JURNAL BECOSS
(Business Economic, Communication, and Social Sciences), Vol.8 No.2 May 2026: 143-153
e-ISSN: 2686-2557
DOI: 10.21512/becossjournal.v8i2.16136

Ransomware Attacks on Investors' Personal Data and the Legal Liability of Securities Companies in Indonesia

Fauzan Wahyu Utomo[1*], Anis Rifai[2], Anas Lutfi[3]

[1-3]Faculty of Law, Master of Laws,
Al Azhar University of Indonesia,
Jakarta 12110, Indonesia
fauzanwahyuutomo@gmail.com; anizrifai@gmail.com;
anaslutfi.jakarta@gmail.com

*Correspondence: fauzanwahyuutomo@gmail.com

ABSTRACT

This article addresses the legal responsibility of securities companies in the event of ransomware attacks that lead to the misuse of investors' personal data in Indonesia. This research uses normative legal research with statute, conceptual, and case approaches to show that the legal framework related to the use of personal data by financial technology companies is the Capital Market Law, the Personal Data Protection Law, the Electronic Information and Transactions Law as amended by Law No. 1 of 2024, the Financial Sector Development and Strengthening Law, and OJK consumer protection regulations. The research gap identified in this study is the lack of a focused analysis of the accountability of securities companies through the doctrines of duty of care, corporate negligence and cyber liability within the context of the capital market. This article concludes that liability can arise contractually, tortiously and administratively when a securities company fails to have reasonable security measures, supervision and incident response. Better harmonization of sectoral rules, clear breach notification standards and risk-based security obligations are thus needed to better protect investors.

Keywords: *legal liability; cybercrime; ransomware; personal data; securities company*

INTRODUCTION

The Indonesian capital market has been digitalized, from a transaction system that is entirely based on face-to-face transactions to a fast-paced service based on apps and electronic platforms. The transformation has definitely democratized access for investors, cut transaction costs, sped up information flows but also created new avenues for cyber criminals to attack. In this regard, the personal data of investors has become a very valuable asset. It includes identity details, account numbers, access credentials and transaction patterns that could be used to take over accounts or make unauthorized transactions. The situation is illustrative of the fact that security of electronic systems is no longer only a technical problem, but a legal obligation closely linked to the protection of the rights of investors.

In terms of regulation, the protection of investors and their personal data is regulated under several interconnected legal frameworks, such as Law No. 8 of 1995 on the Capital Market, Law No. 27 of 2022 on the Protection of Personal Data, Law No. 1 of 2024 on the Second Amendment to the Law on Electronic Information and Transactions, Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, and Financial Services Authority Regulation No. 22/POJK.07/2023 on the Protection of Consumers and the Public in the Financial Services Sector. The problem is that these regulations are still sectoral and have not yet created a truly integrated accountability framework when securities firms are hit by ransomware.

This weakness is clear from two points of view. To start with, data controllers are already required to protect and ensure the security of the data being processed and to provide notification in the event of a personal data breach under personal data protection regulations, but their implementation still requires more robust operational mechanisms, particularly in the financial services sector. Second, the capital markets regime focuses more on general business conduct and investor protection but has not yet explicitly laid out standards for corporate liability for increasingly complex cyber risks. In this case, securities firms are confronted with complicated legal risks. Whether the losses of investors are only caused by external attacks or also related to the negligence of internal security management?

The ransomware attack on the National Data Centre in 2024 has underscored the increasing importance of data protection in the financial sector. It demonstrated how a disruption to one piece of digital infrastructure can significantly affect the provision of public services and wider economic activity. This phenomenon demonstrates that the vulnerabilities of digital systems may have systemic consequences beyond the technology industry itself (Yusliwidaka et al., 2024). In the digital capital market ecosystem, investors' personal data can no longer be perceived as simple administrative identifiers but have turned into an asset with economic value, which may be misused in the shape of illegal access, account takeovers and manipulation of transactions. Thus, the absence of system security at a securities company is not only a technical problem but also has touched on legal issues related to the right of self-defense, honor, dignity and sense of security as guaranteed by Article 28G (1) of the 1945 Constitution of the Republic of Indonesia (Manurung, 2023).

Normatively, Law No. 27 of 2022 concerning the Protection of Personal Data (TPDP) emphasizes that the protection of personal data is a series of measures to protect personal data in the processing process to ensure the constitutional rights of data subjects. In this sense, the protection of personal data is considered not only as an administrative obligation, but also as a legal instrument for the protection of the rights of data subjects at all stages of processing. This is consistent with the opinion of Manurung (2023) who states that the protection of personal data is an integral part of protecting the rights of data subjects.

Securities firms can have formal policies, but that's not sufficient. They must be able to demonstrate that they have adequate technical and organizational security measures in place, such as data encryption, access restrictions, and regular security audits. Furthermore, Article 46 of the Personal Data Protection Act requires the Personal Data Controller to notify the Data Subject in the event of a Personal Data Protection breach; this obligation is reinforced by technical provisions requiring notification to be made no later than 3 x 24 hours from the time the data protection breach is discovered (Yusliwidaka et al., 2024).

Various studies indicate that the main challenges lie in the readiness of cyber security governance, supervisory capacity, and the effectiveness of compliance implementation at the corporate level. This situation indicates that the main problem lies not merely in the presence or absence of regulations, but in the weakness of implementation, supervisory coordination and compliance design at the corporate level. Therefore, this research is important for formulating a more proactive legal protection model for investors through the integration of the principles of 'Data Protection by Design and by Default' into the governance of securities firms (Mayasari, 2023).

Philipus M. Hadjon's theory of legal protection categorizes legal protection into two forms: preventive and repressive. Preventive protection serves to prevent infringements through regulation, supervision and compliance standards, whilst repressive protection comes into play after an infringement has occurred through dispute resolution mechanisms and law enforcement (Rachmat et al., 2024). In this study, this theory is relevant because investor protection must fundamentally be established from the preventative stage, not merely after losses have occurred. Hadjon offers a framework to decide whether current regulations are enough to prevent attacks or whether they are still reactive.

Hans Kelsen's theory of legal liability. Liability is a consequence of violation of a norm. For securities firms, liability is not just about whether or not a ransomware attack has occurred, but rather about whether the firm has properly performed its normative obligations (Syaputra et al., 2024). This link coincides with the theory of tort which emphasizes the elements of an act, fault, damage and a

causal link. Civil liability may be incurred by negligence in the implementation of appropriate security measures; in the conduct of security audits or in the management of system access.

Moreover, the study incorporates the notions of duty of care, corporate negligence, cyber liability and fiduciary responsibility to strengthen the analysis. The duty of care concept entails that securities firms are required to adhere to high standards of care in safeguarding investor data, as part of their governance and consumer protection obligations within the financial services industry (Rosadi et al., 2022). Corporate negligence may refer to the lack of adequate security measures, the failure to conduct regular security audits, or the failure to establish cyber-attack mitigation systems by a corporation, which may result in legal liability (Yuspin et al., 2023). Moreover, the idea of cyber liability shows that cyber incidents leading to losses for investors can have civil and administrative legal consequences for the company (Silviani et al., 2023). Besides, the securities firms' fiduciary duty is to protect investor data as a trust, which cannot be an operational commodity (Shalihah & Mohd Shariff, 2022).

In the field of personal data protection, several studies indicate that Indonesia's legal framework has been moving towards a strengthening of privacy rights, but its implementation still encounters challenges in terms of institutional capacity, industry compliance and supervisory coordination. Rosadi & Pratama (2018) stressed the urgency of protection of personal data in the digital economy; Rosadi & Tahira (2018) stressed the importance of consumer protection in the digital economy era; Disemadi (2021) stressed the importance of specific regulation; and Rosadi et al. (2022) showed that the financial sector needs a combination of comprehensive regulation and self-regulation. Other studies such as Darmawan & Sekar Putri (2025); Sulistianingsih et al. (2023); Wibowo et al. (2024); Yuspin et al. (2023) also show that personal data regulations, especially in the financial sector, are not yet fully in line with modern cybersecurity requirements.

But the presence of such regulations does not answer the question of liability in the case of an actual ransomware attack. The attacks typically involve anonymous attackers, cross-border infrastructure and complex digital traces, making it difficult to prove fault, negligence and causation. Therefore, this study focuses on two important questions: how positive law protects investors and how the legal liability of securities firms is determined in case of data breaches or misuse due to ransomware attack. In this context, the journal does not only identify legal norms but also assesses whether the existing legal framework is suitable for more sophisticated cyber threats and requires higher due diligence standards from financial services providers.

METHODS

This article is a normative legal study, that is, a study that is primarily concerned with legal norms. The research is concerned with the relationship between regulation of the capital market, protection of personal data, electronic transactions and protection of consumers in the financial services sector. Owing to its normative nature, this study does not collect field data but rather examines and interprets relevant legal materials to address the research questions in a systematic manner.

Based on a literature review, studies that specifically link ransomware, the misuse of investors' personal data, and the liability of securities firms remain relatively limited. Some research addresses personal data in banking, fintech, e-commerce or the metaverse, whilst capital market issues tend to be discussed within the framework of investor protection or cyber risk in general. It is this gap that makes this journal significant, as it seeks to bring together the legal regimes governing the capital markets, personal data protection and electronic system security within a single, comprehensive analysis, as shown in Table 1.

Table 1. Relevant Previous Research

Researcher	Research Focus	Limitations of Previous Research	The Differences in the Focus of This Research	Novelty
Rosadi & Pratama (2018)	The importance of privacy and personal data in the digital economy.	Has not yet addressed the capital markets sector and corporate liability for ransomware attacks.	This study focuses its analysis on securities firms as business entities in the digital capital market.	This article goes beyond the general issue of privacy protection to examine how the legal liability of securities firms is established when investors' personal data is misused as a result of a ransomware attack.
Disemadi (2021)	The urgency of specific regulations and the use of artificial intelligence for the protection of personal data.	The focus remains on general regulatory requirements, rather than on corporate accountability in the financial services sector.	This study assesses the protection of personal data in the relationship between investors and securities firms.	This article broadens the scope of the study from general regulatory requirements to an analysis of the liability of securities firms, using the principles of duty of care and corporate negligence as the basis for assessing liability.
Rosadi et al. (2022)	Data privacy protection in artificial intelligence within Indonesia's financial sector.	It does not yet refer specifically to a ransomware incident and does not yet identify the securities firm as the main subject.	This study examines investor data breaches resulting from cyber-attacks on securities firms.	This article brings together the Personal Data Protection Act (PDP Act), the Electronic Information and Transactions Act (ITE Act) and the Payment Services Act (P2SK Act) within a single analytical framework to assess the legal liability of securities firms in the event of a ransomware attack.
Shalihah & Shariff (2022)	Data protection and investor privacy in equity crowdfunding.	The subject of study differs from that of conventional capital markets and does not focus on securities firms.	This study focuses on capital market investors as the subject of the data in relation to securities firms.	This article shifts the focus from equity crowdfunding to the conventional capital market, thereby examining investor protection in the context of securities firms affected by ransomware attacks.
Widiatedja & Mishra (2023)	The need for an independent data protection authority in Indonesia.	Does not specifically address the financial services sector and corporate accountability.	This study links OJK supervision with investor protection in the event of a cyber incident.	This article treats regulatory coordination as part of the analysis of securities firms' legal liability, rather than merely a discussion of the institutional framework of data protection authorities.

Darmawan & Sekar Putri (2025)	Protection of investors' personal data against cybercrime threats in the capital markets based on IOSCO principles.	Has not yet set out the basis for corporate liability in detail.	This study examines the form of legal liability of securities firms for data breaches caused by ransomware.	This article provides a more detailed analysis of contractual, civil and administrative liability, and links these to obligations regarding data security, monitoring and notification of data breaches.

Source: Compiled by the author from relevant journals

The approaches employed include a legislative approach, a conceptual approach and an analytical approach. The legislative approach was used to examine the Capital Market Act, the Personal Data Protection Act, the amended ITE Act, the P2SK Act and POJK 22/2023. The conceptual approach was used to examine the theories of legal protection, legal liability, unlawful acts, and the security of electronic systems. The analytical approach, meanwhile, was used to assess whether these legal provisions are adequate in addressing ransomware attacks against securities firms, as shown in Figure 1.

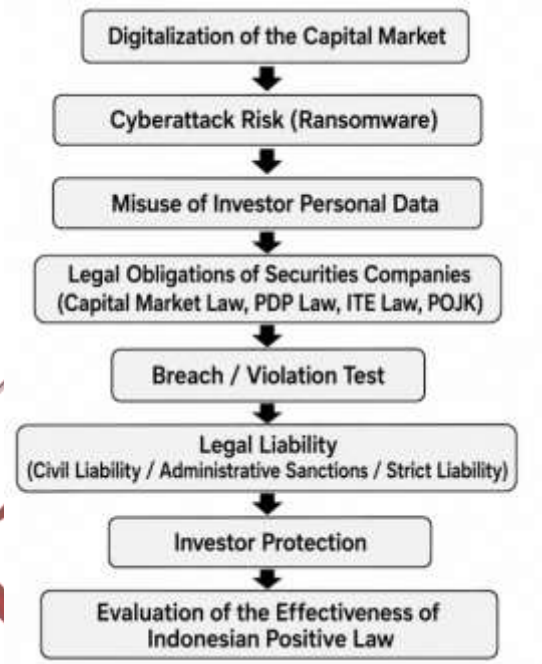

Figure 1. A Conceptual Framework for the Legal Liability of Securities Firms
Source: Compiled by the authors

The legal sources used comprise primary, secondary and tertiary sources. Legislation and OJK regulation as a main source. Secondary sources include books, journals and relevant findings from scientific research. Tertiary sources are used to help clarify terms and concepts. The analysis was conducted in a qualitative manner, through grammatical, systematic and teleological interpretation, providing a comprehensive overview of the basis for liability and forms of legal protection available to investors.

RESULT AND DISCUSSION

Legal Framework and Regulatory Gaps

The legal framework is largely there but has not yet been fully integrated. The Capital Markets Act requires securities firms to operate as business entities to keep order, fairness and investor interests in check. The Personal Data Protection Act increases obligations of data controllers to secure and protect the personal data that they process and requires that written notification be provided no later than 3 x 24 hours in the event of a personal data breach. Meanwhile, the legal basis for action against unauthorised access and manipulation of electronic systems remains the ITE Act as amended by Act No. 1 of 2024. At the same time, the P2SK Act and POJK 22/2023 also strengthen consumer protection, governance and the obligations of PUJKs in maintaining the confidentiality and security of consumer data.

These norms constitute, when read systematically, a fairly robust basis of liability. The main challenge is the lack of operational standards that address specifically how to respond to ransomware events in the capital markets industry. The positive law has not yet explicitly dealt with the burden of the losses in case an attack is launched by an external actor, but the losses are suffered because of the weaknesses of the internal security system. Here is where the concept of duty of care becomes critical as a securities firm cannot simply say that the attack was carried out by a third party, it must still show that reasonable preventative, monitoring and recovery measures were in place.

There are also regulatory gaps in the allocation of responsibilities with technology vendors, cloud providers and other third parties involved in the management of investor data. POJK 22/2023 requires PUJKs to keep the data confidential and secure, and to have other collaborating parties keep the data confidential, too, but this is still a matter of needing more operational standards of proof. The policy makers must therefore define minimum security parameters, periodic audits, encryption, access segmentation and incident response procedures, so that the legal provisions do not remain simply abstract obligations. The main provisions which are the basis of this analysis are summarized in the following table as shown in Table 2.

Table 2. The Relevant Legal Framework for Investor Protection and Data Security

Legal Instruments	Key Standards	Implications for Securities Firms
Law No. 8 of 1995 on the Capital Market	To ensure the orderly functioning of the capital market and safeguard the interests of investors	Securities firms are obliged to act with due care and to uphold investor confidence
Law No. 27 of 2022 on the Protection of Personal Data	Articles 35 and 46: data security obligations and notification of personal data breaches	It is mandatory to implement technical and organisational measures, and to provide timely notification in the event of an incident
Law No. 1 of 2024 on Information and Electronic Transactions	Prohibition of unauthorised access to and manipulation of electronic systems	To serve as the basis for taking action against attacks or unauthorised access to security systems
Law No. 4 of 2023 on P2SK	Strengthening governance and consumer protection in the financial sector	Reaffirming the accountability of financial services institutions in risk management
POJK No. 22/POJK.07/2023	Articles 19, 20, 21 and 22: confidentiality, security, exchange, transfer and prohibition on the use of consumer data	PUJK is obliged to safeguard data security, ensure third parties comply, and be prepared to face sanctions

Source: Compiled by the author from Law No. 8 of 1995, Law No. 27 of 2022, Law No. 1 of 2024, Law No. 4 of 2023, and POJK No. 22/POJK.07/2023.

The protection of privacy and personal data in the digital economy era still depends on fragmented regulations and therefore legal certainty is not yet fully secured (Rosadi & Pratama, 2018). Similarly, Disemadi (2021) argues that the personal data protection instruments in Indonesia are still fragmented and have not yet formed a truly integrated framework. Elsa et al. (2023) found that in the financial services sector, the OJK plays a key role in supervision, but the protection of personal data of users of digital financial services still depends heavily on the compliance of the supervised institutions. Therefore, securities firms must be able to demonstrate security policy, periodic audit, access management, data backup, and incident response readiness, not merely compliance with written standards.

From the regulatory point of view, the Personal Data Protection Act (PDP Act) stated that the protection of personal data includes all efforts to protect personal data in the data processing chain in order to guarantee the constitutional rights of data subjects including the obligations of personal data controllers and administrative sanctions. In the financial services sector, POJK 22/2023 enhances consumer protection by establishing consumer protection principles, specifying the rights and obligations of financial services institutions, imposing obligations for maintaining information system security and cyber resilience, and increasing the sanctions. Consequently, the operational architecture remains to be further clarified, even though the normative framework is already established, so that it is fully prepared to face the increasingly complex cyber threats.

Legal Liability of Securities Firms

There are a number of reasons for a securities firm can be held legally liable for a ransomware attack. First, contractual liability. The relationship between investors and securities firms does not end with the opening of a securities account but also gives rise to an obligation to maintain the integrity of the system, the confidentiality of access and the security of investors' data. If a company has not secured data and a data breach or account takeover occurs, this may be a breach of contract as the company has not sufficiently fulfilled the obligation to maintain security.

Secondly, civil liability for unlawful acts. The elements of an act, fault, loss and causal link can be applied to ransomware cases, thus preserving the relevance of article 1365 of the Civil Code. No intention needed here. Gross negligence will do if a company fails to install security updates, does not implement multi-factor authentication, does not restrict access rights, does not prepare adequate data backups and is not armed with a realistic recovery plan. In this sense, the evaluation concerns not only the behavior of individuals, but also the incapacity of the organization to install an adequate prevention system.

Thirdly, administrative liability. POJK 22/2023 allows the OJK to impose sanctions if financial services providers breach provisions relating to consumer protection, data security and sound governance. Consequently, a securities firm does not need to be the perpetrator of a ransomware attack to be held liable; it is sufficient to prove that it has been negligent in maintaining the requisite security measures. From this perspective, cyber liability can be understood as a corporate legal risk inherent to data controllers when internal security systems are inadequate.

This view is in line with Darmawan & Putri (2025), who highlight the growing threat of cybercrime in the capital markets sector and the need for an adaptive regulatory approach, as well as the research by Widiatedja & Mishra (2023), which emphasizes the importance of an independent data protection authority to effectively strengthen privacy protection. As cyber threats are complex, cross-jurisdictional and often involve anonymous perpetrators, the allocation of liability must be based on measurable standards of due diligence, rather than on the assumption that all attacks automatically constitute the absolute responsibility of the company.

Consequently, it is not yet appropriate to apply the strict liability regime absolutely to all ransomware incidents at securities firms. Cyber-attacks often involve anonymous perpetrators, span multiple jurisdictions and utilize complex attack techniques. Consequently, a more proportionate allocation of liability involves a combination of a high duty of care, a measured standard of proof of negligence, and effective administrative oversight. This model is more consistent with the nature of losses in the financial services sector, which is based on trust and data.

Case Study: The 2024 National Data Centre and Its Implications for the Securities Sector

The 2024 ransomware attack on the Interim National Data Centre showed how weak data security governance can have systemic consequences. BSSN said the incident was a "Brain Cipher" ransomware attack, that there had been attempts to disable Windows Defender and that various critical files and services had been affected. This shows that failure in one piece of digital infrastructure can snowball into a major barrier to public services and a complex technical recovery process.

From an analytical point of view, securities firms are private entities entrusted with the money and data of the investors and should be held to a higher standard of due diligence when it comes to public infrastructure owned by the state, which could be vulnerable to a cyber-attack. It is here that commercial civil liability becomes a much touchier issue as the losses do not just stop with service disruption but can lead directly to financial losses, identity theft and the loss of investor confidence. Therefore, cyber liability for securities firms should be seen as a corporate responsibility, which requires proactive avoidance rather than being a reactive measure.

From the perspective of investor rights protection, data breaches not only cause financial damage but also make investors susceptible to hacking of their accounts, manipulation of transactions and identity theft. Thus, reactive protection in the form of legal action or complaints should be supplemented by preventive measures, including independent security audits, vendor management, access segmentation, internal training and effective incident notification obligations. PDN 2024's experience in this area serves as a warning that data security must not be an administrative formality, but a vital prerequisite for the sustainability of digital services.

Implications for Investor Protection and the Effectiveness of Indonesian Regulation

In concept Indonesian law has gone toward stronger protection, but its effectiveness still relies on consistent implementation. The Personal Data Protection Act (UU PDP) has presented a clear normative framework, the Financial Sector Security Act (UU P2SK) has widened the scope to cover the financial sector ecosystem including the capital market and consumer protection and OJK Regulation No. 22/2023 confirms obligations concerning consumer data protection, information system security and cyber resilience. But without auditable technical guidelines, these obligations may remain only normative declarations. Hence, the incident response standards, common reporting requirements and clear allocation of responsibilities between securities firms, technology providers and regulators need to be clarified.

Investors suffering losses in the context of preventive legal protection should not wait for redress. The legal system must incentivize prevention from the outset, including requiring securities firms to keep data confidential, implement multi-factor authentication, improve digital security education, and provide rapid complaint channels. Only if compliance, supervision, and accountability are built into the business process from the beginning can data and investor protection be effective, according to Rosadi & Pratama (2018), Shalihah & Shariff (2022), and Darmawan & Putri (2025). Therefore, the investor protection regime of the digital capital market has to move from a declarative approach to an operational approach that can be truly tested.

The repressive approach requires investors to have access to the redress of losses through lodging complaints to the OJK, dispute resolution, civil proceedings, or criminal reports where criminal elements are present. This protective repression is important because most ransomware victims are unable to prove the technical details of the attack on their own. The burden of proof should therefore be interpreted in a proportionate way, i.e. requiring companies to explain the security standards they have implemented and to assess whether those standards were appropriate. This approach is in line with OJK's role in supervising the conduct of financial service providers and enforcing compliance and is relevant to strengthening investor protection in the digital capital market.

Therefore, real legal protection is the implementation of supervision, administrative punishment, education on digital security and transparency in incident handling. The present study highlights the fact that the protection of investors' personal data cannot be based solely on general norms but must be based on concrete and verifiable corporate governance practices. Overall, the effectiveness of investor protection in Indonesia will improve if regulations do not stop at abstract

obligations, but move towards auditable technical standards, including data breach notifications, independent security audits, accountability of technology vendors and more robust coordination between OJK, Komdigi and law enforcement agencies.

CONCLUSION

This study concludes that Indonesian positive law has provided a sufficient normative basis for protecting investors' personal data at securities firms, but the regulations remain sector-specific and are not yet fully integrated to address the risk of ransomware. The Capital Market Act, the Personal Data Protection Act, the Information and Electronic Transactions Act (as amended by Act No. 1 of 2024), the P2SK Act, and OJK Regulation No. 22/2023 all emphasise the importance of system security, consumer protection and the accountability of financial services institutions, but have not yet established truly operational technical standards for handling cyber incidents.

This study also found that the legal liability of securities firms can be established through contractual, civil and administrative means. The principles of duty of care, corporate negligence, cyber liability and fiduciary responsibility indicate that securities firms cannot simply hide behind third-party attacks when internal negligence also contributes to the potential for losses. In this context, the most proportionate approach to liability is a fault-based model with a high standard of care, rather than strict liability applied in an absolute manner.

From the perspective of investor protection, the direction of Indonesia's legal reforms should focus on strengthening data breach notifications, independent security audits, the liability of technology vendors, and more effective inter-agency coordination. With these improvements, protection of investors' personal data can move from being a merely declaratory norm to an operational and measurable legal protection that indeed provides legal certainty.

Suggestions

The Government and the Financial Services Authority need to set out more detailed rules for minimum standards of cybersecurity for securities firms including risk classification, audit requirements, data back-ups and incident response procedures.

Securities firms should strengthen security measures based on risk, including multi-factor authentication, access segmentation, system upgrades, regular penetration testing, and strict supervision of third parties managing investor data.

Investors also need access to complaint and redress mechanisms that are fast, transparent and readily available, so that legal protection is not limited to a mere normative recognition but truly instills a sense of security and legal certainty.

REFERENCES

Darmawan, K., & Sekar Putri, A. (2025). Legal protection for investors' personal data against cybercrime threats in capital market based on IOSCO principles. JLPH: Journal of Law, Politic and Humanities, 5(4). https://doi.org/10.38035/jlph.v5i4

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. Jurnal Wawasan Yuridika, 5(2), 177. https://doi.org/10.25072/jwy.v5i2.460

Elsa, Panjaitan, H., & Kandou, H. (2023). Peran otoritas jasa keuangan terhadap perlindungan dan penanggulangan penyalahgunaan data pribadi sebagai upaya perlindungan hukum pengguna layanan fintech. Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat, 9(1). https://doi.org/https://ejournal.fhuki.id/index.php/tora/article/view/535

Manurung, E. A. P. (2023). The right to privacy based on the law of the Republic of Indonesia Number 27 of 2022. Journal of Digital Law and Policy, 2(3). https://doi.org/10.2991/iciir18.2019.32

Mayasari, H. (2023). A examination on personal data protection in metaverse technology in Indonesia: A human rights perspective. Journal of Law, Environmental and Justice, 1(1), 64–85. https://doi.org/10.62264/jlej.v1i1.4

Rachmat, U. M., Riyanto, S., & Fh, A. (2024). Optimalisasi perlindungan konsumen dalam melakukan komplain atas produk barang cacat melalui self regulation pada transaksi pembelian secara online PT.Bukalapak. Jurnal Hukum Jurisdictie, 6(1), 68–83. https://doi.org/10.34005/jhj.v6i1.166

Rosadi, S. D., & Pratama, G. G. (2018). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. Jurnal: Veritas et Justitia, 4(1), 88–110. https://doi.org/10.25123/vej.2916

Rosadi, S. D., & Tahira, Z. (2018). Consumer protection id digital economy era: Law in Indonesia. Jurnal Yustisia, 7(1), 85–97. https://doi.org/https://doi.org/10.20961/yustisia.v7i1.20144

Rosadi, S. D., Yuniarti, S., & Fauzi, R. (2022). Protection of data privacy in the era of artificial intelligence in the financial sector of Indonesia. Journal of Central Banking Law and Institutions, 1(2), 353–366. https://doi.org/10.21098/jcli.v1i2.18

Shalihah, F., & Mohd Shariff, R. N. (2022). Identifying barriers to data protection and investor privacy in equity crowdfunding: Experiences from Indonesia and Malaysia. UUM Journal of Legal Studies, 13(2), 215–242. https://doi.org/10.32890/uumjls2022.13.2.9

Silviani, N. Z., Shahrullah, R. S., Atmaja, V. R., & Hyun, P. J. (2023). Personal data protection in private sector electronic systems for businesses: Indonesia vs. South Korea. Jurnal Hukum Dan Peradilan, 12(3), 517. https://doi.org/10.25216/jhp.12.3.2023.517-546

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Shidqon Prabowo, M. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis Undang-Undang Perlindungan Data Pribadi). Jurnal Masalah-Masalah Hukum, 52(1), 97–106.

Syaputra, M., Irhamsah, I., & Ridwan, R. (2024). Konsekuensi hukum dan tanggung jawab notaris terhadap akta yang mengandung unsur penyalahgunaan keadaan. SENTRI: Jurnal Riset Ilmiah, 3(4), 1901–1910. https://doi.org/10.55681/sentri.v3i4.2564

Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. Cogent Social Sciences, 10(1). https://doi.org/10.1080/23311886.2024.2306751

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: a future–forward perspective. International Review of Law, Computers & Technology, 37(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793

Yusliwidaka, A., Muhammad Ardhi Razaq Abqa, & Khansadhia Afifah Wardana. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? Pandecta Research Law Journal, 19(2), 453–482. https://doi.org/10.15294/pandecta.v19i2.13279

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal data protection law in digital banking governance in Indonesia. Studia Iuridica Lublinensia, 32(1), 99130. https://doi.org/10.17951/sil.2023.32.1.99-130

Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal. https://peraturan.bpk.go.id/Details/46197/uu-no-8-tahun-1995

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. https://peraturan.bpk.go.id/Details/240203/uu-no-4-tahun-2023

Peraturan Otoritas Jasa Keuangan Nomor 22/POJK.07/2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. https://www.ojk.go.id/id/regulasi/Documents/Pages/Pelindungan-Konsumen-danMasyarakat-di-Sektor-JasaKeuangan/POJK%2022%20Tahun%202023%20Pelindungan%20Konsumen%20dan%20Masyarakat%20di%20Sektor%20Jasa%20Keuangan.pdf