impose administrative sanctions on any party holding a licence, approval, or registration from the OJK, including underwriters and securities companies, for violations of the Capital Market Law and its implementing regulations. What remains unsettled is not whether the OJK may act under its present

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

mandate, but how this existing sectoral authority will be reconciled, once the LPPDP is formed under Article 58 and Article 60 of the PDP Law, with the LPPDP's prospective authority to investigate and sanction personal data violations across all sectors (Nurdin et al., 2024). Because the PDP Law establishes the LPPDP as a matter of future law rather than present law, this jurisdictional question is prospective rather than a conflict between two currently enacted norms. The absence of a coordination mechanism between the two institutions nonetheless creates legal uncertainty for issuers and financial industry participants, who must draft their cyber compliance policies against the risk of an enforcement overlap once the LPPDP becomes operational.

Turning to peer jurisdictions, Singapore adopted a much more established model of personal data regulation through the Personal Data Protection Act 2012 (PDPA). The existence of an independent supervisory body, the Personal Data Protection Commission (PDPC), has proven effective in harmonizing personal data protection compliance in the private sector without hindering the pace of financial innovation [28]. The Singapore PDPA is designed to balance the interests of individual privacy protection with the needs of organizations to process personal data for reasonable and legitimate commercial purposes [29]. This standardization is closely monitored by the PDPC which has the authority to issue special implementation guidelines (*Advisory Guidelines)* to guide data governance in the financial services industry [30].

The synchronization between privacy law and capital market regulation in Singapore is highly structured through various official circulars issued by the Monetary Authority of Singapore (MAS). The MAS financial authority has full authority to integrate information technology security standards for all capital market industry players through the issuance of binding Notices [31]. This alignment aims to maintain the credibility and stability of the financial system from the increasingly rampant cross-border cyber threats in the international stock exchange area. This harmonization results in integrated operational rules that limit the movement of financial criminals while consistently protecting customers' privacy rights.

A very significant legal exception in Singapore is governed by MAS Notice SFA04-N02 on the Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries which is updated with effective effect in July 2025. Under this Notice SFA04-N02, underwriters and stockbrokers are granted the explicit right of exemption to collect, use and disclose the personal data of potential investors without the need to obtain consent (*Agree*) specific to the data owner. This legal exception is designed to

[28] Faiza et al., "Strengthening Personal Data Protection through Supervisory Authorities in Indonesia Based on a Comparison of Hong Kong and Singapore Laws."

[29] Fairuz Hamdan et al., "Legal Policy with an Impact on Personal Data: Indonesia and Singapore in the ASEAN Framework," *Proceedings of Airlangga Faculty of Law Colloquium* 1 (2024): 211–23.

[30] Chong Kin Lim, David N Alfred, and Anastasia Chen, "Singapore: A Comprehensive Overview of the Data Protection Landscape.," in *The Guide to Cyber and Data Privacy Investigations*, 4th ed. (Global Investigations Review, 2025), https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/singapore-comprehensive-overview-of-the-data-protection-landscape.

[31] Tuti Elawati et al., "Comparison of Investor Protection Laws Between Indonesia and ASEAN Countries in the Face of Illegal Investments," *Journal Science and Theory of Law* 2, no. 02 (2025).

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

enforce compliance with customer due diligence (*customer due diligence*) to continue to operate effectively to maintain the integrity of global financial markets [32]. This combination of regulations forces issuers and securities companies to implement layered technology risk management and prohibit the use of customer data outside the legitimate interests of capital market transactions. The compliance of issuers in maintaining data confidentiality is seen as a form of seriousness by industry players to build investor trust in the primary market [33].

While it appears to be more integrated, Singapore's legal framework is not without its flaws. Broad consent exemptions under MAS Notice SFA04-N02 have the potential to shift investors' control over their data entirely to underwriters and stockbrokers, without the need for notification (*notification*) that is adequate to investors that their data is processed without consent (Erniwati & Wahyuningrum, 2025). In addition, the data security obligation in the PDPA is only formulated in general terms as the obligation to implement reasonable safeguards (*reasonable security arrangements*), without detailed technical parameters of Articles 35 to 39 of the PDP Law, so its implementation is highly dependent on the PDPC Advisory Guidelines which are guideline and do not have the same binding force as the law (Faiza et al., 2023). This is different from the European Union's approach through the General Data Protection Regulation (GDPR), which is a benchmark for updating the personal data protection framework in Indonesia and Thailand because it regulates technical security parameters in a more detailed and binding manner than the guideline-based approach *(guidance)* which adheres to the Singapore PDPA [34]. Thus, Singapore's legal certainty in terms of consent exemptions is not necessarily followed by equivalent technical certainty in terms of cybersecurity standards, so Singapore's prominence needs to be understood proportionately and not position it as a flawless ideal model.

To deepen this normative comparative analysis, the table below presents a synthesis of the differences in regulatory frameworks between the two jurisdictions:

Main Legal Basis:	Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)	Personal Data Protection Act 2012 (PDPA) Singapura
Comparison Indicators	Indonesia (PDP & SEOJK LAW 25/2025)	Singapore (PDPA, SFA&MAS Notice SFA04-N02)
Sectoral Regulation of e-IPO	Financial Services Authority Circular Letter No. 25/SEOJK.04/2025	Securities and Futures Act (SFA) & MAS Technology

[32] Erniwati and Kartika Sasi Wahyuningrum, "Legal Protection of Insider Trading in Capital Market Laws in Indonesia and Singapore," *Tripantang Journal* 11, no. 1 (2025): 27–51.

[33] Hanz Bryan Joeliant and Ariawan Gunadi, "Issuer Compliance with Disclosure Principles in Insider Trading in the Indonesian Capital Market: A Comparative Study with Singapore and the United States from an Investor Protection Perspective," *Legal idea* 12, no. 2 (2025): 1–15, https://doi.org/10.21070/jihr.v13i2.1095.

[34] Ampuan Situmeang et al., "Sharenting and Child Privacy: The GDPR as a Benchmark for Indonesian and Thai Legal Frameworks," *Lex Scientia Law Review* 10, no. 1 (2026): 233–58, https://doi.org/10.15294/lslr.v10i1.29211.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

		Risk Management Guidelines.
Consent Principle	Explicit consent from the data owner is required for all public offering activities	Consent is explicitly excluded for the benefit of Customer Due Diligence (CDD)/AML.
Due Diligent Duty	The Underwriter is required to check the current account of the financier for at least the last 3 months of the Definite Allotment	Stockbrokers are obliged to verify the Risk profile and identity without the constraints of the consent procedure
The Principal Supervisory Authority	Dualism of functions between the OJK (sectoral) and the PDP Supervisory Board to be formed	Harmonious synergy between the Personal Data Protection Commission (PDPC) and the Monetary Authority of Singapore (MAS)
Key Limitations	The dualism of authority between the OJK and LPPDP that will be formed, as well as the absence of cyber security technical standards (encryption, auditing, data retention) in SEOJK 25/2025	Broad consent exceptions have the potential to reduce data subject controls, as well as reasonable security arrangements without detailed technical parameters

Based on the comparison in the table, it can be seen that Singapore has a legal framework that provides more operational legal certainty regarding when the consent exemption applies, but this certainty is not followed by the detailed technical parameters of data security that Indonesia has through Articles 35 to 39 of the PDP Law [35]. On the other hand, Indonesia has more explicit technical security norms in the PDP Law, but is still trapped in the horizontal overlap of norms between the obligations of the OJK and the PDP Law that have not been harmoniously coordinated at the institutional level, and have not integrated these technical standards into capital market sectoral regulations such as SEOJK Number 25 of 2025 [36]. Thus, the two jurisdictions both have complementary advantages and disadvantages, so that Indonesian legal reform should ideally not simply imitate the Singapore model, but integrate domestic normative forces in the PDP Law with Singapore's operational clarity. The institutional coordination gap that still occurs in Indonesia is what creates legal uncertainty that is vulnerable to triggering data disputes in the future.

[35] Kharlie et al., "Comparative Analysis of Personal Data Protection in Indonesia and Singapore for a Sustainable Digital Future."

[36] Syakirah and Sayyidah, "The Urgency on Strengthening the Implementation of Personal Data Protection for Financiers in the Financial Services Equity Crowdfunding Sector in Indonesia (A Comparative Study of Malaysia) The Urgency on Strengthening Implementation of Personal Data Protection for Fin."

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

This comparison nonetheless rests on an asymmetry the analysis above should not obscure. Singapore's PDPA has operated since 2012 and has been amended and enforced for over a decade, which has produced a body of PDPC advisory guidelines, published enforcement decisions, and appellate case law that gives its "operational certainty" empirical content rather than leaving it as a claim about statutory text alone. Indonesia's PDP Law took effect only in 2022, and the LPPDP that would generate a comparable enforcement record for the capital market sector has not yet been formed. A comparison of regulatory design is accordingly not yet a comparison of regulatory performance: describing Singapore's framework as more integrated says as much about institutional maturity as it does about the substance of the two regimes. The more precise lesson for Indonesian reform is not that it should adopt Singapore's rules wholesale, but that the LPPDP, once established, will need a comparable period of guideline-issuing and enforcement practice before its coordination with the OJK can be judged on operational performance rather than on the text of the PDP Law alone.

This difference in regulatory readiness ultimately also affects the level of transparency and information asymmetry experienced by retail investors on both stock exchanges. On the Singapore stock exchange, issuers are required to list information technology and cybersecurity system risks as part of non-financial material information in the IPO prospectus [37]. On the other hand, in Indonesia, data security and privacy governance risks are still often ignored or only listed normatively without in-depth analysis in the public offering prospectus, thus deceiving the rational judgment of investors before investing their capital (Purwanto, 2014). As a result, Indonesian retail investors are often disadvantaged because they are not equipped with adequate technology risk information.

As a solution, the reform of the Indonesian capital market law must be immediately directed to solid cross-sectoral harmonization in order to knock down institutional sectoral egos. The government needs to immediately formulate implementing regulations that align the fund due diligence obligations in SEOJK Number 25 of 2025 with data minimization standards and technical security standards of the PDP Law, as well as require periodic cybersecurity audits for all securities underwriters to protect the digital human rights of the capitalist community [38]. Strong institutional supervision and coordination synergy between the OJK as the stock exchange regulator and the LPPDP that will be formed must be realized immediately through the preparation of joint decisions [39]. Thus, Indonesia can build a digital capital market ecosystem that is not only efficient and regionally competitive, but also safe and trusted by the wider community.

[37] Jasmine et al., "Initial Public Offering: Legal Protection of Minority Shareholders and Their Influence on Company Performance."

[38] Danil Erlangga Mahameru et al., "Implementation of the Personal Data Protection Law on the Security of Identity Information in Indonesia," *Journal of Legal Essence* 5, no. 20 (2023): 115–31, https://journal.upnvj.ac.id/index.php/esensihukum/article/view/240.

[39] Fajar Sugianto and Shintaro Tokuyama, "Beyond Administrative Sanctions: Reforming Insider Trading Regulation to Strengthen Investor Protection in Indonesia," *Journal of Legal Media* 31, no. II (2025): 244–61, https://doi.org/10.18196/jmh.v32i2.26257.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

2. Sanctions Received by Companies from the Impact of Investor Data Leaks in Indonesia and Singapore

The leakage of investors' personal data in the stock exchange is a latent cyber threat that demands the readiness of repressive law enforcement instruments firmly and consistently. Theoretically, Philipus M. Hadjon conceptualizes repressive legal protection as an effort to resolve disputes and impose sanctions after the occurrence of rights violations, which rests on three main functions, namely the remediation function (*recovery*) for the victim, the deterrence function (*deterrence*) for violators, and the function of legal certainty for the wider community [40]. These three functions are used as analytical tools in this study to assess the effectiveness of the three repressive sanctions available in Indonesia, namely administrative sanctions, civil sanctions, and criminal sanctions, as a subsidiary and complementary system, rather than just three stand-alone options.

In Indonesia, in the event of a cyber security system failure that results in a leak of the retail financier database, administrative sanctions are positioned as the most important law enforcement guard [41]. Based on Article 57 paragraph (2) of the PDP Law, this administrative sanction can be imposed in stages in the form of written warnings, temporary suspension of data processing activities, deletion or destruction of data, to administrative fines which according to Article 57 paragraph (3) of the PDP Law are pegged at a maximum of two percent of the corporation's annual revenue or revenue to the violation variable. If measured through the deterrence function (*deterrence*) within the framework of Hadjon's theory, the limit of two percent which is flat (*flat rate*) is considered not optimal to cause a deterrent effect for large issuers, because the larger the scale of corporate revenue, the smaller the proportion of financial impact felt compared to the potential profit from negligence in maintaining data security. Many securities industry players still view the cost of cyber compliance (*cost of compliance*) is much higher than the nominal risk of the sanctions imposed, so that the deterrence function that is at the core of Hadjon's repressive ideas has not been maximally achieved at the administrative level. As a result, the threat of leakage of sensitive data in the electronic public offering system is still at a level that endangers the convenience of the retail financier community.

In addition to the general data protection regime, the Financial Services Authority also holds strong sectoral authority to impose administrative sanctions on capital market participants who violate customer data governance provisions [42].). This OJK authority stems from the mandate to protect consumers in the financial services sector based on Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law), which is technically described through OJK Regulation Number 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector. Based on

[40] Hadjon, *Legal Protection for the People in Indonesia: A Study of Its Principles, Its Handling by the Courts in the General Judiciary and the Establishment of State Administrative Courts*.

[41] Alfred Yetno, "The Bank's Responsibility in Maintaining the Security and Confidentiality of Banking Customer Data in Indonesia," *Morality: Journal of Legal Science* 10, no. 1 (2024): 67–76, https://jurnal.upgriplk.ac.id/index.php/morality/article/view/424.

[42] Raissa Avila Nasution et al., "Legal Protection of Personal Data of Banking Service Customers After the Enactment of the Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022," *Journal of Education, Humaniora and Social Sciences (JEHSS)* 7, no. 1 (2024): 71–78, https://doi.org/10.34007/jehss.v7i1.2292.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Articles 108 and 109 of POJK Number 22 of 2023, the OJK is authorized to issue certain orders or actions to Financial Services Business Actors that violate the provisions of customer data governance, including the prohibition of providing customer data to third parties without permission [43]. The OJK's limits of authority are typical of market behavior supervision (*market conduct supervision*) which is oriented towards the stability and trust of the financial services sector, and differs substantially from the substantive authority of the Personal Data Protection Supervisory Agency (LPPDP) which will be established based on Article 58 and Article 60 of the PDP Law, which focuses on compliance with data protection principles across sectors. Article 75 of the PDP Law places the PDP Law as an umbrella rule (*umbrella provision*) which still recognizes the applicability of sectoral regulations such as POJK during the transition period, but does not provide a time limit or a firm coordination mechanism regarding when the OJK's authority ceases and LPPDP's authority begins in the case of data leaks in the capital market sector. This unclear boundary has the potential to cause overlapping authority to impose administrative sanctions, thus contradicting the function of legal certainty which is one of the pillars of Hadjon's theory. However, in many data dispute cases, OJK is often hampered by technical obstacles in proving the negligence of internal systems that trigger cyber leaks. This results in significant delays in the imposition of sanctions, which is detrimental to the principle of fair treatment for affected customers. As a result of this slow repressive legal process, the legal position of retail financiers on the national stock exchange continues to be in a weak asymmetric position.

In addition to administrative sanctions from the government, the protection of repressive laws in Indonesia also opens a loophole for investors to file civil lawsuits for damages. Investors who suffer material losses due to personal data leaks have the right to file a civil lawsuit on the basis of Unlawful Acts (PMH) in the district court [44]. This lawsuit is based on Article 1365 of the Civil Code which demands accountability for every negligent act that causes losses to others. However, proving the existence of a causal relationship and the value of real financial losses due to the misuse of cyber data is very difficult for individual financiers to do independently [45]. If analyzed through the recovery function (*recovery*) in Hadjon's theory, the civil route should be the most direct instrument to recover victims' losses, but this cyber complexity actually positions retail investors on a convoluted burden of proof and costs a lot of money so that the recovery function is not achieved effectively. Most retail customers end up choosing to surrender and ignore their civil rights because there is no certainty of financial recovery from the courts. This inequality situation proves that civil repressive instruments in Indonesia have not been able to provide reliable access to justice and compensation for customers.

[43] Herol Hansen Samin, "Legal Protection of Personal Data Leakage by Data Controllers through a Progressive Legal Approach," *Jurnal Sains Student Research* 1, no. 2 (2023): 1–15, https://doi.org/10.61722/jssr.v1i3.386.

[44] Hayekal Hidayat, Dedi Harianto, and Jelly Leviza, "Legal Protection of Customer Data of PT. PLN in Granting Temporary Termination Letters Based on Law Number 27 of 2022 concerning Personal Data Protection," *Journal of Law, Humanities and Politics* 6, no. 1 (2025): 185–94.

[45] Manga Sandi Sijabat et al., "Legal Protection for Users Who Experience Personal Data Leakage on Online Loan Applications," *Locus: Journal of Legal Concepts* 6, no. March (2026), https://doi.org/10.56128/jkih.v4i3.402.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

The next dimension of repressive law enforcement in Indonesia is the imposition of criminal sanctions as a last resort (*ultimum remedium*) if it is proven that there is an element of intentionality in the cybercrime [46]. The criminal provisions in the PDP Law are regulated in detail in Articles 67 to 70. Article 67 paragraph (1) of the PDP Law requires the element of criminal liability in the form of acts committed "deliberately and unlawfully" to obtain or collect Personal Data that does not belong to him, with the intention of benefiting himself or others, which may result in losses to the data subject, with a maximum penalty of imprisonment of 5 (five) years and/or a maximum fine of Rp5, 000,000,000.00 (five billion rupiah); Similar provisions also apply to the act of disclosing (paragraph (2), a threat of 4 years/IDR 4 billion) and using personal data that does not belong to him (paragraph (3), a threat of 5 years/IDR 5 billion), while Article 68 of the PDP Law regulates a more severe threat, namely a maximum of 6 years imprisonment and/or a maximum fine of IDR 6,000,000,000.00 (six billion rupiah), for the act of falsifying Personal Data. The element of "intentionally" (*Mens Rea*) This is the most crucial but at the same time the most difficult to prove in the context of data leaks in the capital market. Most incidents of investor data leakage stem from the negligence of the security system of issuers or underwriters, not from intentional acts committed by the data controller itself, so that doctrinally Article 67 and Article 68 of the PDP Law are more appropriate to ensnare external parties who actively hack or misuse data (*threat actor*), not ensnaring issuers or securities companies that neglect to secure their systems. Consequently, corporate criminal liability based on Article 70 of the PDP Law, which allows the imposition of a fine of up to ten times on corporations, can only be applied if the criminal acts in Article 67 or Article 68 are actually committed by the corporate management, control holder, or order-giver, and not solely because the corporation is a victim of hacking due to the negligence of its system. The current formulation of the criminal liability in the PDP Law does not explicitly accommodate corporate negligence as the basis for criminal liability, so it is necessary to reconstruct the norm so that the broader principle of liability can be applied to negligent issuers [47]. This lack of norms is what causes most cases of data leaks due to the negligence of the issuer's security system to be charged through the criminal channels of the PDP Law, so that this path in practice is only effective in reaching external actors, not negligent data controllers. However, the enforcement of cyber criminal sanctions in practice often encounters an impasse due to the limited capacity of cyber investigators and the complexity of tracing perpetrators of cross-border hacking [48]. Most data crime cases in the capital market eventually evaporate without any clarity on the legal subjects who must be responsible. This weak forensic evidence lowers the authority of cyber criminal law in

[46] Yetno, "The Bank's Responsibility in Maintaining the Security and Confidentiality of Banking Customer Data in Indonesia."

[47] Ampuan Situmeang, Nadia Carolina Weley, and Hari Sutra Disemadi, "Certainty of Corporate Criminal Law Accountability for the Abuse of Personal Data in Indonesia," *Proceedings Series on Social Sciences & Humanities* 23, no. 2022 (2025): 8–15, https://doi.org/10.30595/pssh.v23i.1544.

[48] Rohmah Dwi Cahyaningsih et al., "Criminal Law Policy for Combating Phishing Crimes Through the Personal Data Protection Act: Compa," *Abdurrauf Science and Society* 1, no. 4 (2025): 800–811, https://doi.org/10.70742/asoc.v1i4.283.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

the eyes of financial technology industry players. This gap is what triggers the flourishing of illegal data trading activities in the cyber black market without fear of criminal threats.

In contrast to Indonesia, Singapore implements a very aggressive repressive approach through the imposition of administrative financial sanctions calculated from the scale of the corporation's business. Under Section 48J of Singapore's Personal Data Protection Act as amended through the Personal Data Protection (Amendment) Act 2020 and effective from 1 October 2022, the Personal Data Protection Commission (PDPC) has the authority to impose financial fines of up to S$1,000,000 (one million Singapore dollars), or ten per cent of the company's total annual turnover in Singapore for entities with a turnover exceeding S$10,000,000, whichever is higher [49]. This turnover-based fine formula is designed to provide a more proportionate financial impact for giant stock exchange issuers that neglect customer data protection compared to the flat fine scheme as it applies in Indonesia. With this double threshold scheme, the fines imposed will remain relevant for both large and small corporations, thus being able to give birth to stricter self-supervision among the board of directors. The Singapore PDPC periodically publishes the financial penalty decision to the public in order to impose social sanctions in the form of the collapse of the corporate business reputation that violates [50]. This publication forces all capital market players in Singapore to regularly update their cybersecurity systems.

Another advantage of Singapore's repressive enforcement system is the realization of integrated synchronization of administrative sanctions between privacy regulators and monetary authorities. Every securities company on the Singapore exchange is required to comply with Technology Risk Management standards, where violations of customer data privacy can have implications for the freezing of business licenses by MAS [51]. MAS has full authority to revoke the Capital Markets Services Licence of stockbrokers who are found to have neglected to maintain the confidentiality of customers' SIDs. This horizontal synchronization closes the gap for exchange corporations to take refuge behind the unclear boundaries of authority between institutions, thus directly answering the problem of overlapping authority that Indonesia still faces between the OJK and LPPDP. This integrated repressive supervision model successfully protects the constitutional right to privacy of customers while maintaining the integrity of the stability of the Singapore stock exchange on a macro basis [52]. Exchange issuers do not dare to speculate on cybersecurity due to the threat of double operational sanctions that can shut down the continuity of their business instantly.

For investors on the Singapore exchange, the recovery of civil losses is also accommodated through a right of personal action (*right of private action*) which is regulated in Section 32 of the Singapore PDPA, which since the 2020 amendment has been

[49] Sanil Khantri, Daryl Seetoh, and Natalie Joy Huang, "Singapore PDPC Fines Several Organizations," Baker McKenzie, 2026, https://www.bakermckenzie.com/en/insight/publications/2026/01/singapore-pdpc-fines-several-organizations.

[50] (Lukewarm & Pu, 2023)

[51] Efrain Janke Zet Mangindaan, Diva A. E. Rombot, and Alsam Polontalo, "Legal Protection for Investors in Securities Buying and Selling Transactions in the Capital Market," *Lex Administratum* 10, no. 4 (2022).

[52] Hamdan et al., "Legal Policy with an Impact on Personal Data: Indonesia and Singapore in the ASEAN Framework."

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

renumbered to Section 48O [53]. This provision gives any person who has suffered "loss or damage" due to a violation of data protection provisions by an organization the right to file a civil lawsuit directly, without having to go through an administrative complaint process to the PDPC first. However, this right of personal action does not necessarily relieve investors of the burden of proof: investors must still prove that there has been a violation of the provisions of the PDPA by the organization, as well as the existence of "loss or damage" that falls under the category of losses recognized by law *common law*, such as financial loss, property damage, or personal injury. Singapore Court of Appeal decision in the case *Reed v Bellingham* [2022] SGCA 60 affirms that simply a loss of control over personal data (*loss of control*) without actual loss is not sufficient to base a claim under Section 48O, although the Court of Appeal ultimately extended the scope of "loss or damage" to include emotional distress (*emotional distress*). This ruling shows that Singapore's civil recourse, although procedurally more concise than Article 1365 of the Indonesian Civil Code, still requires material proof that is not simple for retail investors who only experience concerns over their data leaks without any real financial loss. This civil redress mechanism is resolved independently to recover legally recognized losses, including reputational losses and emotional distress of customers [54]. This efficient civil law route forces issuers to offer voluntary compensation schemes as soon as possible before their case leads to an open lawsuit in court.

Although Singapore's repressive system appears to be more aggressive and integrated, this model is not without its flaws. The authority to impose turnover-based fines in Section 48J of the PDPA is entirely discretionary in the hands of the PDPC, with no binding parameters as to when the ten per cent threshold is actually applied, so in practice that in practice the PDPC often imposes fines well below the statutory maximum, creating a gap between the legal threat on paper and the actual deterrent effect. Similarly, the right of personal action under Section 48O of the PDPA, as demonstrated by *Reed v Bellingham* above, was initially rejected by the High Court of Singapore because the investor failed to prove the existence of a legally recognised "loss or damage", so that Singapore's civil remedies cannot be claimed to be immediately superior and unimpeded to Indonesian civil law. Another critically pleasing weakness is that MAS's freezing mechanism for the Capital Markets Services Licence is very drastic and has the potential to pose a systemic risk to market stability when applied to large-scale underwriters, so in practice MAS must be cautious and tend to take a coaching path before revoking the licence, which in turn may slow down the expected deterrence effect. Thus, Singapore's normative superiority in formulating a high threat of sanctions on paper needs to be understood proportionately, as the effectiveness of its implementation on the ground remains limited by institutional discretion and evidentiary requirements that are not entirely light on victims.

An in-depth comparison of the form of sanctions in the two countries proves that there is a fairly wide gap in regulatory readiness and institutional firmness between

[53] Lim, Alfred, and Chen, "Singapore: A Comprehensive Overview of the Data Protection Landscape."
[54] Joeliant and Gunadi, "Issuer Compliance with Disclosure Principles in Insider Trading in the Indonesian Capital Market: A Comparative Study with Singapore and the United States from an Investor Protection Perspective."

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Indonesia and Singapore, although both systems have limitations in practice. Judging from the Legal Protection Theory of Philipus M. Hadjon, the system of enforcement of repressive sanctions in Singapore is considered superior in fulfilling the function of deterrence thanks to the turnover-based fine scheme and the publication of rulings that give rise to reputational sanctions [55]. On the other hand, repressive instruments in Indonesia are considered less effective in fulfilling all three of Hadjon's repressive functions simultaneously, due to its flat and relatively low administrative fine regime, civil channels that burden investors with conventional PMH proof, and criminal channels that are doctrinally difficult to reach negligent data controllers. The absence of harmonization of horizontal sanctions regulations between the OJK and the new PDP commission can trigger confusion for securities companies in formulating operational compliance [56].

This assessment carries a similar methodological caveat. Singapore's repressive apparatus can be evaluated against more than a decade of PDPC enforcement decisions and at least one reported appellate judgment construing the right of private action, which is what allows this study to identify where its deterrent and compensatory functions fall short in practice. Indonesia's equivalent institutions have no comparable enforcement record to examine: the LPPDP has not been formed, and no reported case has yet tested Article 1365 of the Civil Code or Articles 67 to 70 of the PDP Law in a capital market data breach. The claim that Singapore's repressive system performs better should accordingly be read as a claim about Singapore's demonstrated record measured against Indonesia's as-yet-untested design, not as a claim that Indonesia's instruments are inherently weaker once comparable enforcement experience accumulates.

As an operational step, there are four concrete recommendations that Indonesia can immediately take to strengthen the effectiveness of the three repressive sanction routes. *First*, the Government needs to immediately issue a Government Regulation implementing Article 57 paragraph (5) of the PDP Law which changes the administrative fine scheme from *a flat rate* of two percent to a multi-tiered turnover-based scheme with a double threshold like the Section 48J PDPA model, as well as setting a minimum fine so that it is not too low for small-scale corporations. *Second*, the OJK and LPPDP that will be formed need to sign a *memorandum of understanding (Memorandum of Understanding*) that explicitly regulates the case referral *mechanism* and the deadline for coordination of joint investigations, for example, no later than 30 (thirty) working days from the date the data leak report is received, to prevent overlap or delay in the imposition of administrative sanctions in the capital market sector. *Third*, it is necessary to establish a small *claims mechanism* specifically for investor personal data disputes through the Financial Services Sector Alternative Dispute Resolution Institution (LAPS SJK), with a *shifting scheme of the burden of proof* to issuers or underwriters once the OJK or LPPDP has determined an administrative violation, so that retail investors do not need to prove the technical causality

[55] Hadjon, *Legal Protection for the People in Indonesia: A Study of Its Principles, Its Handling by the Courts in the General Judiciary and the Establishment of State Administrative Courts*.

[56] Syakirah and Sayyidah, "The Urgency on Strengthening the Implementation of Personal Data Protection for Financiers in the Financial Services Equity Crowdfunding Sector in Indonesia (A Comparative Study of Malaysia) The Urgency on Strengthening Implementation of Personal Data Protection for Fin."

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

relationship as required by Article 1365 of the Civil Code. *Fourth*, it is necessary to prepare joint technical guidelines between the OJK and LPPDP regarding minimum cybersecurity parameters (encryption, periodic audits, data retention, and access restrictions as described in the previous section) which are objective references for investigators in assessing the elements of system negligence, thereby making it easier to prove both the administrative and criminal channels of Article 67 and Article 68 of the PDP Law. This operational and measurable repressive legal reform is very urgent to restore the trust of retail financiers and create stability in the national digital capital market that is resilient and trusted in the regional arena.

D. Conclusions and Recommendations

The regulation of the protection of investors' personal data at the stage of registration, verification, and allocation of shares in *the Initial Public Offering* (IPO) process in Indonesia and Singapore shows the dichotomy between a fragmented system and a more integrated system, although both have unresolved normative gaps. In Indonesia, the horizontal disharmony between the principle of data minimization in Article 20 paragraph (2) in conjunction with Article 35 of the PDP Law and the principle of full disclosure in Article 1 number 25 in conjunction with Article 78 and Article 80 of the Capital Market Law still continues, especially after the enactment of SEOJK Number 25 of 2025 which requires underwriters to conduct due diligence on the current accounts of the last three months for Fixed *Allotment financiers* without being accompanied by clear cybersecurity technical standards in the form of encryption, periodic audits, data retention, and access restrictions as outlined in Articles 35 to 39 of the PDP Law. The basic confusion of data processing also exacerbates the situation, as e-IPO industry players often mistakenly equate all data processing with the obligation to obtain *consent*, even though Article 20 paragraph (2) of the PDP Law recognizes the legal obligation of data controllers as a separate processing basis that does not require separate consent. In contrast, Singapore has established a legal framework that provides more operational certainty through explicit consent exemptions for the benefit of *Customer Due Diligence* (CDD) based on MAS Notice SFA04-N02, as well as mature institutional synchronization between capital market authorities (MAS) and privacy supervisors (PDPC). However, this certainty is not followed by the detailed technical parameters of data security in the PDP Law, because the security obligations in the PDPA are only formulated in general as *reasonable security arrangements* without technical references that are binding on the equivalent of the law. The gap in cross-jurisdictional coordination in Indonesia has also created tactical legal uncertainty for industry players, especially with the potential dualism of supervisory authority between the OJK and the Personal Data Protection Supervisory Agency (LPPDP) to be established.

Regarding the form of sanctions received by companies due to the impact of investor data leaks, the application of Philipus M. Hadjon's Repressive Legal Protection Theory through its three main functions, namely recovery, deterrence, and legal certainty, shows that the three sanctions channels in Indonesia (administrative, civil, and criminal) have not worked optimally as a complementary system. The administrative sanction of two percent

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

of annual revenue based on Article 57 of the PDP Law is still flat and has not caused an adequate deterrent effect, while the limit of its authority with the OJK based on POJK Number 22 of 2023 has not been expressly coordinated with the authority of LPPDP based on Article 58 and Article 60 of the PDP Law. The civil route through Article 1365 of the Civil Code burdens investors with a heavy proof of causality, while the criminal route of Article 67 and Article 68 of the PDP Law, which requires the element of "willful and unlawful", is doctrinally more appropriate to ensnare the perpetrators of external hacking than issuers who neglect to secure their systems, so that many incidents of data leakage due to system negligence cannot be prosecuted through these criminal channels. Singapore applies a more normatively restrictive repressive approach through turnover-based administrative fines of up to ten percent or S$1,000,000 (whichever is higher) under Section 48J of the PDPA, as well as *the right of private action* under Section 48O (formerly Section 32) of the PDPA, which allows investors to claim compensation without a prior administrative complaint process. However, these normative advantages are not necessarily free from practical weaknesses, because the authority to impose PDPC fines is discretionary and the right of personal action still requires proof of *loss or damage* recognized by law, as shown by the decision *of Reed v Bellingham* [2022] SGCA 60 which initially rejected the investor's lawsuit because the element of loss was not met. Therefore, Indonesia needs more operational repressive legal reforms, including the revision of the Government Regulation implementing Article 57 paragraph (5) of the PDP Law into a turnover-based tiered fine scheme, the preparation of a memorandum of understanding between OJK and LPPDP with a clear coordination deadline, the establishment of a simple lawsuit mechanism through the Financial Services Sector Alternative Dispute Resolution Institution (LAPS SJK) accompanied by the transfer of the burden of proof, and the preparation of joint cybersecurity technical guidelines, so that the sanctions imposed are not only administrative financial fines, but also provide real restoration of rights for affected investors.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

References

Abdul Malik. "Definition, Stages, and How to Buy It." Bareksa, 2025. https://www.bareksa.com/berita/saham/2025-12-02/e-ipo-pengertian-tahapan-dan-cara-belinya.

Agustianto, Agustianto, Michael T. Sacramed, Winda Fitri, Nadia Carolina Weley, and Hari Sutra Disemadi. "Regulatory Gaps in Data Protection and Proportionality in Digital Banking: Legal Issues in ASEAN." *Syura: Journal of Law* 4, no. 1 (2026): 55–86. https://doi.org/https://doi.org/10.58223/syura.v4i1.811.

Alfaaiz, and Mohamad Gery. "Comparison of Personal Data Protection Regulations Between Indonesia and Singapore in the Context of the Worldcoin Case." *Journal Equitable* 10, no. 3 (2025): 95–110. https://ejurnal.umri.ac.id/index.php/JEQ/article/download/4554/2166.

Cahyaningsih, Rohmah Dwi, Anis Fauzan, Saupi Hasbi, and Atik Winanti. "Criminal Law Policy for Combating Phishing Crimes Through the Personal Data Protection Act: Compa." *Abdurrauf Science and Society* 1, no. 4 (2025): 800–811. https://doi.org/10.70742/asoc.v1i4.283.

CNN Indonesia. "2.9 Million User Data Cermati.Com Hacked," 2020. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/9e47e8a7538de5d/survei-ini-produk-keuangan-yang-dianggap-rentan-kebocoran-data%0A https://www.cnnindonesia.com/teknologi/20201102103348-185-564812/29-juta-data-pengguna-cermaticom-diretas.

Darmawan, Kevin, and Aninditha Sekar Putri. "Legal Protection for Investors' Personal Data Against Cybercrime Threats in Capital Market Based on IOSCO Principles." *Journal of Law, Politic and Humanities* 5, no. 4 (2025): 2293–2303. https://doi.org/10.38035/jlph.v5i4.1458.

Disemadi, Sutra Day. "The Lens of Legal Research: A Descriptive Essay on Legal Research Methodology." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. http://dx.doi.org/10.37253/jjr.v.

Elawati, Tuti, La Ode Mbunai, Muhammad Panca Prana Mustaqim Sinaga, and Yusup Suparman. "Comparison of Investor Protection Laws Between Indonesia and ASEAN Countries in the Face of Illegal Investments." *Journal of Science and Theory of Law* 2, no. 02 (2025).

Erniwati, and Kartika Sasi Wahyuningrum. "Legal Protection of Insider Trading in Capital Market Laws in Indonesia and Singapore." *Journal of Tripantang* 11, no. 1 (2025): 27–51.

Faiza, Azza Fitrahul, Sinta Dewi Rosadi, Garry Gumelar Pratama, Dharmawan, and Ananda Fersa. "Strengthening Personal Data Protection through Supervisory Authorities in Indonesia Based on a Comparison of the Laws of Hong Kong and Singapore." *Hakim: Journal of Legal and Social Sciences* 1 (2023).

Fajariah, Kurniastuti Sri, and Niru Anita Sinaga. "Legal Protection for Consumers in Buying and Selling Transactions through the Bukalapak E-Commerce Platform." *Lex Progressium* 1, no. 2 (2024): 153–69.

Fikri, Muhammad, and Shelvi Rusdiana. "The Scope of Personal Data Protection: A Study of Indonesian Positive Law." *Ganesha Law Review* 5, no. 1 (2023): 125–39. https://doi.org/https://doi.org/10.23887/glr.v5i1.2237.

Fintech News Singapore. "Tokenize Xchange Shutdown Leaves Investors in Limbo," 2025. https://fintechnews.sg/116488/crypto/tokenize-xchange-shutdown-singapore-investors/.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Hadjon, Philipus M. *Legal Protection for the People in Indonesia: A Study of the Principles, Their Handling by the Courts in the General Judicial Environment and the Establishment of the State Administrative Court*. Surabaya: Bina Ilmu, 1987.

Hamdan, Fairuz, Rosa Ristawati, Mardianta Anggara, and Nabilah Hamdan. "Legal Policy with an Impact on Personal Data: Indonesia and Singapore in the ASEAN Framework." *Proceedings of Airlangga Faculty of Law Colloquium* 1 (2024): 211–23.

Hasbuddin Khalid. "Law and Investment: Aspects of Legal Protection by Financial Services Authorities for Capital Market Investors." *Unes Law Review* 6, no. 1 (2023): 737–45. https://review-unes.com/https://creativecommons.org/licenses/by/4.0/.

Hidayat, Hayekal, Dedi Harianto, and Jelly Leviza. "Legal Protection of Customer Data of PT. PLN in Granting Temporary Termination Letter Based on Law Number 27 of 2022 concerning Personal Data Protection." *Journal of Law, Humanities and Politics* 6, no. 1 (2025): 185–94.

Jasmine, Alifia, Azmi Yasmine, Nurul Sharfina, and Aisyah Fathhurrohmah. "Initial Public Offering: Legal Protection of Minority Shareholders and Influence on Company Performance." *Journal of Law & Development* 54, no. 1 (2024). https://doi.org/10.21143/jhp.vol54.no1.1606.

Joeliant, Hanz Bryan, and Ariawan Gunadi. "Issuer Compliance with Disclosure Principles in Insider Trading in the Indonesian Capital Market: A Comparative Study with Singapore and the United States from an Investor Protection Perspective." *Rechtsidee* 12, no. 2 (2025): 1–15. https://doi.org/10.21070/jihr.v13i2.1095.

Databoks Katadata. "Survey: These Financial Products Are Considered Vulnerable to Data Leaks," 2021. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/9e47e8a7538de5d/survei-ini-produk-keuangan-yang-dianggap-rentan-kebocoran-data%0A https://www.cnnindonesia.com/teknologi/20201102103348-185-564812/29-juta-data-pengguna-cermaticom-diretas.

Khantri, Sanil, Daryl Seetoh, and Natalie Joy Huang. "Singapore PDPC Fines Several Organizations." Baker McKenzie, 2026. https://www.bakermckenzie.com/en/insight/publications/2026/01/singapore-pdpc-fines-several-organizations.

Kharlie, Ahmad Tholabi, Fathudin Fathudin, Firman El Amny Azra, and Solahudeen Cheduerame. "Comparative Analysis of Personal Data Protection in Indonesia and Singapore for a Sustainable Digital Future." *Towards Resilient Societies: The Synergy of Religion, Education, Health, Science, and Technology*, no. Fuster 2014 (2025): 593–98. https://doi.org/10.1201/9781003645542-95.

Lauw, Nick, and Fang Ching Pu. "Fines for PDPA Breaches: How Clear Is the Crystal Ball?" RPC, 2023. https://www.rpclegal.com/thinking/data-and-privacy/fines-for-pdpa-breaches-how-clear-is-the-crystal-ball/.

Lim, Chong Kin, David N Alfred, and Anastasia Chen. "Singapore: A Comprehensive Overview of the Data Protection Landscape." In *The Guide to Cyber and Data Privacy Investigations*, 4th ed. Global Investigations Review, 2025. https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/singapore-comprehensive-overview-of-the-data-protection-landscape.

Mahameru, Danil Erlangga, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal, and Mohamad Haikal Rahmadia. "Implementation of the Personal Data Protection Law on Identity Information Security in Indonesia." *Journal of Legal Essence* 5, no. 20 (2023): 115–31. https://journal.upnvj.ac.id/index.php/esensihukum/article/view/240.

Mangindaan, Efrain Janke Zet, Diva A. E. Rombot, and Alsam Polontalo. "Legal Protection for Investors in Securities Buying and Selling Transactions in the Capital Market." *Lex*

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Administratum 10, no. 4 (2022).

Nasution, Raissa Avila, Budiman Ginting, Mahmul Siregar, and Tengku Keizerina Devi Azwar. "Legal Protection of Personal Data of Banking Service Customers After the Enactment of the Financial Services Authority Regulation (POJK) Number 6/Pojk.O7/2022." *Journal of Education, Humanities and Social Sciences (JEHSS)* 7, no. 1 (2024): 71–78. https://doi.org/10.34007/jehss.v7i1.2292.

Nidia, Nyoman, Sari Hayati, and Sri Warjiyati. "Juridical Analysis of the Omnibus Law Concept in the Harmonization of Laws and Regulations in Indonesia." *Journal of Justice Ocean* Law 16, no. 1 (2021): 1–18.

Pohan, Ghiffary Akmal Alija, FX. Joko Priyono, and Ery Agus Priyono. "Application of Principle Full Disclosure and Legal Protection for Investor Due To Market Manipulation of Shareprices By Issuers in Capital Market." *Crepido* 5, no. 1 (2023): 104–15. https://doi.org/10.14710/crepido.5.1.104-115.

Pratiwi, Indira. "Legal Protection for Investors in the Implementation of Stock Transactions with Online Trading Systems." *Dharmasisya: Journal of the Master of Law Program, Faculty of the University of Indonesia* 2, no. January (2023): 1335–37.

Raila, Tiara Almira, Sinta Dewi Rosadi, and Rika Ratna Permata. "Privacy Data Protection in Indonesia and Singapore Related to the Implementation of Digital Contact Tracing as an Effort to Prevent Covid-19 and Its Responsibilities." *Journal of Legal Certainty and Justice* 2, no. 1 (2021): 1. https://doi.org/10.32502/khdk.v2i1.3044.

Samin, Herol Hansen. "Legal Protection of Personal Data Leakage by Data Controllers through a Progressive Legal Approach." *Journal of Science Student Research* 1, no. 2 (2023): 1–15. https://doi.org/10.61722/jssr.v1i3.386.

Sijabat, Manga Sandi, Tahasak Sahay, Elin Sudiarti, and Karlinae D.Bangas. "Legal Protection for Users Who Experience Personal Data Leakage on Online Loan Applications." *Locus: Journal of Legal Concepts* 6, no. March (2026). https://doi.org/10.56128/jkih.v4i3.402.

Situmeang, Ampuan, Abdurrakhman Alhakim, Ruetaitip Chansrakaeo, Winda Fitri, and Winsherly Tan. "Sharenting and Child Privacy: The GDPR as a Benchmark for Indonesian and Thai Legal Frameworks." *Lex Scientia Law Review* 10, no. 1 (2026): 233–58. https://doi.org/10.15294/lslr.v10i1.29211.

Situmeang, Ampuan, Lu Sudirman, Ida Bagus Rahmadi Supancana, Nurlaily, and Hari Sutra Disemadi. "International Journal of Educational Review, Law, and Social Sciences (IJERLAS)." *International Journal of Educational Review, Law, and Social Sciences (IJERLAS)* 6, no. 1 (2026): 184–94. https://doi.org/10.3390/fi17020083.13.

Situmeang, Ampuan, Nadia Carolina Weley, and Hari Sutra Disemadi. "The Certainty of Corporate Criminal Law Accountability for the Abuse of Personal Data in Indonesia." *Proceedings Series on Social Sciences & Humanities* 23, no. 2022 (2025): 8–15. https://doi.org/10.30595/pssh.v23i.1544.

Sugianto, Fajar, and Shintaro Tokuyama. "Beyond Administrative Sanctions: Reforming Insider Trading Regulation to Strengthen Investor Protection in Indonesia." *Jurnal Media Hukum* 31, no. II (2025): 244–61. https://doi.org/10.18196/jmh.v32i2.26257.

Syahyu, Yulianto. "Legal Protection of Investor in the Indonesian Capital Market." *International Journal of Research and Review* 12, no. 11 (2025): 85–94. https://doi.org/10.52403/ijrr.20251110.

Syakirah, Salwa Naya, and Haipa Nisrina Sayyidah. "The Urgency on Strengthening Implementation of Personal Data Protection for Fins" 12 (2024): 109–22.

Syazali, Emir Adhan. "Legal Protection for Investors in Initial Public Offerings (IPOs): Between Das Sein and Das Sollen." *Al-Qanun: Journal of Islamic Law Thought and Reform* 28, no. 2 (2025). https://doi.org/https://doi.org/10.15642/alqanun.2025.28.2.269-283.

Volume 12, Number 03, July-September 2026, Pages 366-388
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i2
Sinta 3; decree No.0173/C3/DT.0500/2025

Yetno, Alfred. "The Responsibility of Banks in Maintaining the Security and Confidentiality of Banking Customer Data in Indonesia." *Morality: Journal of Law* 10, no. 1 (2024): 67–76. https://jurnal.upgriplk.ac.id/index.php/morality/article/view/424.