Jurnal Multidisiplin Indonesia (JOUMI)
Vol.3, No.2 Juni 2025
e-ISSN: 2986-7541; p-ISSN: 2986-7533, Hal 01-23
DOI: https://doi.org/10.62007/joumi.v3i2.404

Protection of Personal Data of Indonesian Migrant Workers regarding Certainty of Protection of Indonesian Migrant Workers while in the Destination Country

Muhammad Abdurrohman Sholih
Universitas Borobudur
Email: omanji@gmail.com

Richard
Universitas Borobudur
Email: richard@borobudur.ac.id

*Korespondensi penulis: *omanji@gmail.com*

Abstract: *Indonesian Migrant Workers (PMI) are a vulnerable group who face various risks in destination countries, including the potential for misuse of their personal data. As the migration process becomes digital, the volume and sensitivity of PMI data managed by various parties increases, creating a strong urgency for data protection. This study aims to analyze the relationship between personal data protection and the certainty of legal protection and overall security of PMI in destination countries. Using a qualitative research method based on secondary data analysis covering Law Number 27 of 2022 concerning Protection of Personal Data (UU PDP), Law Number 18 of 2017 concerning Protection of Indonesian Migrant Workers (UU PPMI), reports from related institutions, and case studies, this study examines the legal framework, international dimensions, risks, and implementation challenges. The findings show that the PDP Law is an important legal foundation, complementing the PPMI Law, but its implementation faces significant challenges related to institutional capacity, coordination, private sector compliance, system security, PMI literacy, and cross-border law enforcement. Strengthening comprehensive and integrated PMI data governance is urgently needed to ensure the security and certainty of protection of PMI rights abroad.*
Keywords: *Personal Data Protection, Indonesian Migrant Workers, PDP Law, PPMI Law, Legal Certainty, Cyber Security, Cross-Border Data Transfer.*

INTRODUCTION

Indonesian Migrant Workers (PMI) are important actors in the national economy, especially through their significant remittance contributions to state revenues and the welfare of their families in their homeland. However, behind these contributions, PMI often face various forms of vulnerability and rights violations, both in the migration process and during their work in the destination country. Issues such as unpaid wages, inhumane working conditions, violence, even exploitation and human trafficking, are real threats that loom over them. In the current era of globalization and digitalization, the dynamics of migrant worker placement not only involve physical and administrative aspects, but also involve digital aspects in the form of the collection, management, and distribution of personal data on a large scale. Various actors are involved in managing this data, ranging from government agencies such as BP2MI and foreign representatives, placement companies (P3MI), agents in destination countries, to employers, all of whom have access to PMI's personal data, including highly sensitive information such as health records, biometric data, and financial information.

Unfortunately, data processing in the context of labor migration does not fully guarantee the protection of PMI privacy rights. Several cases show that PMI personal data is

Received Juni 06, 2024; Accepted Juni 24 2025; Published Juni 30, 2025
*Muhammad Abdurrohman Sholih, *omanji@gmail.com*

often the target of misuse, both by irresponsible parties domestically and by individuals in the destination country. Practices such as document falsification for illegal recruitment, fake job vacancy fraud that leads to human trafficking (TPPO), and exploitation that uses data as a tool of intimidation, are real forms of weak PMI data protection. Data leaks from unsafe management systems also open up great opportunities for identity theft and other losses. In this context, protection of personal data is not just a technical issue, but is an integral part of legal protection and human dignity of PMI.

In response to this issue, the Indonesian government has passed two important laws, namely Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers (PPMI Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PPMI Law generally establishes a framework for protecting migrant workers in all stages of migration, while the PDP Law provides a more technical and detailed legal basis for protecting personal data in all sectors, including labor migration. Although both have the spirit of protection, there is still the potential for a lack of synergy between the administrative provisions in the PPMI Law and the principles of personal data control in the PDP Law. In practice, institutions such as BP2MI or P3MI can be trapped in fulfilling administrative obligations without paying attention to the aspects of data subject rights as required by the PDP Law.

Therefore, it is important to examine how these two legal frameworks interact and are implemented in an integrated manner, and how they are able to address the real challenges faced by migrant workers, especially regarding the management of personal data in the destination country. This study focuses on the analysis of national legal frameworks and relevant international standards, with the aim of assessing the effectiveness of data protection in creating legal certainty and a sense of security for migrant workers. In addition, this study also aims to identify challenges in implementing the law, both at the domestic level and across jurisdictions, and explore the possibility of improving policies and protection mechanisms that are more responsive to the needs of migrant workers. With a qualitative approach and based on secondary data, this study is expected to provide conceptual and practical contributions in formulating a more comprehensive migrant worker protection strategy in the future.

RESEARCH METHODS

This study uses a qualitative method with a normative legal approach and case studies based on secondary data (Somantri, 2005). The normative legal approach is used to examine the applicable positive legal norms relevant to the protection of personal data of Indonesian Migrant Workers (PMI), especially as regulated in Law Number 27 of 2022 concerning Protection of Personal Data (UU PDP) and Law Number 18 of 2017 concerning Protection of Indonesian Migrant Workers (UU PPMI). The primary data in this study are in the form of official texts of these laws and regulations, which are analyzed in order to understand the formal legal framework that forms the normative basis for PMI protection. In addition, this study also utilizes case studies to understand the dynamics and actual problems faced by PMI in the context of protecting their personal data, both in the placement process and during their work abroad.

Secondary data in this study were collected from various credible sources to enrich the perspective of the analysis. These sources include official reports from government institutions such as the Indonesian Migrant Workers Protection Agency (BP2MI) and Komnas HAM, report documents from non-governmental organizations such as Migrant CARE which are

active in advocating for migrant workers' rights, articles from scientific journals discussing the legal and social aspects of migrant protection, and news from the mass media documenting actual cases related to leaks or misuse of migrant workers' data. In addition, bilateral agreement documents between Indonesia and the destination countries were also analyzed to see how the issue of personal data protection is regulated in the context of cross-border cooperation.

Data analysis was conducted interpretively with the aim of identifying patterns, relationships, and meanings contained in regulations and practices for protecting PMI personal data. Through this approach, the research not only focuses on the normative content of legal texts, but also tries to understand how these provisions are implemented in reality, and how effective they are in guaranteeing PMI privacy and security rights. This analysis process also involves a synthesis between legal norms and empirical findings from secondary data in order to form a more comprehensive understanding. Thus, this methodological approach is expected to reveal potential gaps between norms and practices, and contribute to strengthening data protection policies for PMI in a more integrated and effective manner.

RESULTS AND DISCUSSION

International Standards and Laws of the Main Destination Countries

Globally, there are several frameworks and principles that serve as references in protecting personal data. The OECD Privacy Guidelines, for example, set out eight basic principles: limitation of collection, data quality, purpose specification, limitation of use, security safeguards, transparency, individual participation, and accountability. These principles have been adopted by many countries and form the basis for the development of data protection legal frameworks, including the Indonesian PDP Law. In the Asia-Pacific region, the APEC Privacy Framework and the Cross-Border Privacy Rules (CBPR) System are also relevant. The CBPR, which is based on the APEC Privacy Framework (which itself is inspired by the OECD Guidelines), provides a voluntary certification mechanism for companies to demonstrate compliance with internationally recognized data protection standards, facilitating cross-border data transfers among participating APEC economies. The APEC CBPR emphasizes the principle of accountability rather than restrictions on data transfers based on the domestic laws of the recipient country.

However, the implementation of PMI data protection in the field is highly dependent on the specific laws applicable in each destination country (Djafar & Santoso, 2019). There is significant variation in the level of maturity and stringency of data protection laws across PMI's main destination countries:

1. Malaysia:Has Personal Data Protection Act (PDPA) 2010. In 2024, Malaysia passed significant amendments to PDPA 2010, aimed at aligning it more closely with international standards. These amendments broadened the definition of sensitive data (to include biometric data), introduced a definition of "personal data breach", required the appointment of a Data Protection Officer (DPO), required notification of data breaches to authorities and data subjects, significantly increased penalties (fines up to MYR 1 million, imprisonment up to 3 years), reorganized the cross-border data transfer mechanism (replacing the "white-list" regime), and introduced the right to data portability. However, issues of effective enforcement and the need for transparency in the management of PMI data in Malaysia remain concerns (Kusnadi, 2021).
2. Saudi Arabia:Implementing the Personal Data Protection Law (PDPL) effective September 2023, with a grace period for compliance until September 2024. The PDPL sets out data subject rights (access, rectification, erasure, etc.), obligations for data controllers and

processors (including registration with authorities, DPIAs, appointment of DPOs in certain circumstances), and data breach notification mechanisms. The rules for overseas data transfers are considered stricter than the GDPR, requiring data subject consent or meeting specific conditions such as treaty obligations, national interest, or the existence of an equivalent level of protection in the recipient country. The supervisory authority is the Saudi Data and Artificial Intelligence Authority (SDAIA) (Veranda & Nusantara, 2024).

3. Hong Kong:Having the Personal Data (Privacy) Ordinance (PDPO) in place since 1996, it is one of the oldest data protection regimes in Asia. The PDPO is based on six Data Protection Principles (DPPs) that govern data collection, accuracy and retention, use, security, disclosure of information and access. Amendments in 2021 focused on tackling doxing. The PDPO applies to data of living individuals processed in Hong Kong, including PMI data. There is no legal obligation to appoint a DPO, although best practices are recommended. PMI immigration-related data is also managed by the Hong Kong Immigration Department (Faizah et al, 2023).
4. Taiwan:Governed by the Personal Data Protection Act (PDPA), which initially applied to certain sectors but was expanded to all sectors since 2012. The last amendment was made in 2023. Taiwan is in the process of establishing the Personal Data Protection Commission (PDPC) as a single independent supervisory authority, expected to be fully operational by August 2025. There are also specific regulations instructing migrant worker remittance companies to have a personal data security plan (Nugroho et al, 2025).
5. Singapore:Implementing the Personal Data Protection Act (PDPA) 2012, with amendments in 2020. This Act has extraterritorial effect and applies to private organisations that process personal data of Singapore residents. Singapore's PDPA sets out nine core obligations: Consent, Purpose Limitation, Notification, Access and Correction, Accuracy, Protection, Retention Limitation, Transfer Limitation, and compliance with the Do Not Call (DNC) Registry. The Act also provides individuals with the right to data portability. The public sector is governed by a separate framework (IM8 and the Public Sector Governance Act) (Soemitro et al, 2023).

These variations in the legal framework create complexities for Indonesia in ensuring consistent protection of migrant worker data across destination countries, as mandated by Article 56 of the PDP Law. Assessing the "equivalence" of the level of protection becomes a complex task for data controllers (P3MI/BP2MI) and Indonesian PDP Institutions. For countries with newer rules or untested implementation (such as Saudi Arabia), reliance on "adequate safeguard" mechanisms (e.g. bilateral agreements) or "migrant worker consent" becomes more likely. However, migrant worker consent, in the context of often unequal power relations between workers and employers/agents, does not necessarily meet the standard of free, specific, informed and unambiguous consent as expected under the data protection principles (Rosadi, 2023).

Furthermore, the existence of the PDP Law in the destination country does not automatically guarantee the security of migrant worker data in practice. The specific application of the law to migrant worker data, which is often managed by individual employers in the informal sector or small-scale placement agencies, may face its own law enforcement challenges in that country. Individual employers may be untouched by regulations or unaware of their obligations. Small agencies may lack the resources to comply. The PDP authority of the destination country may also prioritize supervision of large corporations. As a result, migrant workers remain vulnerable to data misuse by parties who directly manage their

information, even if there is a formal data protection law in the country. This strengthens the argument that protecting migrant worker data requires a multi-layered approach involving Indonesian national law, destination country law, and specific monitoring and enforcement mechanisms that focus on the migrant worker sector, ideally through strong bilateral agreements and active monitoring by the Indonesian Representative (Firmansyah, 2024).

Cross-Border Data Transfers and Bilateral Agreements

The transfer of personal data of Indonesian migrant workers from Indonesia to the destination country is a necessity in the placement process. Article 56 of the PDP Law is the main legal basis that regulates this transfer mechanism, by requiring an equal or higher level of protection in the recipient country, or adequate and binding safeguards, or approval from the migrant worker themselves (Aulia, 2024). In this context, a bilateral agreement or Memorandum of Understanding (MoU) between Indonesia and the destination country can function as a form of adequate and binding safeguard.

Analysis of existing MoUs with some key destination countries reveals diverse focuses and challenges regarding data management:

1. Malaysia:The MoU signed in April 2022 mandates the use of the One Channel System (OCS) as the sole mechanism for the entire process of placement, monitoring, and repatriation of domestic migrant workers. The OCS is designed as a data-sharing platform between the two countries to increase transparency and oversight. However, its implementation faces serious challenges. Malaysia is reportedly still using an alternative online recruitment system (Maid Online System/SMO) which is considered not in accordance with the spirit of the OCS and has the potential to facilitate non-procedural placement, which led to the temporary suspension of Indonesian migrant worker deployment in mid-2022. In addition to implementation issues, the cybersecurity of the OCS system itself is also a crucial question. A study shows that the OCS has not met adequate cybersecurity standards and there is no ministry that is clearly responsible for its security, so that the integrated migrant worker data in it is potentially vulnerable (Cabinet Secretariat of the Republik of Indonesia, 2022).
2. Saudi Arabia:After a moratorium on sending migrant workers since 2015 due to rampant cases of exploitation, Indonesia and Saudi Arabia are in the process of reopening cooperation on placement. The new MoU plan is expected to include a better protection scheme, including a minimum wage guarantee, health and life insurance, and data integration between the two countries for monitoring (Ikhsan, 2021). Previously, there was a Technical Arrangement (TA) regarding the OCS Pilot Project for limited deployment. This data integration is expected to improve protection, but also brings similar data security challenges to OCS in Malaysia if not designed and managed properly.
3. Hong Kong:Available sources do not detail any specific MoU regarding data sharing protocols with Hong Kong. Protection of Indonesian Migrant Workers relies more on the role of the Indonesian Consulate General (KJRI) and monitoring of placement agencies. The PPMI Law is the main legal basis for protection (Maulida, 2020).
4. Taiwan:Indonesia and Taiwan (through IETO and TETO) signed an MoU in December 2018 on the recruitment, placement, and protection of Indonesian migrant workers. The MoU aims to enhance cooperation, prevent exploitation, and ensure that Indonesian migrant workers receive protection in accordance with applicable laws in Taiwan. The Indonesian Economic and Trade Office (IETO) in Taipei plays an important role in protecting Indonesian migrant workers, including immigration matters (Mita Noveria,

2021).

While MoUs are important instruments, the main challenge is that negotiations often focus more on physical placement, wage standards, working conditions, and resolving visible cases of exploitation. The more technical and 'less visible' aspects of personal data protection may not be a top priority in bilateral negotiations. As a result, the resulting MoUs may not contain sufficiently strong, specific, and measurable data protection clauses in accordance with PDP Law standards or international best practices. For example, they do not set minimum security standards for migrant worker data held by employers or agencies in the destination country, do not establish PDP compliance audit mechanisms, or are unclear about procedures for handling cross-border data breaches. The implementation of the OCS in Malaysia also shows that agreements on paper do not necessarily run smoothly in the field (Abdurrohman, 2020).

Furthermore, centralized data sharing systems such as the OCS or the one planned with Saudi Arabia, while well-intentioned, create single points of failure. If these systems fail to be adequately secured, the potential for PMI data leaks could have a massive impact, compromising the privacy and safety of thousands of PMIs simultaneously. This is far more risky than sporadic data leaks from individual P3MIs. System failures such as the OCS not only harm PMIs but also undermine trust between countries and hinder future bilateral cooperation. Therefore, the design and implementation of cross-border PMI data sharing systems must prioritize cybersecurity and adherence to data protection principles (such as privacy by design) from the outset, rather than as an afterthought. Independent security audits and clear incident response protocols are an absolute necessity. The Indonesian negotiating team also needs to increase capacity and awareness of the urgency of data protection, ensuring that strong data protection clauses are a standard part of any PMI-related MoU negotiations.

CONCLUSION

The conclusion of the research results and discussion shows that the application of artificial intelligence (AI) technology has great potential to revolutionize the DPR RI's oversight function. Identification of strategic areas of supervision, such as budget supervision, implementation of laws, government policies, procurement of goods/services, and management of public aspirations, indicates that AI can strengthen the accuracy, efficiency, and timeliness of legislative decision-making. In budget supervision, AI enables earlier detection of anomalies and potential fraud through machine learning and data mining, while also helping to design more accurate budget predictions. In terms of supervision of the implementation of laws, AI, especially Natural Language Processing (NLP), is able to analyze regulatory compliance and systematically assess the impact of policies with the support of quantitative and qualitative data. In terms of government policy supervision, AI offers the ability to analyze public sentiment broadly and simulate the impact of alternative policies before they are implemented. Meanwhile, in procurement supervision, AI can uncover corrupt patterns such as collusion or price mark-ups through e-procurement analysis and project reporting. Furthermore, the use of AI in managing public aspirations also shows high significance. With a very large volume of complaints, AI can classify and direct issues quickly and accurately to relevant parties, while also assisting the DPR in setting priorities for the oversight agenda based on societal trends. Various technologies such as NLP, machine learning, computer vision, and AI-based interactive dashboards show concrete contributions in every line of oversight. The case study of ETLE (e-ticketing) in Indonesia strengthens the argument that AI has been able to be applied

in the law enforcement system and shows increased accountability and process efficiency. However, the complexity of legislative oversight tasks requires wisdom and political considerations that cannot be completely replaced by machines. Therefore, AI should be positioned as a strategic tool, not as a substitute for legislators, in order to strengthen the quality and reach of DPR oversight as a whole. With proper implementation, AI can help transform legislative oversight to be more proactive, data-based, and adaptive to the dynamics of the times.

REFERENCES

Abdurrohman, MG Policy on Sending Female Workers Abroad; Comparison of Government Regulation No. 10 of 2020 and Fatwa of the 6th National Conference of the Indonesian Ulema Council Number: 7/Munas VI/Munas 2000 (Bachelor's thesis, Faculty of Sharia and Law, UIN Syarif Hidayatullah Jakarta).

Aresta, TDY Trade Unions as the Epicenter of Increasing Migrant Workers' Participation in Policy Formation. *National Civil Liberties 2023, 195*.

Aulia, E. (2024). Analysis of Article 56 in Law Number 27 of 2022 concerning Protection of Personal Data from the Perspective of Legal Certainty. *UNES Law Review, 7(1)*, 220-227.

Djafar, W., & Santoso, MJ (2019). *Personal Data Protection. Concepts, Instruments, and Principles*, Institute for the Study and Advocacy of Society (ELSAM), Jakarta.

Faizah, AF, Rosadi, SD, Pratama, GG, & Dharmawan, AF (2023). Strengthening personal data protection through supervisory authorities in Indonesia based on a comparison of Hong Kong and Singapore law. *Hakim: Journal of Law and Social Sciences, 1(3)*, 01-27.

Firmansyah, R. (2024). Reconstruction of Law Enforcement Regulations for the Placement of Illegal Workers Based on Justice Values (Doctoral dissertation, Sultan Agung Islamic University (Indonesia)).

Ikhsan, A. (2021). Efforts of the Indonesian Government in Handling the Problem of Indonesian Migrant Workers (PMI) Overstaying in Saudi Arabia for the Period 2014-2020 (Bachelor's thesis).

Kusnadi, SA (2021). Legal Protection of Personal Data as a Privacy Right. AL WASATH *Journal of Legal Science, 2(1),* 9-16.

Maulida, NA (2020). *Efforts of the Indonesian Government in Handling Underpayment Cases of Indonesian Migrant Workers in Hong Kong 2011-2017* (Bachelor's thesis, FISIP UIN Jakarta).

Mita Noveria, et al. (2021). *Protection of Indonesian Migrant Workers*. Indonesian Obor Library Foundation.

Nugroho, TWA, Indarti, ST, Nugraha, SS, Chanifah, MN, Revanzha, RR, Fathya, VN, ... & Jade, EYK (2025). *Post-Pandemic Indonesian Immigration and Borders: Challenges, Innovations, and Solutions*. Directorate General of Immigration.

Rosadi, SD (2023). *Discussion of the Personal Data Protection* Law (Law of the Republic of Indonesia No. 27 of 2022). Sinar Grafika.

SecretariatCabinet of the Republic of Indonesia. (2022, April 1). Indonesia and Malaysia Agree on Cooperation on Placement and Protection of Indonesian Migrant Workers in Malaysia.https://setkab.go.id/indonesia-and-malaysia-agree-on-work-to-place-and-protect-migrant-workers-in-malaysia/

Soemitro, DP, Wicaksono, MA, & Putri, NA (2023). Penal provisions in the personal data protection law: a comparative legal study between Indonesia and Singapore. *SIGn Jurnal Hukum, 5(1)*, 155-167.

Somantri, GR (2005). Understanding Qualitative Methods. *Makara Human Behavior Studies in Asia, 9(2),* 57-65.

Tantri, E. (2022). Legal protection for Indonesian workers abroad according to Law Number 18 of 2017. *Lex Privatum, 10(3)*.

The First Lady, H., Puspitawati, L., Putri, SO, Arifin, M., & Berkahi, AMA (2024). SOCIALIZATION OF WEST JAVA GASTRODIPLOMACY IN IMPROVING THE ECONOMY OF INDONESIAN MIGRANT WORKERS (PMI) IN MALAYSIA. *Journal of Creativity and Innovation (Kreanova Journal), 4(3),* 94-102.

Veranda, C., & Nusantara, MAZ (2024). Comparative Analysis of Personal Data Protection between Indonesia and Saudi Arabia. *PUSKAPSI Law Review, 4(2)*, 236-256.