E-JUSTICE: JOURNAL OF LAW AND TECHNOLOGY

Vol. 1 No. 1, September 2024, pp 1-15

Research Article

Towards Enhanced Personal Data Protection: A Novel Approach to Regulation and Practice in Indonesia

Andi Rifky Maulana *Efendy*[1]

Corresponding e-mail: mey22023@grips.ac.jp

Article Information

Article History
Received: May 26th, 2024
Revised: Sept 21st, 2024
Accepted: Sept 24st, 2024

Keywords:
Data Breach; Data Privacy; Data Protection Law; Data Protection; Indonesia; Personal Data.

How to Cite:
Efendy, Andi Rifky Maulana. "Towards Enhanced Personal Data Protection: A Novel Approach to Regulation and Practice in Indonesia." *E-Justice: Journal of Law and Technology* 1, no. 1 (2024): 1-15.

Abstract

Background: The digital era has significantly impacted various sectors, increasing internet usage in Indonesia to over 170 million in 2021. This surge raises critical concerns about personal data protection, which includes safeguarding information like names, addresses, and online activities from misuse.

Methodology: A qualitative, descriptive-analytical approach is used, reviewing secondary data from legal documents, academic literature, regulatory reports, and case studies. Content analysis identifies themes related to data protection, implementation challenges, and international regulatory comparisons.

Objectives: This study evaluates the Indonesia's personal data protection regulations, compares them with international standards like the GDPR, and identifies challenges in implementation. The goal is to provide actionable recommendations for improving data protection in Indonesia.

Findings: Significant weaknesses in Indonesia's data protection regulations include ambiguous definitions and insufficient guidelines for cross-border data transfers. Challenges include low public awareness, limited law enforcement capacity, and rapidly evolving technology outpacing regulatory updates. Data breaches, such as those involving SIM card and bank customer data, underscore the need for improved protection measures. Comparisons with GDPR highlight the need for

[1] National Graduates Institute for Policy Studies, Japan | https://orcid.org/0009-0005-1923-1030

broader regulatory scope, clearer definitions, stronger individual rights, and stricter sanctions in Indonesia.

Originality/Novelty: This study integrates multiple perspectives and offers a comprehensive approach to understanding and improving personal data protection in Indonesia. By comparing local regulations with international best practices, it provides insights and innovative recommendations tailored to Indonesia's specific context, crucial for enhancing regulatory effectiveness and fostering a secure digital environment.

Introduction

The digital era has brought significant changes in various aspects of human life. Advances in information and communication technology have opened up vast opportunities in various fields, including the economy, education, health, and governance.[1] In Indonesia, internet usage has drastically increased in recent years. According to data from the Association of Internet Service Providers in Indonesia (APJII), the number of internet users in Indonesia reached over 170 million people in 2021. This demonstrates the importance of the internet in the daily lives of Indonesian society.

However, along with the increasing use of digital technology, various issues related to the protection of personal data have emerged. Personal data refers to information that can be used to identify individuals, such as names, addresses, phone numbers, email addresses, national identification numbers, and financial information. In the digital context, personal data also includes information collected through online activities, such as search history, geographical location, and social media interactions.[2]

The protection of personal data is becoming increasingly important because personal data is often processed and stored by various parties, including technology companies, internet service providers, and social media platforms.[3] This personal data can be used for various purposes, such as marketing, business analysis, and research. However, without adequate

[1] Jacqueline Hicks, "A 'Data Realm' for the Global South? Evidence from Indonesia," *Third World Quarterly* 42, no. 7 (July 3, 2021): 1417–35, https://doi.org/10.1080/01436597.2021.1901570.
[2] Dona Budi Kharisma and Alvalerie Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare* 17, no. 2 (May 16, 2024): 157–69, https://doi.org/10.1108/IJHRH-04-2022-0035.
[3] H. Matnuh, "Rectifying Consumer Protection Law and Establishing of a Consumer Court in Indonesia," *Journal of Consumer Policy* 44, no. 3 (September 5, 2021): 483–95, https://doi.org/10.1007/s10603-021-09487-z.

protection, personal data can be misused by irresponsible parties, such as identity theft, fraud, and privacy violations.

In Indonesia, the issue of personal data protection has received serious attention from the government and the public.[4] The Indonesian government has adopted various regulations to protect the personal data of citizens, including Minister of Communication and Information Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems. However, there are still many challenges in implementing these regulations, such as the lack of public awareness of the importance of personal data protection, the limited capacity of law enforcement, and the rapid pace of technological development that exceeds the speed of regulation.[5]

Several previous studies have examined aspects of personal data protection in Indonesia. For example, research by Setiadi (2018) highlighted the gap between existing regulations and practices in the field, as well as the need to enhance law enforcement capacity. Another study by Amalia (2020) discussed the importance of public education in increasing awareness of personal data protection. Furthermore, research by Rachman (2019) compared data protection regulations in several Southeast Asian countries, indicating that Indonesia is still lagging behind in several important aspects. However, most of these studies tend to focus on a specific aspect, such as regulation or education, without integrating various perspectives into a comprehensive analytical framework.

Unlike previous studies that tend to focus on a specific aspect, this research takes a comprehensive approach by examining the effectiveness of personal data protection regulations in Indonesia and comparing them in depth with international regulations such as the GDPR. This research not only focuses on the analysis of existing regulations but also considers various challenges in their implementation from legal, technical, and institutional perspectives. Thus, this research is expected to provide innovative and applicable recommendations that are suitable for the specific context and needs of Indonesia, as well as to help increase public awareness and understanding of the importance of personal data protection. The main difference between this research and previous studies is the integration of multidimensional perspectives and comparison with international practices, providing a holistic approach to understanding and improving personal data protection in Indonesia.

Based on the above background, there are several main issues that need to be identified and further analyzed. Current personal data protection regulations in Indonesia need to be examined more deeply to understand how effective the existing rules are in protecting the

[4] Leon Trakman, Robert Walters, and Bruno Zeller, "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience," *Information & Communications Technology Law* 29, no. 2 (May 3, 2020): 218–49, https://doi.org/10.1080/13600834.2020.1726021.

[5] Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (January 3, 2024): 1, https://doi.org/10.20956/halrev.v10i1.5016.

personal data of citizens. Furthermore, it is important to identify the challenges faced in implementing these regulations, including legal, technical, and institutional factors that may hinder effective personal data protection. Furthermore, comparison with international regulations such as the General Data Protection Regulation (GDPR) in the European Union will provide insights into best practices that can be adopted in Indonesia. Ultimately, this research aims to provide concrete and applicable recommendations for improving personal data protection in Indonesia.

Research Method

This research uses a qualitative design with a descriptive-analytical approach to examine personal data protection regulations in Indonesia and identify challenges in their implementation. The data sources used are secondary data obtained through literature reviews and analysis of legal documents, academic literature, regulatory reports, and case studies. The legal documents analyzed include Regulations on Personal Data Protection in Electronic Systems and various other related regulations. Furthermore, this research also compares regulations in Indonesia with international regulations such as the General Data Protection Regulation (GDPR) in the European Union to gain a more comprehensive understanding of personal data protection practices.

Data collection techniques are conducted through content analysis of relevant legal documents and literature. These documents and literature are selected based on their relevance to the research topic and their contribution to providing insights into personal data protection. Data analysis is carried out by identifying the main themes related to personal data protection, implementation challenges, and comparison with international regulations. The findings from this analysis are then used to develop recommendations that can be implemented to improve personal data protection in Indonesia. This methodology allows researchers to examine in-depth the legal and policy aspects that affect personal data protection in Indonesia, as well as to provide informed views for the improvement of regulations in the future.

Overview of Personal Data Protection Regulation in Indonesia

The protection of personal data is becoming increasingly crucial in this digital era where information exchange and the use of information technology are rampant. In Indonesia, efforts to safeguard personal data have been regulated by various laws; however, the effectiveness and depth of such protection remain significant questions.[6] One of the primary regulations governing personal data protection in Indonesia is Minister of Communication and Information Regulation No. 20 of 2016 concerning Personal Data

[6] Danarto Tri Sasongko, Putu Wuri Handayani, and Riri Satria, "Analysis of Factors Affecting Continuance Use Intention of the Electronic Money Application in Indonesia," *Procedia Computer Science* 197 (2022): 42–50, https://doi.org/10.1016/j.procs.2021.12.116.

Protection in Electronic Systems.[7] While this regulation establishes a legal framework for data protection, its implementation in practice has faced several challenges. These include inconsistent enforcement, limited public awareness, and the lack of comprehensive oversight mechanisms, all of which undermine the regulation's effectiveness in safeguarding personal data.

This regulation aims to govern the collection, processing, storage, and deletion of personal data within electronic systems. It encompasses various provisions that outline the responsibilities of electronic system providers in maintaining the confidentiality, integrity, and availability of the personal data they manage. Furthermore, the regulation establishes individuals' rights regarding their personal data, such as the right to access, correct, and delete their personal data.[8]

Despite efforts to regulate personal data protection, this regulation still has several weaknesses that need to be addressed. One of them is the lack of detail and clarity in certain provisions. For instance, the regulation does not specifically define the types of personal data that should be protected and does not provide clear guidelines on the technical security measures that electronic system providers should implement. This ambiguity can lead to different interpretations and leave loopholes for detrimental practices.[9]

Moreover, the scope of this regulation is limited to electronic system providers operating in Indonesia. In a globally connected digital era, personal data is often processed and stored by entities outside Indonesia's jurisdiction. This poses challenges in law enforcement because Indonesian regulations lack the authority to oversee or penalize foreign entities that violate the privacy of Indonesian citizens. The lack of international cooperation regarding personal data protection also hinders addressing cases involving foreign entities.

Another weakness of this regulation is the lack of provisions regarding cross-border data transfers. In the digital era, cross-border data transfers are common occurrences, both in international business contexts and personal interactions. Existing regulations have not clearly stipulated how cross-border data transfers should be conducted and what requirements must be met to ensure the continued protection of personal data when transferred abroad. This is crucial to address considering the numerous multinational companies operating in Indonesia and often engaging in international data transfers.

---

[7] Ratna Januarita, Indra Fajar Alamsyah, and Arif Perdana, "Guardians of Data: TruMe Life's Continuous Quest for Data Protection," *Journal of Information Technology Teaching Cases*, March 26, 2024, https://doi.org/10.1177/20438869241242141.

[8] David Erdos, "The 'Right to Be Forgotten' beyond the EU: An Analysis of Wider G20 Regulatory Action and Potential next Steps," *Journal of Media Law* 13, no. 1 (January 2, 2021): 1–35, https://doi.org/10.1080/17577632.2021.1884947.

[9] Sukarmi Sukarmi, Kukuh Tejomurti, and Udin Silalahi, "Digital Market and Its Adequacy of Merger Assessment in Indonesian Business Competition Law," *International Journal of Law and Management*, March 21, 2024, https://doi.org/10.1108/IJLMA-08-2023-0185.

Furthermore, despite the existence of regulations governing personal data protection in Indonesia, their implementation still poses challenges. Effective regulation implementation requires strong and consistent law enforcement. However, the capacity of law enforcement agencies to handle cases of personal data breaches is limited. Law enforcement officers often lack adequate resources or technical capabilities to identify and address cases of personal data breaches. This results in low levels of law enforcement and sanctions against violators, thus failing to provide sufficient deterrence. Weak law enforcement also impacts public trust in the government's ability to protect their personal data.

Besides, the rapid advancements in information technology present a unique challenge in the implementation of personal data protection regulations. Existing regulations often struggle to keep pace with the speed of technological innovation, making them less relevant and effective in addressing new challenges. For example, the emergence of big data technology, artificial intelligence, and the Internet of Things (IoT) brings new challenges in terms of the collection and use of personal data. Existing regulations need to be continuously updated and adapted to these technological developments to remain effective.[10]

In response to various shortcomings and challenges in existing regulations, the Indonesian government has enacted Law No. 27 of 2022 on Personal Data Protection. This law is expected to provide a stronger and more comprehensive legal foundation for protecting personal data in Indonesia. Law No. 27 of 2022 establishes various new provisions that are more detailed and clear compared to previous regulations.

This law provides a clearer definition of personal data, encompassing information that can identify an individual directly or indirectly. Data subjects are granted broader rights, including the right to know the purpose and legal basis of data collection, the right to withdraw consent, and the right not to be subject to fully automated decisions. Data controllers are required to ensure that the personal data they manage is protected with adequate security measures and in accordance with applicable standards. They must also appoint a data protection officer and report data breach incidents within a specified period.[11]

The law regulates cross-border data transfers in more detail, stipulating that personal data can only be transferred to countries that have equivalent or higher levels of data protection, or through mechanisms approved by the competent authority. Law enforcement is

[10] Zaka Firma Aditya and Sholahuddin Al-Fatih, "Indonesian Constitutional Rights: Expressing and Purposing Opinions on the Internet," *The International Journal of Human Rights* 25, no. 9 (October 21, 2021): 1395–1419, https://doi.org/10.1080/13642987.2020.1826450.

[11] Ari Wibowo, Widya Alawiyah, and Azriadi, "The Importance of Personal Data Protection in Indonesia's Economic Development," *Cogent Social Sciences* 10, no. 1 (December 31, 2024), https://doi.org/10.1080/23311886.2024.2306751.

strengthened with provisions on administrative and criminal sanctions for violators, including significant fines and the possibility of imprisonment for serious violations.

With the enactment of Law No. 27 of 2022, it is hoped that the protection of personal data in Indonesia can be enhanced. This law provides a clearer and more detailed framework, which is expected to reduce legal loopholes and increase legal certainty for all parties involved in managing personal data. However, the success of implementing this law still depends on the commitment of all parties, including the government, law enforcement agencies, and industry players, to enforce and comply with the existing provisions.

Challenges in the Implementation of Personal Data Protection

The challenges in implementing personal data protection in Indonesia are highly complex and require a holistic approach. One of the main challenges is the low level of awareness and understanding among the public regarding the importance of personal data protection. Many individuals in Indonesia are unaware of the risks associated with the misuse of personal data. This is exacerbated by the lack of education and awareness campaigns conducted by the government and other relevant parties. Without adequate understanding of the importance of personal data protection, people tend to be less cautious about sharing their personal information online, leaving gaps for cybercriminals to exploit their data.[12]

In addition to the low public awareness, the capacity of law enforcement agencies to handle cases of personal data breaches is also a serious challenge. Law enforcement agencies often lack adequate resources or technical capabilities needed to identify and handle cases of personal data breaches.[13] As a result, the enforcement of laws against personal data breaches is low, failing to provide sufficient deterrence for violators and, in turn, reducing public trust in the government's ability to protect their personal data.

The rapid development of information technology also poses challenges in the implementation of personal data protection. Existing regulations often cannot keep pace with the pace of technological innovation, making them less relevant and effective in addressing emerging challenges. For example, the emergence of big data technology, artificial intelligence, and the Internet of Things (IoT) brings new challenges in terms of the collection and use of personal data. Big data analytics can lead to privacy concerns due to the large-scale aggregation of data, often without explicit consent. Artificial intelligence can make decisions based on personal data, raising issues of transparency, bias, and accountability. The IoT, with its interconnected devices, increases the risk of unauthorized

[12] Admiral Admiral and Mega Ardina Pauck, "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services," *Lex Scientia Law Review* 7, no. 2 (November 30, 2023): 995–1048, https://doi.org/10.15294/lesrev.v7i2.77881.
[13] Leanna Ireland, "Predicting Online Target Hardening Behaviors: An Extension of Routine Activity Theory for Privacy-Enhancing Technologies and Techniques," *Deviant Behavior* 42, no. 12 (December 2, 2021): 1532–48, https://doi.org/10.1080/01639625.2020.1760418.

access and data breaches. Therefore, existing regulations need to be continuously updated and adjusted to these technological developments to remain effective and relevant.

Furthermore, there are still weaknesses in the regulations governing personal data protection in Indonesia. One of them is the lack of provisions governing cross-border data transfers. In this era of globalization, cross-border data transfers are common, both in the context of international business and personal interactions. However, existing regulations have not clearly stipulated how cross-border data transfers should be conducted and what requirements must be met to ensure that personal data remains protected when transferred abroad. This lack of provisions leaves room for harmful practices and complicates law enforcement at the international level.

Moreover, the implementation of personal data protection in Indonesia also faces challenges related to the diversity of sectors and interests involved. Each sector, such as banking, telecommunications, and healthcare, has different characteristics and needs regarding personal data protection. This requires a more holistic and integrative approach to ensure that all sectors can protect personal data to high standards. Separate sectoral approaches can lead to inconsistencies and legal gaps that can be exploited by violators.[14]

By identifying and addressing these challenges, it is hoped that the implementation of personal data protection in Indonesia can be enhanced. Collaborative efforts between the government, the private sector, and civil society are needed to increase public awareness, enhance law enforcement capacity, update existing regulations, and address the challenges faced. Only through a holistic approach and strong cooperation from various parties can effective and sustainable personal data protection be achieved in Indonesia.[15]

Cases of Personal Data Violations

Cases of personal data violations are alarming incidents often resulting in significant impacts on individuals, companies, and society at large. In Indonesia, as in many other countries, these cases have garnered significant attention due to the increased penetration of information technology and internet usage.[16] According to data from the Ministry of Communication and Information, there have been 79 cases of data theft in Indonesia since 2019. Just in the period from January to June 2023, there were 35 cases, surpassing the

[14] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57, https://doi.org/10.1108/JFC-09-2021-0193.
[15] Reza Ashari Nasution et al., "Digital Mastery in Indonesia: The Organization and Individual Contrast," *Journal of Management Development* 39, no. 4 (May 11, 2020): 359–90, https://doi.org/10.1108/JMD-03-2019-0081.
[16] Sinta Dewi Rosadi et al., "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?," *International Review of Law, Computers & Technology* 37, no. 1 (January 2, 2023): 78–90, https://doi.org/10.1080/13600869.2022.2114660.

number of data leaks that occurred annually from 2019 to 2021. Below are some notable data leakage cases that have occurred in Indonesia:

In 2022, the personal data of Indonesian citizens' SIM cards was sold by a hacker known as Bjorka. Reportedly, approximately 1.3 billion SIM card registration data were leaked, including NIK (Indonesian ID number), provider telephone numbers, and registration dates, totaling 87 GB in data size. These data were priced at Rp743.5 million.

In 2023, a data breach involving Bank Syariah Indonesia (BSI) customers occurred. The incident began with service disruption complaints on May 8, 2023. The Lockbit ransomware group, originating from Russia, claimed to have successfully stolen 1.5 TB of personal data of BSI customers. They negotiated with BSI for a ransom of Rp296 billion. As the ransom was not paid, Lockbit distributed the data on the black market on May 16, 2023. In the same year, another data breach occurred with the leakage of 34 million passport data. This data breach was also carried out by hacker Bjorka. The data was uploaded on July 5, 2023, including names, passport numbers, passport expiration dates, dates of birth, and genders. These data were sold for Rp150 million.

The latest data breach occurred on July 14, 2023, with the leakage of 337 million Dukcapil (Population Administration) data uploaded to the BreachForums site by a user claiming to be RRR. The leaked data included names, family card numbers (KK), dates of birth, addresses, parents' NIKs, birth certificate numbers, marriage certificate numbers, and religions. These cases highlight the vulnerability of personal data to cyberattacks and the importance of personal data protection.[17] Challenges in handling cases of personal data violations include identification, handling, and law enforcement against perpetrators. This process requires strong cooperation and effective coordination among various institutions and stakeholders, both nationally and internationally.

Amidst increasingly complex and diverse threats, companies and government institutions need to enhance their security measures to protect the personal data of users and customers. Public education and awareness of cyber threats also need to be improved to help individuals identify and avoid cyberattacks.[18] Only through collective efforts from various parties can we protect personal data and maintain privacy and security in this increasingly connected digital era.

Comparison with International Regulations

In addressing the challenges of personal data protection, it is important to compare with international regulations, especially with regulations considered as global standards, such as the General Data Protection Regulation (GDPR) in the European Union. GDPR has been

[17] Kharisma and Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union."
[18] Ratna Yudhiyati, Afrida Putritama, and Diana Rahmawati, "What Small Businesses in Developing Country Think of Cybersecurity Risks in the Digital Age: Indonesian Case," *Journal of Information, Communication and Ethics in Society* 19, no. 4 (December 13, 2021): 446–62, https://doi.org/10.1108/JICES-03-2021-0035.

the primary reference in regulating personal data protection worldwide since its enforcement in May 2018.[19] In comparison, Minister of Communication and Information Regulation No. 20 of 2016 in Indonesia, although attempting to regulate personal data protection, differs significantly from GDPR in several key aspects.[20]

One major difference between these regulations is in terms of scope and definitions. GDPR has a broader scope, not only limiting itself to entities in the European Union but also regulating any entities processing data of individuals in the EU, including entities outside the EU. This means that GDPR has extensive extraterritorial effects, compelling global companies to comply with high standards of personal data protection if they want to operate in the EU market.[21] Meanwhile, regulations in Indonesia are more focused on entities operating domestically, without considering activities of entities operating abroad but processing data of Indonesian citizens.

Furthermore, in terms of definitions, GDPR is more detailed and comprehensive in defining various terms used in the regulation, such as the definition of personal data, data processing, and data controller. These clear and detailed definitions provide better legal clarity and certainty for stakeholders, as well as minimize potential variations in interpretation.[22] On the other hand, regulations in Indonesia tend to be more general in their definitions, leaving room for broader interpretations and potential ambiguity in implementation.

Moreover, there are differences in the individual rights recognized and protected by both regulations. GDPR grants extensive rights to individuals regarding their personal data, including the right to access their personal data, request correction if there are errors, delete data (right to be forgotten), and refuse data processing for specific purposes. These rights provide significant control to individuals over their personal data and promote transparency from data controllers.[23] In contrast, regulations in Indonesia, while acknowledging some individual rights, may not be as comprehensive as GDPR in recognizing and protecting these rights.

---

[19] Rizaldy Anggriawan et al., "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?," *Hasanuddin Law Review* 8, no. 2 (July 30, 2022): 95, https://doi.org/10.20956/halrev.v8i2.2844.

[20] Sihabudin Sihabudin, "Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations," *Brawijaya Law Journal* 10, no. 1 (April 30, 2023): 59–71, https://doi.org/10.21776/ub.blj.2023.010.01.04.

[21] Fatema Kawaf, Annaleis Montgomery, and Marius Thuemmler, "Unpacking the Privacy–Personalisation Paradox in GDPR-2018 Regulated Environments: Consumer Vulnerability and the Curse of Personalisation," *Information Technology & People* 37, no. 4 (May 6, 2024): 1674–95, https://doi.org/10.1108/ITP-04-2022-0275.

[22] Andreas Häuselmann and Bart Custers, "Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR," *Computer Law & Security Review* 52 (April 2024): 105942, https://doi.org/10.1016/j.clsr.2024.105942.

[23] Max von Grafenstein et al., "Privacy Icons as a Component of Effective Transparency and Controls under the GDPR: Effective Data Protection by Design Based on Art. 25 GDPR," *Computer Law & Security Review* 52 (April 2024): 105924, https://doi.org/10.1016/j.clsr.2023.105924.

Furthermore, GDPR imposes heavy sanctions on violators. Penalties that can reach up to 20 million euros or 4% of the total global annual revenue of a company, whichever is higher, provide strong deterrent effects and encourage companies to seriously comply with the regulations. These severe penalties compel companies to take adequate security measures and ensure that the personal data they manage is well-protected.[24] On the other hand, to date, regulations in Indonesia may not have enforced sanctions as stringent as GDPR, which could reduce incentives for companies to comply with the regulations seriously.[25]

Nevertheless, comparing with international regulations, such as GDPR, can be a valuable learning source for Indonesia in efforts to improve and strengthen regulations on personal data protection in the country. Indonesia could adopt several specific aspects of the GDPR, such as its clear definitions of personal data and sensitive data, which enhance understanding and enforcement. Furthermore, incorporating individual rights—like the right to data portability and the right to be forgotten—would empower citizens over their personal information. Furthermore, establishing robust mechanisms for enforcement and significant penalties for violations, as seen in the GDPR, could incentivize compliance among organizations..[26] By looking at best practices applied by international regulations and adopting them according to local contexts and needs, Indonesia can enhance the effectiveness and relevance of regulations on personal data protection, thus safeguarding the privacy and security of citizens' personal data in this digital age.[27]

Conclusion

The digital era has brought significant changes in various aspects of life, including in Indonesia, with a drastic increase in internet users. However, along with the benefits of technology, issues of protecting personal data have emerged that are important to address. Personal data, whether collected online or offline, needs to be safeguarded to prevent misuse such as identity theft and privacy breaches. Indonesia has taken important steps through various regulations, such as Minister of Communication and Informatics Regulation No. 20 of 2016 and Law No. 27 of 2022 concerning Personal Data Protection. These regulations aim to regulate the collection, processing, storage, and deletion of

[24] Valentin Rupp and Max von Grafenstein, "Clarifying 'Personal Data' and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection," *Computer Law & Security Review* 52 (April 2024): 105932, https://doi.org/10.1016/j.clsr.2023.105932.

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

[26] Lena Enqvist, "Rule-Based versus AI-Driven Benefits Allocation: GDPR and AIA Legal Implications and Challenges for Automation in Public Social Security Administration," *Information & Communications Technology Law*, May 9, 2024, 1–25, https://doi.org/10.1080/13600834.2024.2349835.

[27] Muhammad Khaeruddin Hamsin et al., "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection," *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (April 17, 2023): 53–66, https://doi.org/10.24090/mnh.v17i1.7633.

personal data, as well as to establish individuals' rights regarding their data. Nevertheless, challenges in implementing these regulations remain significant, including low public awareness, limited law enforcement capacity, and rapid technological developments.

Cases of personal data breaches, such as those involving SIM card and bank customer data theft, demonstrate the urgency to enhance personal data protection. Other challenges faced include suboptimal regulations in governing cross-border data transfers and weak law enforcement. Comparisons with international regulations such as GDPR in the European Union indicate that Indonesia needs to expand the scope of regulations, clarify definitions, strengthen individual rights, and increase sanctions for violations. Adopting best practices from international regulations can assist Indonesia in enhancing the effectiveness of personal data protection. Success in protecting personal data in Indonesia will depend on collaboration among the government, law enforcement, private sector, and society. Through joint efforts, it is hoped that the protection of personal data can be enhanced, preserving privacy and providing security in this increasingly interconnected digital era.

Acknowledgement

None

Conflict of Interest

None

Author(s) Contribution

Author contribution : Initiated the research ideas, data collection, analysis, and draft writing.

References

Aditya, Zaka Firma, and Sholahuddin Al-Fatih. "Indonesian Constitutional Rights: Expressing and Purposing Opinions on the Internet." *The International Journal of Human Rights* 25, no. 9 (October 21, 2021): 1395–1419. https://doi.org/10.1080/13642987.2020.1826450.

Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." *Lex Scientia Law Review* 7, no. 2 (November 30, 2023): 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881.

Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?" *Hasanuddin Law Review* 8, no. 2 (July 30, 2022): 95. https://doi.org/10.20956/halrev.v8i2.2844.

Enqvist, Lena. "Rule-Based versus AI-Driven Benefits Allocation: GDPR and AIA Legal Implications and Challenges for Automation in Public Social Security Administration." *Information & Communications Technology Law*, May 9, 2024, 1–25. https://doi.org/10.1080/13600834.2024.2349835.

Erdos, David. "The 'Right to Be Forgotten' beyond the EU: An Analysis of Wider G20 Regulatory Action and Potential next Steps." *Journal of Media Law* 13, no. 1 (January 2, 2021): 1–35. https://doi.org/10.1080/17577632.2021.1884947.

Grafenstein, Max von, Isabel Kiefaber, Julie Heumüller, Valentin Rupp, Paul Graßl, Otto Kolless, and Zsófia Puzst. "Privacy Icons as a Component of Effective Transparency and Controls under the GDPR: Effective Data Protection by Design Based on Art. 25 GDPR." *Computer Law & Security Review* 52 (April 2024): 105924. https://doi.org/10.1016/j.clsr.2023.105924.

Hamsin, Muhammad Khaeruddin, Abdul Halim, Rizaldy Anggriawan, and Hilda Lutfiani. "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection." *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (April 17, 2023): 53–66. https://doi.org/10.24090/mnh.v17i1.7633.

Häuselmann, Andreas, and Bart Custers. "Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR." *Computer Law & Security Review* 52 (April 2024): 105942. https://doi.org/10.1016/j.clsr.2024.105942.

Hicks, Jacqueline. "A 'Data Realm' for the Global South? Evidence from Indonesia." *Third World Quarterly* 42, no. 7 (July 3, 2021): 1417–35. https://doi.org/10.1080/01436597.2021.1901570.

Ireland, Leanna. "Predicting Online Target Hardening Behaviors: An Extension of Routine Activity Theory for Privacy-Enhancing Technologies and Techniques." *Deviant Behavior* 42, no. 12 (December 2, 2021): 1532–48. https://doi.org/10.1080/01639625.2020.1760418.

Januarita, Ratna, Indra Fajar Alamsyah, and Arif Perdana. "Guardians of Data: TruMe Life's Continuous Quest for Data Protection." *Journal of Information Technology Teaching Cases*, March 26, 2024. https://doi.org/10.1177/20438869241242141.

Kawaf, Fatema, Annaleis Montgomery, and Marius Thuemmler. "Unpacking the Privacy–Personalisation Paradox in GDPR-2018 Regulated Environments: Consumer Vulnerability and the Curse of Personalisation." *Information Technology & People* 37, no. 4 (May 6, 2024): 1674–95. https://doi.org/10.1108/ITP-04-2022-0275.

Kharisma, Dona Budi, and Alvalerie Diakanza. "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union." *International Journal of Human Rights in Healthcare* 17, no. 2 (May 16, 2024): 157–69. https://doi.org/10.1108/IJHRH-04-2022-0035.

Matnuh, H. "Rectifying Consumer Protection Law and Establishing of a Consumer Court

in Indonesia." *Journal of Consumer Policy* 44, no. 3 (September 5, 2021): 483–95. https://doi.org/10.1007/s10603-021-09487-z.

Nasution, Reza Ashari, Devi Arnita, Linda Sendy Lediana Rusnandi, Elis Qodariah, Priyantono Rudito, and Mardi Fretdi Natalina Sinaga. "Digital Mastery in Indonesia: The Organization and Individual Contrast." *Journal of Management Development* 39, no. 4 (May 11, 2020): 359–90. https://doi.org/10.1108/JMD-03-2019-0081.

Rosadi, Sinta Dewi, Andreas Noviandika, Robert Walters, and Firsta Rahadatul Aisy. "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?" *International Review of Law, Computers & Technology* 37, no. 1 (January 2, 2023): 78–90. https://doi.org/10.1080/13600869.2022.2114660.

Rupp, Valentin, and Max von Grafenstein. "Clarifying 'Personal Data' and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection." *Computer Law & Security Review* 52 (April 2024): 105932. https://doi.org/10.1016/j.clsr.2023.105932.

Sasongko, Danarto Tri, Putu Wuri Handayani, and Riri Satria. "Analysis of Factors Affecting Continuance Use Intention of the Electronic Money Application in Indonesia." *Procedia Computer Science* 197 (2022): 42–50. https://doi.org/10.1016/j.procs.2021.12.116.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (January 3, 2024): 1. https://doi.org/10.20956/halrev.v10i1.5016.

Sihabudin, Sihabudin. "Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations." *Brawijaya Law Journal* 10, no. 1 (April 30, 2023): 59–71. https://doi.org/10.21776/ub.blj.2023.010.01.04.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (September 30, 2022): 1443–57. https://doi.org/10.1108/JFC-09-2021-0193.

Sukarmi, Sukarmi, Kukuh Tejomurti, and Udin Silalahi. "Digital Market and Its Adequacy of Merger Assessment in Indonesian Business Competition Law." *International Journal of Law and Management*, March 21, 2024. https://doi.org/10.1108/IJLMA-08-2023-0185.

Trakman, Leon, Robert Walters, and Bruno Zeller. "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience." *Information & Communications Technology Law* 29, no. 2 (May 3, 2020): 218–49. https://doi.org/10.1080/13600834.2020.1726021.

Wibowo, Ari, Widya Alawiyah, and Azriadi. "The Importance of Personal Data Protection in Indonesia's Economic Development." *Cogent Social Sciences* 10, no. 1 (December 31, 2024). https://doi.org/10.1080/23311886.2024.2306751.

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

Yudhiyati, Ratna, Afrida Putritama, and Diana Rahmawati. "What Small Businesses in Developing Country Think of Cybersecurity Risks in the Digital Age: Indonesian Case." *Journal of Information, Communication and Ethics in Society* 19, no. 4 (December 13, 2021): 446–62. https://doi.org/10.1108/JICES-03-2021-0035.