Volume 1 Issue 2 (2024) 11-18
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v1i2.2
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

Legal Implications of Data Breach Cases in Indonesia: Challenges And Solutions in The Era of Personal Data Protection

Abdullah Khudori[1*], Andi Lala[2]
[1] Politeknik Siber Cerdika Internasional
[2] Institut Teknologi Petroleum Balongan Indramayu
Corresponding email:abdullahkhudori62@gmail.com*

ABSTRACT

In the digital era, cases of Data leaks in Indonesia continue to increase, causing various implications for the law on personal data protection. Inadequate regulation and a lack of law enforcement lead to uncertainty and financial loss for individuals and organizations. Therefore, an effective solution is needed to overcome the challenges in the era of personal data protection. Study This aiming to analyze the implications of the law from case data leaks in Indonesia and offers solutions to face the challenges that arise along with the implementation of the Constitution on Personal Data Protection. This study employs a qualitative method with a case study approach. Data obtained through analysis of documents, laws, regulations, and studies of literature about data leaks in Indonesia. Additionally, interviews with expert lawyers and practitioners in the field of data security are conducted to gain a more in-depth understanding. Research results show that challenges in personal data protection in Indonesia include the uncertainty of the law, weak enforcement of regulations, and a lack of public awareness. Research This also provides recommendation policy For strengthen regulation and improve mechanism personal data protection in Indonesia.

Keywords: *data breaches, personal data protection, regulation law, challenges law, Indonesia*

1. Introduction

In the increasingly digital era, the issue of personal data leakage has become a serious concern in many countries, including Indonesia (Gani, 2024; Marune & Hartanto, 2021). As the number of online transactions and interactions increases, the amount of personal data collected, processed, and stored by various parties also continues to rise. Unfortunately, inadequate system security often causes data leaks, which not only harm individuals but also damage the company's reputation and

expose it to legal risks. A major data breach case involving a number of institutions in Indonesia, such as what happened with BPJS Kesehatan in 2021, show urgency greater protection of personal data strict (Kominfo, 2021).

Urgency study This driven by the existence of significant threat to privacy individual and inadequacy regulations that exist in Indonesia in face data leak. Although has There is Constitution Personal Data Protection (PDP Law), challenges in its implementation Still Lots found. One of the most common problems happen is weakness mechanism enforcement law and not existence clear minimum standards about personal data protection in Indonesia. This is strengthen need For identify solution practical that can implemented soon (Setiadi, 2022).

Table 1. The Urgency of Data Breach in Indonesia

NO	FACTS/FINDINGS	SOURCE
1	BPJS Health Data Leak	Ministry of Communication and Information, 2021
2	Improvement of the incident data leak in	Statistics, 2022
3	Weakness mechanism enforcement law after the PDP Law was passed (2022)	Digital Rights Asia,
4	Ranking in the Data Protection Regulations Index (2023)	Data Protection Regulations Index, 2023
5	70% of companies do not yet understand the PDP Law	Indonesian Cybersecurity Forum,
6	65% of institutions use standard security that is not GDPR compliant (2022)	Indonesian Information Security Association, 2022

Sources: Compiled by the authors from various official reports (2021–2023)

In general, theoretically, data leaks can be viewed from a contractual perspective, where the service provider lacks sufficient legal protections to safeguard the personal data of its users. In several jurisdictions, improperly handled data leaks can be considered a breach of contract or negligence, resulting in severe legal sanctions (Ehimuan et al., 2024). In Indonesia, although the PDP Law has been ratified, the implementation of the data security standard is still minimal. This fact confirms the importance of increasing awareness about the inadequate responses to law-related data leaks and the need to enhance security information.

Several studies have previously examined data leaks and their impact on society. Al Ikhsan (2024) researched case data leaks in the e-commerce sector and found that weak regulation contributes to a high amount of case data leaks. On the other hand, Pemmasani (2022) highlighted the critical role of strong regulation in reducing data leaks in the public sector. Research emphasizes the need to reform regulatory and enforcement laws to address the challenge of data leaks.

Although several studies have been conducted on data leaks, there have been no studies specifically analyzing the implications of data leaks in Indonesia, focusing

on the changes and hazards. It has not been done. Not much has been done. Most studies are limited to evaluating policy without addressing the aspect of enforcing effective laws in the event of data leaks. This is a research gap that needs to be filled with a more in depth analysis of the solution law that can be applied in a practical way in Indonesia.

The uniqueness of the study lies in its comprehensive approach to analyzing not only the challenges posed by regulations but also solutions that can be applied to enhance personal data protection in Indonesia. Research. This also provides an analysis and comparison between practice data protection in Indonesia and other countries that have successfully addressed case data leaks, such as the European Union, through the General Data Protection Regulation (GDPR).

This study aims to analyze the implications of data leaks in Indonesia, identify challenges in implementing the PDP Law, and offer solutions to enhance personal data protection in Indonesia. Thus, research is expected to give a real contribution to strengthening regulations and mechanisms for greater protection of personal data.

2. Method

Types of research

Study: This approach uses qualitative design studies. A qualitative approach was chosen because the study aims to comprehensively and in-depth understand the implications of laws and challenges related to personal data leaks in Indonesia, as well as offer relevant solutions within the context of data protection. A case study was conducted to investigate data leaks that have occurred in Indonesia, both in the public and private sectors.

Population and Sampling

The study's population encompasses all institutions, government agencies, private companies, and user services affected by data leaks in Indonesia. A research sample was taken purposively, focusing on a few cases, including the most significant data leaks ever, such as the BPJS Kesehatan data leak and e-commerce incidents. In addition, experts in law, privacy-focused attorneys, and cybersecurity practitioners were also interviewed to provide a deeper insight into related challenges and solutions regarding data leaks.

Instrument Research (Research Instrument)

Instrument research used includes guidelines, semi structured interviews, and analysis of Documents. Guideline interviews were used to gather information from expert lawyers, cybersecurity practitioners, and representatives of affected institutions. A data leakage analysis was conducted on policies, laws, and regulations related to personal data protection, including the Personal Data Protection Act and the rules issued by the Ministry of Communications and Information.

Collection Technique (Data Collection Technique)

Data collected through two primary methods:

1. Interview deeply with the experts in law, practitioner security, cyber, and privacy focused lawyers. Interview. This aims to gain a better understanding of the challenges faced in implementing the Personal Data Protection Act and handling data leaks.
2. Analysis of laws, regulations, and cases of data leaks that occurred in Indonesia. Documents analyzed include the Personal Data Protection Act, cybersecurity policies, and reports on official case data leaks.

Procedure Research (Research Procedure)

The procedure study started with a stage of collecting literature and documents related to data leaks and personal data protection in Indonesia. After that, the selection of a sample case of significant data leak became the focus of research. An interview with experts, law practitioners, security, and cyber professionals was conducted after the guidelines interview was arranged. Every interview was recorded and transcribed for analysis. More continues. Data from analysis documents and interviews, then integrated to get comprehensive findings.

Data Analysis Technique

Data analyzed uses a thematic analysis technique. First step is to read the transcript interviews and documents to identify the main themes related to implications of law data leaks, challenges in implementing data protection, and proposed solutions. After the theme's main identified, the data is then categorized into relevant subthemes. Analysis done in an iterative way to ensure that all important aspects from implications, law, challenges, and solutions are covered well. Analysis results are then exposed in a descriptive form to describe the solution law that can be implemented in Indonesia.

3. Result & Discussion

Analysis Legal Implications of Data Breach Cases in Indonesia

leak cases in Indonesia have give impact significant law, both for responsible institution answer on data management and individuals who are victims (Tanzilla et al., 2023). In some cases, such as BPJS Health data leak, there is ambiguity in implementation sanctions law for negligent party (Pattipeilohy, 2023; Shahrullah et al., 2024). Constitution The Personal Data Protection Act (PDP Act) which was enacted in 2022 actually designed For give more protection strong, but its enforcement Still face various obstacle (Syailendra et al., 2024). Many companies and institutions the public who have not fully understand or apply regulation This in a way effective (Dwivedi et al., 2021).

In addition, data leaks are often considered as violation privacy, which has implications for loss reputation for company or the relevant institution. In law, personal data protection violations can categorized as violation contractual or even violation laws, depending on the context and magnitude impact. Interview results with practitioner law show that Lots company No own standard adequate security,

so that increase risk data leak (Landoll, 2021). This becomes problem crucial in the middle the more development digital transactions in Indonesia.

Implications law from data leaks also involve uncertainty in implementation sanctions. Although the PDP Law has arrange about sanctions administrative and criminal, in the practice enforcement law Still less than optimal. No supervisory body strong independent make Lots violation No investigated with serious, so that victims of data leaks often do not get adequate protection (Solove & Hartzog, 2022). This is confirm the need improvement effort in strengthen enforcement law in the sector personal data protection.

Challenges in Implementation of the Personal Data Protection Act in Indonesia

One of challenge the biggest in the implementation of the PDP Law in Indonesia is weakness enforcement law. Although Constitution the has designed with Enough comprehensive, its implementation in the field Still meet various constraints. Many companies Not yet own adequate internal policies For protect personal data, and authorities enforcer law often not own sufficient capacity For supervise data breach effective (Lancieri, 2022). This is exacerbated by the low awareness public about importance personal data protection.

Challenge next lies in the lack of infrastructure adequate technology For support data protection. Many companies and institutions public Still use old technology is vulnerable to attack cyber. In the case of e-commerce data leaks in Indonesia, for example, were discovered that system encryption used Not yet follow standard more international safe, so that increase risk data hacking (Uriawan et al., 2024). Disadvantages in matter technology This put Lots organization in a weak position in guard personal data security user.

In addition, the challenges in the implementation of the PDP Law is also related with insufficiency source Power competent human being in the field data security (Usman, 2024). Many organizations Not yet own dedicated team For manage and protect personal data. Lack of training and education in the field This make Lots company No Ready face threat data leak. This is show the need improvement capacity at various levels, including government and sector private, for ensure that personal data protection can implemented with Good.

Legal and Policy Solutions For Strengthen Personal Data Protection

One of solution main For overcome problem data leaks in Indonesia are strengthen mechanism enforcement law. This is can done with form a supervisory body independent who has authority full For supervise implementation of the PDP Law in various sector. This agency must own authority For give strict sanctions to offender as well as provide clear guidelines for company related standard personal data security (Voss & Bouthinon-Dumas, 2021). In addition, the government need adopt standard more international strict in personal data protection.

Improvement competence source Power humans also become solution important. Through training specializing in the field data security, both in the sector government and also private, organization can more Ready in face challenge data leak. Training This No only intended to IT team, but also to management the company that

must understand implications law from data leaks (Al-Harrasi et al., 2021). In addition, the company must required For to form team special handling personal data protection in a way professional and sustainable.

From a technological standpoint, updating system security becomes a necessity. Using more sophisticated encryption, such as encryption based on blockchain, can become a solution to reduce the risk of future data leaks. Standards of security. This must be adopted by all companies that manage personal data, particularly those operating in highly vulnerable sectors such as banking, healthcare, and e-commerce (Morić et al., 2024). With a combination of more vigorous enforcement of laws, increased human Power, and more sophisticated technology, personal data protection in Indonesia is expected to be more guaranteed.

4. Conclusion

This study highlights the implications of the law, challenges, and solutions in the face of data leaks in Indonesia, particularly after the enactment of the Personal Data Protection Act. From the results analysis, it can be concluded that data leaks have a significant impact on the law, both for individuals who are victims and for institutions that are negligent in protecting data. Enforcement law in Indonesia regarding data leaks remains suboptimal, primarily due to weaknesses in the implementation of regulations, a shortage of competent human resources, and inadequate infrastructure and technology.

Challenge in implementation of the PDP Law also includes weakness in public awareness, as well as low understanding of companies and institutions of their obligations under the law they protect personal data. Although regulations have been implemented, without supervision and enforcement, a strong law, risk data leaks persist at a high rate. In addition, the cybersecurity infrastructure in many organizations is still inadequate to face the increasingly complex threats.

To overcome this challenge, some proposed solutions include the formation of an independent supervisory body with the authority to uphold the law, improve competence, and source Power through training, as well as the adoption of more secure technologies, such as encryption and blockchain-based encryption. With these steps, it is expected that personal data protection in Indonesia can be significantly improved, providing better protection for society and minimizing the impact of future data leaks.

5. References

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875–888.

Al Ikhsan, M. I., & Zubaedah, R. (2024). Legal Protection For Platform User Who Are Harmed By Data Leaks In E-Commerce And Prevention Efforts By The

Government. *International Journal of Education, Information Technology, and Others*, *7*(1), 179–186.

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., & Krishen, A. S. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, *59*, 102168.

Ehimuan, B., Chimezie, O., Akagha, O. V., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070.

Lancieri, F. (2022). Narrowing data protection's enforcement gap. *Me. L. Rev.*, *74*, 15.

Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press.

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, *4*(3), 731–761.

Pattipeilohy, E. C. T. (2023). Juridical analysis of personal data protection in the case of BPJS personal data leakage reviewed from a positive legal perspective. *The International Journal of Politics and Sociology Research*, *11*(2), 373–383.

Pemmasani, P. K., & Abd Nasaruddin, M. A. (2022). Strengthening Public Sector Data Governance: Risk Management Strategies for Government Organizations. *International Journal of Modern Computing*, *5*(1), 108–118.

Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, *10*(1), 1–20.

Solove, D. J., & Hartzog, W. (2022). *Breached!: Why data security law fails and how to improve it*. Oxford University Press.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indon. L. Rev.*, *14*, 175.

Tanzilla, F. D., Hanita, M., & Widiawan, B. (2023). Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. *International Journal of Progressive Sciences and Technologies (IJPSAT)*, *40*(2).

Uriawan, W., Musthofa, A., Sutrisno, A. E. P., & Ali, F. I. (2024). *Digital Forensics for Vulnerability Personal Data on E-Commerce Platform (Case Study: Tokopedia Customer Data)*.

Usman, N. (2024). Legal Protection Of Personal Data And Authority Accountability For Cyber Security: Pdp Law Review. *Law Research Review Quarterly*, *10*(1).

Voss, W. G., & Bouthinon-Dumas, H. (2021). EU general data protection regulation sanctions in theory and in practice. *Santa Clara High Tech. LJ*, *37*, 1.