Triyanti, Ninuk., I Gusti Ayu Ketut Rachmi Handayani, and Lego Karjoko. "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law," *Hasanuddin Law Review* 11 no. 1 (2025): 132-147. DOI: 10.20956/halrev.v11i1.6177

HasanuddinLawReview

Volume 11 Issue 1, April 2025
P-ISSN: 2442-9880, E-ISSN: 2442-9899

Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law

Ninuk Triyanti[1], I Gusti Ayu Ketut Rachmi Handayani[2], Lego Karjoko[3]

[1] *Faculty of Law, Universitas Sebelas Maret, Surakarta, Jawa Tengah, Indonesia. E-mail: ninuk.za@gmail.com*
[2] *Faculty of Law, Universitas Sebelas Maret, Surakarta, Jawa Tengah, Indonesia. E-mail: ayu_igk@staff.uns.ac.id*
[3] *Faculty of Law, Universitas Sebelas Maret, Surakarta, Jawa Tengah, Indonesia. E-mail: legokarjoko@staff.uns.ac.id*

Abstract: This study critically examines the existing legal framework for personal data protection within Indonesia's population administration system. Through a normative legal research approach, it identifies significant regulatory gaps that leave personal information vulnerable to misuse and breaches. The results show that the current legal policies remain insufficient, as numerous aspects of personal data protection have yet to be explicitly regulated in the Population Administration Law. Despite the enactment of a national personal data protection law, its effectiveness is undermined by the lack of comprehensive integration into the Population Administration Law. This research proposes reconstructing the legal framework to address essential aspects of data management—such as collection, utilization, safeguarding, exchange, and misuse prevention—while establishing clear access rights, prohibitions on unauthorized activities, and a structured system of proportional sanctions. By incorporating specialized legal provisions and aligning with international best practices, these reforms would strengthen Indonesia's data protection framework, enhance public trust, and reinforce the government's role in safeguarding citizens' personal information.

Keywords: Cybersecurity; Data Misuse; Digital Governance; Personal Data Protection; Privacy Rights

1. Introduction

The 1945 Constitution of the Republic of Indonesia guarantees the protection of all citizens, ensuring personal security and legal recognition. These constitutional provisions affirm every individual's right to legal certainty, equal treatment under the law, personal safety, and recognition as a legal entity. To fulfill these rights, a well-structured, accurate, and comprehensive civil registration system and personal data protection framework are essential. Since the enactment of the Population Administration Law in 2006—later revised in 2013—Indonesia has made efforts to improve population data management.

The Population Administration Law not only secures individuals' civil rights but also promotes orderly administration by developing a national population database containing accurate demographic details. This data is utilized for development planning and public services.[1] However, storing and utilizing population data comes with risks,

[1] Purtova, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.

particularly concerning data breaches and misuse. Several high-profile data leaks, including the 2021 e-HAC application breach, the sale of BPJS participant data in 2022, and the exposure of voter data by the General Election Commission, highlight the urgency of strengthening data protection measures.[2]

A report by Surfshark, a Netherlands-based VPN service, placed Indonesia among the top 10 countries for the highest number of data breaches in the first quarter of 2022, with 429,860 personal data records exposed online—far surpassing earlier figures from the CTI BSSN in 2021. These breaches highlight the government's weak role in safeguarding personal data, despite existing regulations under the 2008 Electronic Information and Transactions Law (ITE), which lacked specific provisions for personal data protection until the enactment of the Personal Data Protection Law in 2022.[3]

In the second quarter of 2022, approximately 1.04 million personal account data in Indonesia was hacked. This figure represents a 143% increase compared to the second quarter of 2021. As a result of the numerous data hacking incidents, Indonesia ranks third among countries with the highest data breach rates in the world. This leak of personal data not only negatively impacts individuals, such as identity theft for fraud or bank account breaches, but also affects corporations, leading to a decline in company reputation, significant recovery costs, and fines in accordance with applicable regulations.[4] Other negative impacts include a decrease in public trust, threats to individual privacy, disruptions to economic activities and development, and a decline in foreign investment interest.[5] The misuse of personal data clearly harms individuals and constitutes a violation of human rights. Therefore, many countries, including Indonesia.

The issue of personal data protection in population administration is critical due to its direct impact on national security, governance integrity, and citizens' fundamental rights. The increasing digitalization of public services, combined with weak enforcement mechanisms, has left personal data vulnerable to cyber threats, identity theft, and unauthorized use.[6] The absence of a comprehensive legal framework that explicitly regulates the collection, storage, processing, and exchange of personal data in population administration exacerbates these risks. Without immediate intervention, the growing

[2] KOMPAS.com. "Kilas Balik Lima Kasus Kebocoran Data Pribadi di Indonesia." KOMPAS, September 6, 2022. https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-?page=all&utm_source. Accessed 6 September 2024.

[3] Ramadhan, Kiki Rezki, and Chandra Wijaya. "The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia." *Technium Soc. Sci. J.* 36 (2022): 18-28.

[4] Wibowo, Ari, Widya Alawiyah, and Azriadi. "The importance of personal data protection in Indonesia's economic development." *Cogent Social Sciences* 10, no. 1 (2024): 1-20

[5] Muin, Indriani. "Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia." *Journal Law and Justice* 1, no. 2 (2023), 39.

[6] BBC News. "Indonesia's Data Protection Challenges." BBC Indonesia, July 18, 2023. https://www.bbc.com/indonesia/articles/c51v25916zlo?utm_source, Accessed 18 July 2024.

reliance on digital identity systems, such as the Digital Population Identity (IKD), may expose citizens to even greater privacy threats.

Furthermore, the lack of strict legal provisions creates a regulatory gap that allows both government institutions and private entities to exploit population data without adequate oversight. Many cases of data breaches stem from internal weaknesses, including poor data management practices, lack of security standards, and insufficient legal accountability for data handlers. The absence of explicit penalties for unauthorized access, misuse, or failure to secure population data has made it difficult to hold perpetrators accountable. This condition not only endangers individual privacy but also erodes public trust in the government's ability to protect its citizens' personal information.

Addressing these concerns requires a robust legal framework that aligns with international best practices, such as the General Data Protection Regulation (GDPR) and the ASEAN Framework on Personal Data Protection. Many countries have adopted stringent laws that regulate data security, privacy rights, and institutional accountability to prevent misuse. In contrast, Indonesia's existing legal structure remains fragmented, with overlapping regulations that lack enforcement power. Thus, this study aims to evaluate and propose legal reconstructions for personal data protection within the Population Administration Law to ensure comprehensive safeguards against unauthorized access, misuse, and data breaches. Strengthening these regulations is imperative to protect Indonesian citizens from digital vulnerabilities while upholding their constitutional rights.

2. Method

This research is a normative legal study using a qualitative research design through comprehensive literature review.[7] The approach employed involves analyzing various legal sources, scientific literature, journals, and relevant materials related to personal data protection. The main legal framework in this study is the Population Administration Law, which serves as a foundation for understanding the legal basis for personal data protection in the administration of population affairs. This research examines the extent to which the Population Administration Law can provide protection for the personal data of residents as part of the protection of human rights guaranteed in the 1945 Constitution. The findings of this study aim to reconstruct the legal regulations on personal data protection within the Population Administration Law and provide policy recommendations to optimize personal data protection in the administration of population affairs in Indonesia.

[7] Irwansyah. (2021) *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel (Edisi Revisi).* Revised edition. Yogyakarta: Mirra Buana Media, p. 162

3. The Concept of Personal Data in the Population Administration Law

The concept of personal data in the Population Administration Law refers to specific individual data elements that are part of population data, which are stored, maintained, and safeguarded for accuracy and confidentiality. This includes three elements: biometric data (fingerprints, iris scans, and signatures), information on physical and/or mental disabilities, and other data elements that may be considered a person's shame. Biometric data is data that includes the distinctive characteristics of its owner, both physical and non-physical,[8] which have unique characteristics, making them difficult to forge. It is this uniqueness that makes biometric data widely used in the fields of security and authentication.[9]

The Population Administration Law defines personal data as specific individual data elements stored, maintained, and protected for accuracy and confidentiality. These include biometric data, information on physical and/or mental disabilities, and other sensitive elements that may cause stigma. Biometric data, such as fingerprints, iris scans, and signatures, are particularly crucial due to their unique and irreplaceable characteristics, making them a key component in security and authentication systems. However, the potential risks associated with the misuse or leakage of such data necessitate robust legal protections. If not properly safeguarded, personal data misuse can lead to violations of human rights, particularly in terms of personal security, dignity, and legal recognition.

Considering that biometric data is very vital information, it must be thoroughly guaranteed for its security.[10] The elements of personal data of residents related to information about physical and/or mental disabilities, as well as other data elements that constitute a person's shame, must be specially protected because they are related to an individual's honor and dignity. If not protected and misused by irresponsible parties, this can cause suffering and loss for the individuals concerned, as it injures their self-respect and dignity. This clearly violates human rights, particularly Article 28 G paragraph (1), which essentially states that *"everyone has the right to personal protection, honor, and dignity."*

The principle of legitimate interest in the processing of personal data emphasizes that the collection and use of data must have a clear legal basis and legitimate purpose. In the context of population administration, this principle is relevant to ensure that the personal

[8] Palimbani, Muhammad Adin. "Polemik Keamanan Data Biometrik." *Retrieved from Gama Cendekia UGM: https://gc.ukm.ugm.ac.id/2020/08/polemik-keamanan-data-biometrik* (2020).

[9] Rizki, Miyuki Fattah, and Abdul Salam. "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris)." *Lex Patrimonium* 2, no. 2 (2023): 9.

[10] Sembiring, Patricia Edina, Ahmad M. Ramli, and Laina Rafianti. "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik." *Veritas et Justitia* 10, no. 1 (2024): 127-152.

data of residents is only used for the purposes that have been specified, such as data verification needs or public services, without misuse by unauthorized parties. The right to privacy regarding personal data includes the right of each individual to know what happens to their personal data, who accesses it, for what purposes the data is used, and how the data is processed and stored. Furthermore, this principle also involves the right to give consent for the use of personal data, as well as the right to request the deletion of data (right to be forgotten) or correction if the data is inaccurate.[11]

The right to be forgotten is a right closely related to privacy rights in the use of information technology. In the context of Indonesian law, this right has been regulated in Article 26 paragraph (3) of the revised Electronic Information and Transactions Law (UU ITE) and Article 43 paragraph (1) of the Personal Data Protection Law (UU PDP). This right provides individuals the opportunity to request the deletion of personal data that is no longer relevant or obtained unlawfully. However, the implementation of this right faces significant challenges, particularly in balancing individual privacy rights with the public's right to know information. Additionally, data deletion is often hindered by the cross-border nature of the internet, where data that has been deleted in one country can still be accessed in another.[12]

A key principle in personal data protection is legitimate interest, which ensures that data collection and usage have a clear legal basis and serve a legitimate purpose. In population administration, this principle is particularly relevant to ensure that data is used only for specific purposes, such as verification and public services, without unauthorized exploitation. Additionally, the right to privacy over personal data grants individuals control over their data, including knowledge of how it is accessed, used, and stored.[13] This principle aligns with the right to be forgotten, a critical aspect of modern data protection laws that allows individuals to request the deletion of outdated or unlawfully obtained data. However, the enforcement of this right in Indonesia faces challenges, particularly in the global digital landscape where deleted data may still be accessible in other jurisdictions.

Indonesia has attempted to address these concerns through Law No. 27 of 2022 on Personal Data Protection (PDP Law), which marks a significant step in regulating personal data at the national level. This law categorizes personal data into general and specific types, including biometric, health, and financial data, aligning with international data protection frameworks such as the General Data Protection Regulation (GDPR) and the

[11] Roos, Anneliese. "Core principles of data protection law." *Comparative and International Law Journal of Southern Africa* 39, no. 1 (2006): 103-130.

[12] Nopit Ernasari, "Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana di Era Digital Ditinjau dari Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia," *Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan* 15, no. 2, (2024): 163-174

[13] Syailendra, Moody Rizqy, Gunardi Lie, and Amad Sudiro. "Personal Data Protection Law in Indonesia: Challenges and Opportunities." *Indonesia Law Review,* 14 (2024): 175.

ASEAN Framework on Personal Data Protection. However, despite this legal milestone, challenges remain in its implementation, particularly in relation to its integration with the Population Administration Law. The fact that population data is managed by the Ministry of Home Affairs and can be accessed by various public institutions increases the potential for misuse, unauthorized access, and data leaks. Without clear and explicit regulations within the Population Administration Law, the effectiveness of the PDP Law remains limited.

Considering that biometric data and other personal data elements related to information about physical and/or mental disabilities, as well as other data elements that may be considered a stigma for an individual, are very vital, and that this personal data has been stored in the national population database managed by the Ministry of Home Affairs, which can be accessed and utilized by public institutions in accordance with Article 79 paragraph (2) of Law Number 24 of 2013.[14] The storage and utilization of personal data have the potential for misuse, manipulation, data leaks, and other illegal actions, making the regulation of personal data protection in the Population Administration Law a very central and strategic issue.

Comparative analysis with South Korea's Personal Information Protection Act (PIPA) highlights the need for stronger technical regulations and enforcement mechanisms in Indonesia. PIPA enforces explicit consent requirements, restrictions on data usage, and rights for individuals to access and control their data. Indonesia's regulatory framework still lacks these crucial elements, leading to frequent large-scale data breaches that compromise citizens' privacy and trust in government institutions. The Indonesian government's introduction of Digital Population Identity (IKD) as an alternative to traditional ID cards represents a positive step towards digital transformation but also introduces new vulnerabilities.[15] The success of IKD will depend on public awareness, cybersecurity infrastructure, and digital literacy initiatives to ensure citizens can safely adopt and use the technology.

From a criminal law perspective, personal data breaches should be recognized as serious legal violations. Unlawful data misuse can result in financial fraud, identity theft, reputational harm, and violations of fundamental privacy rights. The PDP Law outlines penalties for unauthorized access, misuse, and disclosure of personal data, but enforcement remains weak due to fragmented legal frameworks and limited institutional oversight. Strengthening enforcement mechanisms and ensuring clear accountability for data handlers—both in public and private sectors—are critical for effective personal data protection.

[14] Article 79 paragraph (2) of Law Number 24 of 2013 emphasizes that "the Minister of Home Affairs is responsible for providing access to population data to provincial officers, implementing agency officials, and users."

[15] 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 (2024): 1-20.

One concrete step that the Indonesian government has taken to protect personal data is the implementation of Digital Population Identity (IKD). IKD is an Android-based application that allows residents to have a digital identity as an alternative to physical electronic ID cards (KTP). This application uses biometric data authentication, verification codes, and QR codes to ensure the security of personal data. However, the implementation of IKD still faces various challenges, such as a lack of socialization to the public, limited internet access in some areas, and low levels of digital literacy among the population. Therefore, the success of IKD implementation requires active participation from both the government and the community, including through enhanced socialization and strengthening of information technology infrastructure.[16]

The importance of personal data protection can also be viewed from a criminal law perspective, where the unlawful misuse of someone's personal data can violate fundamental privacy rights. This privacy right encompasses two main aspects: privacy concerning a person's persona and privacy regarding a person's data. In practice, violations of this privacy often occur through the dissemination of embarrassing personal facts, the use of data for commercial purposes without consent, or the disclosure of personal information that should remain confidential. Therefore, the enforcement of criminal law becomes crucial to provide robust legal protection against such actions, as stipulated in Article 65 of the Personal Data Protection Law.[17]

Given the persistent issues in personal data security and administration, legal reconstruction of the Population Administration Law is necessary to ensure comprehensive data protection. The current framework lacks explicit procedural safeguards, enforcement mechanisms, and clear sanctioning provisions, making it ineffective in preventing data misuse. Integrating Articles 65–69 of the PDP Law into the Population Administration Law would strengthen its legal authority and create a more unified and enforceable legal structure.

Additionally, implementing international best practices, such as those in the GDPR and PIPA, would enhance Indonesia’s approach to personal data security. These regulations emphasize explicit consent, data minimization, and independent oversight, which could be key elements in strengthening the Indonesian data protection framework. The government must also establish an independent data protection authority to oversee compliance, investigate breaches, and impose sanctions on violators.

Furthermore, the rapid digital transformation in population administration necessitates increased investment in cybersecurity, data encryption technologies, and digital literacy programs. Public institutions must be held accountable for securing personal data, and

[16] Permadi, Ikhsan Bagus, and Ali Rokhman. "Implementasi Identitas Kependudukan Digital Dalam Upaya Pengamanan Data pribadi." *JOPPAS: Journal of Public Policy and Administration Silampari* 4, no. 2 (2023): 80-88.

[17] Watkat, Fransiscus Xaverius, Muhammad Toha Ingratubun, and Adelia Apriyanti. "Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana Di Indonesia." *Jurnal Hukum Ius Publicum* 5, no. 1 (2024): 153-175.

clear guidelines should be established for data-sharing agreements between government agencies and third parties. By addressing these challenges through stronger legal frameworks, enhanced enforcement, and public awareness initiatives, Indonesia can significantly improve its population data governance while upholding citizens' fundamental rights to privacy and security.

4. Strengthening Legal Provisions for Personal Data Protection: Towards Comprehensive Personal Data Protection in Indonesia

The current framework for personal data protection under the Population Administration Law remains inadequate, as it fails to comprehensively regulate crucial aspects such as enforcement mechanisms, rights of data subjects, and security standards for data processing. While Law No. 27 of 2022 on Personal Data Protection (PDP Law) provides a more detailed legal structure, its implementation within the population administration system remains weak due to the lack of integration with the Population Administration Law. Without a synchronized approach, legal loopholes continue to exist, allowing unauthorized access, misuse, and data leaks.

One major weakness in Indonesia's current legal framework is the lack of an independent oversight body responsible for monitoring data protection compliance. Many countries with strong data protection laws, such as South Korea (PIPA) and the European Union (GDPR), have established independent data protection authorities. Indonesia must create an independent supervisory agency separate from government institutions involved in population data management. This agency should have the authority to audit compliance, investigate breaches, impose sanctions, and enforce data security policies. Without independent oversight, personal data stored in national databases remains vulnerable to unauthorized use by both public and private entities.[18]

The protection of personal data in this research focuses on legal protection as one of the mechanisms for safeguarding personal data. According to Muchsin, legal protection is an effort to protect every individual through enforceable regulations that come with sanctions, and one form of this is preventive legal protection, which involves prevention through the creation of laws and regulations.[19] The author uses preventive legal protection to analyze the legal protection of personal data in the administration of population affairs.

[18] Adhikari, Kamala, Scott B. Patten, Alka B. Patel, Shahirose Premji, Suzanne Tough, Nicole Letourneau, Gerald Giesbrecht, and Amy Metcalfe. "Data harmonization and data pooling from cohort studies: a practical approach for data management." *International journal of population data science*6, no. 1 (2021): 1680.

[19] Muchsin. "Perlindungan dan Kepastian Hukum bagi Investor di Indonesia." *Universitas Sebelas Maret* (2003). Universitas Sebelas Maret, Surakarta, p. 20.

In the Population Administration Law, there are 5 (five) articles that regulate the protection of personal data, namely:

1. Personal data is a part of individual data that is stored, maintained, and kept accurate, as well as protected for its confidentiality.
2. Every resident has the right to obtain protection of personal data.
3. Personal data that must be protected includes information about physical and/or mental disabilities, iris patterns, fingerprints, signatures, and other data elements that may be considered sensitive or stigmatizing.[20]
4. The state is required to store and protect the personal data of its residents. The Central Government, provincial governments, district/city governments, and the population and civil registration offices of districts/cities must ensure its accuracy and protect its confidentiality.
5. Provincial and district/city officials are prohibited from disseminating personal data that is not within their authority. If violated, the penalty is a maximum prison sentence of 2 (two) years and/or a fine of up to Rp25,000,000.00 (twenty-five million rupiah).[21]

Considering the limited regulations on personal data protection and that personal data is part of individual data which constitutes an element of population data, the policy for the protection of population data in the Population Administration Law can be applied to the protection of personal data, which is regulated in several articles, namely:

1. The population and civil registration office of the district/city is obligated to ensure the confidentiality and security of data regarding population events and significant occurrences experienced by residents.
2. The state is required to store and protect the confidentiality of personal data and population documents.
3. Provincial and district/city officials and users are prohibited from disseminating population data beyond their authority. If violated, it is punishable by a maximum prison sentence of 2 (two) years and/or a fine of up to Rp25,000,000.00 (twenty-five million rupiah).[22]
4. Everyone is prohibited from ordering and/or facilitating and/or manipulating population data and/or elements of population data. If violated, it is punishable by imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp75,000,000.00 (seventy-five million rupiah).[23]
5. The utilization of population data must obtain permission from the Central Government, provincial government, and district/city government.[24]

[20] Article 84 paragraph (1) of Law Number 24 of 2013.
[21] Article 95A of Law Number 24 of 2013.
[22] Article 95A of Law Number 24 of 2013.
[23] Article 94 of Law Number 24 of 2013.
[24] Article 83 paragraph (2) of Law Number 23 of 2006.

An analysis of the regulations concerning personal data and population data protection within the Population Administration Law reveals several unaddressed areas. These gaps could obstruct efforts to safeguard personal and population data effectively within the framework of population administration.

First, the Population Administration Law lacks clearly defined principles, standards, procedures, and mechanisms for protecting both personal and population data. This gap arises from the law's primary focus on managing population affairs rather than safeguarding personal information, leaving personal data vulnerable to misuse due to the absence of comprehensive protection guidelines.

Second, the law does not provide detailed prohibitions against illegal actions that harm data owners, such as the falsification of population data.[25] While it addresses data manipulation, legal literature distinguishes manipulation from falsification—manipulation involves altering or rearranging data for specific purposes without fabricating new data, whereas falsification entails creating false data or forging information for unlawful purposes, such as producing fake identification cards.

Third, not all violations related to personal and population data protection are accompanied by clear sanctions. For instance, there are no penalties for provincial civil registry officers who misuse data beyond their authority. Legal theorists like Hans Kelsen, John Austin, and Rudolf von Jhering emphasize the importance of sanctions in ensuring compliance with legal norms.[26] Without sanctions, these laws risk losing their effectiveness and fail to provide legal certainty or deter violations.

Fourth, the regulations concerning data security measures remain limited, lacking specific technical guidelines to prevent data leaks, manipulation, or illegal activities. This reflects broader weaknesses in the data protection system, as enforcement against misuse tends to be inconsistent, allowing repeated violations to occur.

Fifth, the Population Administration Law does not explicitly recognize the rights of personal and population data owners. Individuals are not granted rights to access, correct, delete, or refuse the use of their personal data, thereby limiting their control over how their information is managed and utilized.

Sixth, there is no mechanism for independent oversight in the management of population data. Oversight remains entirely under the control of the Directorate General of Population and Civil Registration, without an independent authority to supervise data protection.[27] This weakens both transparency and accountability, making enforcement

[25] Setiawan, Joko Tri. "Hukum Tindak Pidana Pemalsuan Dokumen Pencatatan Sipil UKUM (Studi Kasus Putusan Nomor 1251/Pid. B/2020/PN Jkt. Utr)." *Jurnal Bevinding* 1, no. 03 (2023): 44-53.

[26] Murti, Aditya Khrisna. "Penerapan Regulasi Alokasi Pendapatan Pajak Air Tanah Dari Usaha Hotel Kota Yogyakarta Guna Konservasi Air Tanah untuk Pemenuhan Hak Atas Air." PhD diss., Universitas Islam Indonesia, 2024, p. 66.

[27] Kurdi, Kurdi, and Joko Cahyono. "Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (2024): 330-339.

under the Personal Data Protection Law (PDP Law) challenging due to the absence of an autonomous supervisory body.

Seventh, the Population Administration Law has yet to establish clear procedures for data transfers between agencies or third parties. This lack of detailed regulation means that data-sharing arrangements between government institutions and private entities are often carried out without adequate protection, despite the Ministry of Home Affairs holding the authority to grant access through formal agreements.

Last but not least, the law has not yet incorporated internationally recognized data protection principles, such as those outlined in the General Data Protection Regulation (GDPR). Key principles like legality, transparency, accountability, and purpose limitation are absent from the framework, increasing the risk that population data could be used for unintended purposes without the explicit consent of the data owner.

Since 2022, Indonesia has had a law specifically regulating the protection of personal data, namely Law Number 27 of 2022 concerning Personal Data Protection. Article 1, paragraph 1 of Law Number 27 of 2022 states that personal data is data about an individual that is identified or can be identified either alone or in combination with other information, whether directly or indirectly, through electronic or non-electronic systems. Furthermore, Article 4, paragraphs (1), (2), (160), and (3) emphasize that personal data consists of specific personal data and general personal data. Specific personal data includes health data and information, biometric data, genetic data, criminal records, children's data, personal identification data, and/or other data in accordance with the provisions of laws and regulations.

Meanwhile, general personal data includes: Full name, gender, religion, marital status, and/or personal data that can be combined to identify an individual.[28] The definition of personal data in the Population Administration Law can be categorized as a specific form of personal data, namely biometric data and personal information. To strengthen the protection of personal data in the administration of population affairs, the provisions in Law Number 27 of 2022, particularly those related to prohibitions not yet regulated in the Population Administration Law, can be applied as a mechanism for protecting personal data in the administration of population affairs. Some of these articles are:

a. Article 65 (1) emphasizes the prohibition for any person to unlawfully obtain or collect personal data that does not belong to them with the intent to benefit themselves or others, which may result in harm to the owner of the personal data. Paragraph (2) regulates the prohibition against unlawfully disclosing personal data that does not belong to them, while paragraph (3) regulates the unlawful use of personal data that does not belong to them.

[28] Article 4 paragraph (3) of Law Number 27 of 2022.

b. Article 66 states the prohibition for any person to create false personal data or to falsify personal data with the intent to benefit oneself or others, which may result in harm to others.

c. Article 67 regulates the threat of sanctions for violations of Article 65 paragraph (1) with a maximum prison sentence of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah). The threat of sanctions for violations of Article 65 paragraph (2) is punishable by a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiah). The threat of sanctions for violations of Article 65 paragraph (3) carries a maximum prison sentence of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah).

d. Article 68 emphasizes the threat of sanctions for violations of Article 66, with a maximum prison sentence of 6 (six) years and/or a maximum fine of Rp 6,000,000,000.00 (six billion rupiah).

e. Article 69 states that in addition to being subject to criminal penalties as regulated in Articles 67 and 68, offenders may also be imposed with additional penalties in the form of confiscation of profits and/or assets obtained from the criminal act, as well as being required to pay compensation for damages.

Considering the inadequacy and lack of clarity in the regulations regarding the protection of personal data and population data in the Population Administration Law, it is based on the principle of *lex specialis derogate lex generalis*.[29] The provisions of Articles 65 to 69 of Law Number 27 of 2022 can be applied to optimize the protection of personal data in the administration of population affairs.

In the context of legal reconstruction, Law Number 27 of 2022 brings significant changes by adopting internationally recognized principles of personal data protection, as outlined in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. These principles include legality, transparency, accountability, and data usage limitations in accordance with established purposes. Furthermore, Law Number 27 of 2022 also introduces new mechanisms such as the appointment of a data protection officer, regulations for cross-border data transfers that require equivalent protection in the receiving country, as well as stricter administrative and criminal sanctions.

With the enactment of Law Number 27 of 2022, Indonesia now has a more comprehensive legal framework for protecting personal data, which can be integrated into the Population Administration Law to address shortcomings in the regulation of principles, standards, and mechanisms for personal data protection. This is crucial to

[29] Rosadi, Otong. "Hukum Kodrat, Pancasila dan asas hukum dalam pembentukan hukum di Indonesia." *Jurnal Dinamika Hukum* 10, no. 3 (2010): 277-284.

ensure that the management of population data not only meets administrative needs but also optimally protects individual privacy rights.[30]

In the context of legal reconstruction, internationally recognized principles of personal data protection, such as those found in the General Data Protection Regulation (GDPR) and the ASEAN Framework on Personal Data Protection, can serve as important references to strengthen regulations within the Population Administration Law. These principles include legality in data processing, transparency, accountability of data managers, and restrictions on data use in accordance with established purposes. Additionally, more detailed regulations regarding the rights of data owners, such as the right to access, correct, and delete personal data, also need to be adopted to ensure more comprehensive protection. By integrating these principles, population data management not only meets administrative needs but also optimally protects individual privacy rights.[31]

The principle of "legitimate interest" in the processing of personal data is one of the important principles recognized internationally, as outlined in the General Data Protection Regulation (GDPR). This principle allows for the processing of personal data to be carried out for legitimate interests, both by data controllers and third parties, while still considering the balance between the interests of the data controller and the fundamental rights of data subjects. However, in the context of personal data protection law in Indonesia, this principle is still regulated in a general manner without clear criteria, which could potentially lead to abuse of power. To address this, the implementation of a "balancing test" is necessary to measure the balance between the interests of the data controller and the protection of the rights of data subjects. This step is crucial to ensure that the processing of personal data not only meets commercial or administrative needs but also optimally protects individual privacy rights.

Although Law Number 27 of 2022 can be applied in cases of illegal actions related to personal data that are not regulated under the Population Administration Law, according to Indrati, the law can be effectively implemented if it contains comprehensive and fundamental material, without relying too much on other regulations.[32] This means that the Population Administration Law has not been effective in providing protection for residents' personal data because it has not comprehensively regulated personal data. Therefore, according to Asshiddiqie, it must be ensured that the regulations in the law are complete by integrating the substance of one law with the substance of various related laws.[33] This means that the Population Administration Law can adopt provisions

[30] Yuniarti, Siti, Ahmad M. Ramli, Sinta Dewi Rosadi, and Danrivanto Budhijanto. "The New Chapter Of Indonesia's Data Protection On Digital Economy Perspective." *Journal of Southwest Jiaotong University* 58, no. 3 (2023): 109-117

[31] Shahrullah, et al., Loc.Cit.

[32] Indrati, Maria Farida. 2007, *Ilmu Perundang-Undangan, Proses dan Teknik Pembentukannya*, Jakarta: Kanisius. p. 43.

[33] Asshiddiqie, Jimly, 2021, *Teori Hierarki Norma Hukum*. Jakarta: Konstitusi Press (Konpress), p. 49.

from Law Number 27 of 2022 that are relevant to the protection of personal data in the implementation of population administration.

The reconstruction of the Population Administration Law is not merely an option—it is a necessity in the face of increasing digitalization, cybersecurity threats, and global data protection standards. The integration of Law No. 27 of 2022, coupled with international best practices from GDPR, ASEAN, and PIPA, would strengthen Indonesia's data governance framework, ensuring legal certainty, data security, and respect for individual privacy rights. Without immediate legal reforms, Indonesia risks continued large-scale data breaches, loss of public trust, and vulnerability to cyber threats, undermining national security and economic stability. The government must take proactive steps to enact comprehensive reforms, ensuring that personal data protection is not just a legal formality but an enforceable right for every Indonesian citizen.

5. Conclusion

The current legal provisions for personal data protection in Indonesia's population administration system remain fragmented and insufficient to prevent data misuse and breaches. While the Personal Data Protection Law offers a more robust legal structure, its weak integration with the Population Administration Law results in legal loopholes that compromise data security and citizens' privacy rights. To address these shortcomings, a comprehensive legal reconstruction of the Population Administration Law is necessary. This reform should establish clear standards for data collection, storage, usage, and protection, alongside detailed enforcement mechanisms and structured sanctions for violations. Additionally, integrating international best practices—such as those outlined in the General Data Protection Regulation and ASEAN's data protection framework—would ensure stronger legal safeguards and align Indonesia's regulations with global standards. An independent data protection authority should also be established to oversee compliance, enforce legal provisions, and foster accountability among public and private data handlers. Without these critical reforms, the risk of large-scale data breaches and diminishing public trust will continue to undermine national security, governance integrity, and Indonesia's digital transformation efforts.

References

Adhikari, Kamala, Scott B. Patten, Alka B. Patel, Shahirose Premji, Suzanne Tough, Nicole Letourneau, Gerald Giesbrecht, and Amy Metcalfe. "Data Harmonization and Data Pooling from Cohort Studies: A Practical Approach for Data Management." *International Journal of Population Data Science* 6, no. 1 (2021): 1680.

Asshiddiqie, Jimly. *Teori Hierarki Norma Hukum.* Jakarta: Konstitusi Press (Konpress), 2021.

BBC News. "Indonesia’s Data Protection Challenges." *BBC Indonesia*, July 18, 2023. https://www.bbc.com/indonesia/articles/c51v25916zlo?utm_source. Accessed July 18, 2024.

Indrati, Maria Farida. *Ilmu Perundang-Undangan, Proses dan Teknik Pembentukannya.* Jakarta: Kanisius, 2007.

Irwansyah. *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel* (Edisi Revisi). Yogyakarta: Mirra Buana Media, 2021.

KOMPAS.com. "Kilas Balik Lima Kasus Kebocoran Data Pribadi di Indonesia." *KOMPAS*, September 6, 2022. https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-?page=all&utm_source. Accessed September 6, 2024.

Kurdi, Kurdi, and Joko Cahyono. "Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (2024): 330-339.

Muchsin. *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia.* Surakarta: Universitas Sebelas Maret, 2003.

Muin, Indriani. "Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia." *Journal Law and Justice* 1, no. 2 (2023): 39.

Murti, Aditya Khrisna. "Penerapan Regulasi Alokasi Pendapatan Pajak Air Tanah Dari Usaha Hotel Kota Yogyakarta Guna Konservasi Air Tanah untuk Pemenuhan Hak Atas Air." PhD diss., Universitas Islam Indonesia, 2024.

Nopit Ernasari. "Perlindungan Data Pribadi Dalam Penegakan Hukum Pidana di Era Digital Ditinjau dari Perspektif Implementasi Prinsip Right to be Forgotten di Indonesia." *Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan* 15, no. 2 (2024): 163-174.

Permadi, Ikhsan Bagus, and Ali Rokhman. "Implementasi Identitas Kependudukan Digital Dalam Upaya Pengamanan Data Pribadi." *JOPPAS: Journal of Public Policy and Administration Silampari* 4, no. 2 (2023): 80-88.

Purtova, Nadezhda. "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.

Ramadhan, Kiki Rezki, and Chandra Wijaya. "The Challenges of Personal Data Protection Policy in Indonesia: Lesson Learned from the European Union, Singapore, and Malaysia." *Technium Social Sciences Journal* 36 (2022): 18-28.

Rizki, Miyuki Fattah, and Abdul Salam. "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris)." *Lex Patrimonium* 2, no. 2 (2023): 9.

Roos, Anneliese. "Core Principles of Data Protection Law." *Comparative and International Law Journal of Southern Africa* 39, no. 1 (2006): 103-130.

Rosadi, Otong. "Hukum Kodrat, Pancasila dan Asas Hukum dalam Pembentukan Hukum di Indonesia." *Jurnal Dinamika Hukum* 10, no. 3 (2010): 277-284.

Sembiring, Patricia Edina, Ahmad M. Ramli, and Laina Rafianti. "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik." *Veritas et Justitia* 10, no. 1 (2024): 127-152.

Setiawan, Joko Tri. "Hukum Tindak Pidana Pemalsuan Dokumen Pencatatan Sipil UKUM (Studi Kasus Putusan Nomor 1251/Pid. B/2020/PN Jkt. Utr)." *Jurnal Bevinding* 1, no. 3 (2023): 44-53.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024): 1-20.

Syailendra, Moody Rizqy, Gunardi Lie, and Ahmad Sudiro. "Personal Data Protection Law in Indonesia: Challenges and Opportunities." *Indonesia Law Review* 14 (2024): 175.

Watkat, Fransiscus Xaverius, Muhammad Toha Ingratubun, and Adelia Apriyanti. "Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana di Indonesia." *Jurnal Hukum Ius Publicum* 5, no. 1 (2024): 153-175.

Wibowo, Ari, Widya Alawiyah, and Azriadi. "The Importance of Personal Data Protection in Indonesia’s Economic Development." *Cogent Social Sciences* 10, no. 1 (2024): 1-20.

Yuniarti, Siti, Ahmad M. Ramli, Sinta Dewi Rosadi, and Danrivanto Budhijanto. "The New Chapter of Indonesia’s Data Protection on Digital Economy Perspective." *Journal of Southwest Jiaotong University* 58, no. 3 (2023): 109-117.

Conflict of Interest Statement: The author(s) declares that the research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest.

Hasanuddin Law Review (Hasanuddin Law Rev. – HALREV) is an open access and peer-reviewed journal published by Faculty of Law, Hasanuddin University, Indonesia.

Open Access