

Comparing Data Protection and Due Process Implementation in Indonesia

Arista Candra Irawati¹, Hendra Wijaya², Ade Pratama³

Universitas Ngudi Waluyo, Central java, Indonesia

*Correspondence e-mail: aristacandrairawati@unw.ac.id

Submission

2024-Jul-05

Review

2024-Dec-15

Accepted

2025-Feb-22

Publish

2025-Apr-12

Abstract

This study aims to analyze and examine legal issues related to personal data protection in Indonesia and Malaysia, as well as to assess the principle of due process of law and its implementation in ensuring legal certainty in personal data protection, particularly in Case No. 46/Pid.Sus/2023/PN.Slt. The research employs an empirical juridical method using statutory, conceptual, and case approaches. The data consist of primary, secondary, and tertiary sources. The findings indicate, first, that both Indonesia and Malaysia are committed to protecting personal data as part of human rights. Indonesia has enacted the Personal Data Protection Law (UU PDP) and its derivatives, while Malaysia has implemented the Personal Data Protection Act 2010. These frameworks demonstrate that both countries possess adequate legal structures to safeguard their citizens' privacy in the digital era. Second, the application of the due process of law principle in the context of personal data protection – as illustrated in Case No. 46/Pid.Sus/2023/PN.Slt – highlights the importance of transparent, fair, and equitable legal enforcement. The implementation of this principle provides legal certainty for individuals concerning the collection, processing, and protection of their personal data. Upholding due process of law also prevents abuse of authority by law enforcement and ensures that any action taken in handling personal data complies with lawful and accountable procedures.

Keywords: Legal Certainty; Criminal Act of SIM Card Registration; Due Process of Law

How to Cite: Arista Candra Irawati. et.al." Perbandingan Pengaturan Perlindungan Data Pribadi dan Implementasi Due Process of Law di Indonesia" *Jurnal Ilmiah Dunia Hukum*, 9 no. 2 (2025): 18-36. DOI : 10.35973/jidh.xxxxxx

1. Introduction

In the digital era, the advancement of information technology has significantly impacted the ways in which personal data is managed and protected.¹ Personal data, which fundamentally encompasses all information related to an individual, has become highly vulnerable to misuse, leakage, and violations of privacy rights.² Personal data can be understood as information that identifies an individual either directly or indirectly, whether stored in electronic or non-electronic systems. The term refers to data covering various aspects such as personal identity, address, identification numbers, and even biometric information. Juridically, personal data protection is a

¹ Refaldy Braif Carundeng² Anna S. Wahongan³ Presly Prayogo⁴, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diredas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik," *Lex Privatum* 10, no. 1 (2022).

² Hasbi Pratama Arya Agung, "Perlindungan Data Pribadi Dalam Proses Pengurusan Perizinan Perusahaan Berbasis Elektronik Online Single Submission (OSS)," *Jurnal Ilmiah Galuh Justisi* 9, no. 1 (2021), <https://doi.org/10.25157/justisi.v9i1.4862>.

fundamental human right guaranteed by the constitution and enforced through various applicable regulations.³

The legal issues arising from the increasing misuse of personal data primarily concern the suboptimal mechanisms for its protection.⁴ From a juridical perspective, although personal data protection is regulated under the Personal Data Protection Law (UU PDP) in Indonesia, challenges remain in ensuring its effective implementation—particularly in the public service and telecommunications sectors. One notable example is the misuse of personal data during the registration of prepaid telecommunication cards, where such data is utilized without the knowledge or consent of the individual concerned. This issue is further exacerbated by the frequent occurrence of data breaches, which not only harm the public but also erode trust in digital systems.⁵

On the empirical side, violations of personal data often go insufficiently addressed.⁶ For instance, the data breach involving Tokopedia users in 2020 illustrates a significant gap between existing regulations and their implementation in practice. Moreover, the widespread phenomenon of improperly conducted SIM card registrations serves as a concrete example of non-compliance with regulations, ultimately resulting in violations of individual rights. In this context, a comparative approach to personal data protection systems in other countries can offer valuable insights into the steps Indonesia needs to take to improve its data protection policies.⁷

Supporting data and evidence in this study aim to provide case-based analyses of personal data violations in Indonesia, underscoring the urgency of a more robust protection system. Notable examples include data leaks involving major marketplaces such as Bukalapak and Tokopedia, as well as reports from institutions like McKinsey, which reveal a high incidence of personal data breaches. This study also references a number of judicial decisions related to the misuse of personal data and highlights the ongoing challenges in implementing effective protection policies.

Several previous studies have addressed themes related to personal data protection. For instance, Hanifan Niffari's research titled "*Personal Data Protection as Part of Human Rights to Personal Security (A Comparative Review of Legislation in Other Countries)*"

³ Aditama Candra Kusuma and Ayu Diah Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI: Jurnal Hukum* 5, no. 1 (2022), <https://doi.org/10.36441/supremasi.v5i1.721>.

⁴ Abd. Rahman Saleh, "Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana," *HUKMY: Jurnal Hukum* 1, no. 1 (2021), <https://doi.org/10.35316/hukmy.2021.v1i1.91-108>.

⁵ John F. Mariani, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *The Encyclopedia of American Food and Drink* 3 (2020).

⁶ Gugum Gumilar et al., "Personal Data Protection Framework for Web Developers and API Providers under UU PDP," in *2023 International Conference on Informatics, Multimedia, Cyber and Information Systems, ICIMCIS 2023*, 2023, <https://doi.org/10.1109/ICIMCIS60089.2023.10349040>.

⁷ Maciej Serda et al., "Pengaruh Terpaan Berita Tentang Kebocoran Data Pengguna Tokopedia Dan Aktivitas Word of Mouth Terhadap Tingkat Kepercayaan Dalam Menggunakan Tokopedia," *Interaksi Online* 9, no. 2 (2021).

concludes that the urgency of regulating personal data protection through a separate legal framework—as mandated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia—has become increasingly evident in light of the growing misuse of personal data in the digital age.⁸

Another study by Moses Blessing, titled "*Comparative Analysis of Data Protection Laws: Learning from Global Best Practices*," emphasizes the importance of general principles such as consent, data minimization, and user rights. The study also identifies key challenges in law enforcement and compliance, and highlights the need for international cooperation and legal harmonization to enhance data security and build consumer trust.⁹

Lastly, an international study by Kurdi titled "Personal Data Protection in the Digital Era Based on Law No. 27 of 2022," points out that although Law No. 27 of 2022 on Personal Data Protection (UU PDP) provides both preventive and repressive measures for data protection, its implementation still faces significant challenges, particularly in law enforcement. The absence of a dedicated supervisory authority to monitor and enforce sanctions is identified as a major obstacle. Consequently, the study concludes that establishing an independent oversight authority is essential to strengthen the legal protection of personal data and to foster public trust in the digital era.¹⁰

Based on previous research data, it is evident that the author's study shares a fundamental similarity with earlier studies, namely the emphasis on personal data protection as an integral part of human rights that must be guaranteed by the state. The main focus lies in the urgency of legal regulation and protection of personal data in the digital era. However, this study distinguishes itself by conducting a juridical comparison between Indonesia and Malaysia, specifically between Indonesia's Personal Data Protection Law of 2022 (UU PDP) and Malaysia's Personal Data Protection Act of 2010 (PDPA). Furthermore, this research incorporates a concrete case study—Case No. 46/Pid.Sus/2023/PN.Slt.—as an analytical tool to examine the application of the principle of due process of law. Unlike prior research, which remains largely conceptual or normative, this study offers an empirical perspective by analyzing a specific legal case.

The objective of this study is to analyze the protection of personal data in Indonesia and Malaysia, as well as the application of due process of law in the context of personal

⁸ Hanifan Niffari, "PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain," *Jurnal Hukum Dan Bisnis (Selisik)* 6, no. 1 (2020), <https://doi.org/10.35814/selisik.v6i1.1699>.

⁹ Moses Blessing, "Comparative Analysis of Data Protection Laws : Learning from Global Best Comparative Analysis of Data Protection Laws : Learning from Global Best Practices Author : Moses Blessing Date : 5 Th Oct , 2024 Abstract :," no. October (2024).

¹⁰ Joko Cahyono, "JUNCTO: Jurnal Ilmiah Hukum Perlindungan Data Pribadi Di Era Digital Berdasarkan" 6, no. 2 (2024): 330–39, <https://doi.org/10.31289/juncto.v6i2.5443>.

data violations related to the registration of prepaid SIM cards, using Case No. 46/Pid.Sus/2023/PN.Slt. as a case study. Additionally, the research aims to explore how existing legal provisions can be optimized to ensure stronger protection of individual rights in the current digital landscape.

2. Research Method

This research adopts an empirical juridical method employing a statute approach, a conceptual approach, and a case approach. The primary data consists of interviews conducted with relevant stakeholders, including law enforcement officials, personal data managers, and judicial authorities involved in Case No. 46/Pid.Sus/2023/PN.Slt. The secondary data includes statutory regulations, jurisprudence, legal literature, scholarly journals, and other official documents relevant to the topic of personal data protection in Indonesia and Malaysia. Tertiary data, such as the Kamus Besar Bahasa Indonesia (KBBI) and legal dictionaries, are used to clarify the meanings of key terms used throughout the study. Data collection techniques involve document analysis, in-depth interviews, and field observations concerning personal data protection practices within related institutions or agencies. The collected data is analyzed using descriptive-analytical techniques, which involve describing, examining, and comparing legal regulations and the implementation of the due process of law principle in the context of personal data protection, particularly in the case under study. The analysis aims to assess the effectiveness of current regulations and the extent to which procedural justice principles are upheld during legal proceedings involving personal data protection violations.

3. Research Results and Discussion

3.1. Personal Data Protection in Indonesia and Malaysia

The protection of personal data is a constitutional mandate as stipulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right to security and protection of oneself from threats to human rights.¹¹ This protection serves as a citizen's right to personal data confidentiality, enhances public awareness, and affirms the recognition of personal data as part of fundamental human rights. In Indonesia, personal data protection has been regulated through various sectoral laws, such as the Banking Law, Consumer Protection Law, Human Rights Law, Telecommunications Law, Population Administration Law, Public Information Disclosure Law, and the Law on Electronic Information and Transactions. These

¹¹ Yahya Ziqra, "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online," *Iuris Studia: Jurnal Kajian Hukum*, 2021, <https://doi.org/10.55357/is.v2i2.146>.

provisions are further reinforced by the enactment of Law Number 27 of 2022 on Personal Data Protection, which serves as the core regulatory framework.¹²

Various legal instruments related to personal data protection include Law No. 24 of 2013 concerning Amendments to Law No. 24 of 2006 on Population Administration, which addresses the confidentiality and security of civil registration data. Article 8 paragraph (1) letter e states that:

- a. "To register civil events and record vital events";
- b. "To provide equal and professional services to every resident reporting civil events and vital events";
- c. "To print, issue, and distribute civil registration documents"
- d. "To document the results of population registration and civil recording";
- e. "To ensure the confidentiality and security of data regarding civil events and vital events"; and
- f. "To verify and validate the information data provided by the population in the delivery of population registration and civil recording services."

In accordance with the authority of the Civil Registration Implementing Agency, it holds full responsibility and has access rights concerning the confidentiality and security of data for the population. The data security referred to in letter e includes personal data of the population as outlined in Article 84 paragraph (1). This personal data includes the Family Card (KK) number, information on physical and/or mental health records, the Population Identification Number (NIK), the NIK of the mother, the NIK of the father, the date/month/year of birth, as well as several other important records.

In accordance with the authority of the Civil Registration Implementing Agency, it holds full responsibility and has access rights concerning the confidentiality and security of data for the population. The data security referred to in letter e includes personal data of the population as outlined in Article 84 paragraph (1). This personal data includes the Family Card (KK) number, information on physical and/or mental health records, the Population Identification Number (NIK), the NIK of the mother, the NIK of the father, the date/month/year of birth, as well as several other important records.

Procedures for accessing population data must comply with applicable regulations. In the event of a violation or unauthorized access, criminal sanctions shall be imposed in accordance with the provisions outlined in Articles 77 and 86. Article 77 states, "Any person is prohibited from ordering and/or

¹² Thiara Dewi Purnama and Abdurrahman Alhakim, "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia," *E-Journal Komunitas Yustisia* 4, no. 3 (2021).

facilitating and/or manipulating Population Data and/or population data elements." ¹³

Regulations regarding criminal sanctions related to privacy violations and the misuse of personal data in civil registration administration are further outlined in Articles 94 and 95A. Article 94 states, "Any person who orders and/or facilitates and/or manipulates Population Data and/or population data elements as referred to in Article 77 shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 75,000,000 (seventy-five million rupiah)." Article 95A states, "Any person who unlawfully disseminates Population Data as referred to in Article 79 paragraph (3) and Personal Data as referred to in Article 86 paragraph (1a) shall be punished with imprisonment for a maximum of 2 (two) years and/or a fine of up to IDR 25,000,000 (twenty-five million rupiah)."¹⁴

Furthermore, the protection of personal data in accordance with Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law) applies to electronic transactions and regulates aspects of protection for users' personal data and privacy. The use of electronic information, protection of personal rights, personal data, and economic interests must be ensured.

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions, Article 32 states:¹⁵

- (1) Any person who intentionally and without authorization or unlawfully, by any means, alters, adds, reduces, transmits, damages, removes, moves, hides any Electronic Information and/or Electronic Documents belonging to another person or to the public
- (2) Any person who intentionally and without authorization or unlawfully, by any means, transfers or transfers Electronic Information and/or Electronic Documents to the Electronic System of another person who is not entitled.
- (3) Any act referred to in paragraph (1) that results in the disclosure of one Electronic Information and/or Electronic Document that is confidential and becomes accessible to the public with data integrity that is not as it should be."

¹³ Anryana S, Ahmad Yamin, and Muhammad Nur Fietroh, "Penerapan E-Government Melalui Aplikasi Identitas Kependudukan Digital Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Sumbawa Barat," *JiIP - Jurnal Ilmiah Ilmu Pendidikan* 7, no. 1 (2024), <https://doi.org/10.54371/jiip.v7i1.3619>.

¹⁴ Teguh Prasetyo and Jamalum Sinambela Sinambela, "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat," *SPEKTRUM HUKUM* 20, no. 1 (2023), <https://doi.org/10.56444/sh.v20i1.3663>.

¹⁵ Rahmat Suhargon, Ari Dermawan, and Taufiq Hidayah, "URGensi UU ITE DALAM MENJALANKAN PERAN AKTIF KEDUDUKAN HUKUM BISNIS DI INDONESIA," *Journal of Science and Social Research* 7, no. 1 (2024).

Regarding the application of sanctions against individuals who are known to be perpetrators of crimes involving the unauthorized use of personal data, which violates the privacy rights of others, and who meet the criteria of criminal offenses under the Electronic Information and Transactions Law (UU ITE), this is outlined in Article 48.

The application of sanctions against parties proven to commit crimes related to the unauthorized use of personal data and violations of others' rights to privacy is regulated in the Electronic Information and Transactions Law (UU ITE). According to Article 48 of the ITE Law, perpetrators who fulfill the elements of criminal offenses as stipulated in Article 32 will face imprisonment with varying durations, depending on the severity of the violation. The criminal sanction of imprisonment can last up to 8 years, with a maximum fine of IDR 2 billion for violations that meet the criteria of Article 32 paragraph (1). If the criteria in Article 32 paragraph (2) are met, the perpetrator may be sentenced to up to 9 years of imprisonment and a fine of up to IDR 3 billion. For violations that meet the criteria of Article 32 paragraph (3), the perpetrator may be sentenced to a maximum of 10 years in prison and a fine of up to IDR 5 billion.

Furthermore, particularly with the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP), there is significant potential in the government's efforts to protect human rights. The existence of the UU PDP, when viewed from philosophical, sociological, and juridical perspectives, reflects the following aspects:¹⁶

First, the philosophical foundation is rooted in the principles of human rights and social justice, which are reflected in Pancasila as the state ideology of Indonesia. Specifically, the philosophical foundation is outlined in the value of humanity, where personal data is part of an individual's dignity and identity. The regulation of its protection aims to ensure that personal data is not misused or treated unfairly, which could harm individuals. The values of Justice and Equality demand that everyone receives fair treatment, including the protection of their personal data. This Law aims to ensure that every individual has control over their personal data and that it is not misused by any party, be it the state, corporations, or individuals. It also emphasizes the value of individual freedom and autonomy. The principle of personal freedom ensures that every individual has the right to manage and control their personal data without coercion or abuse by others.

Second, from a sociological perspective, this Law emerges as a response to the rapid development of technology and digitalization, where personal data is

¹⁶ Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Lex Renaissance* 7, no. 3 (2022), <https://doi.org/10.20885/jlr.vol7.iss3.art1>.

increasingly easy to collect, process, and disseminate. This is driven by advancements in technology, particularly in the fields of the internet and social media, which have accelerated the collection of personal data and information. The need for regulations that protect personal data from misuse and exploitation has become urgent. As digital communication becomes more prevalent, awareness of the importance of protecting personal data has also increased. Misuse of personal data can lead to financial, social, and psychological harm, highlighting the need for regulations to ensure its security and protection. The growing access to personal data in public and virtual spaces, along with changing social norms regarding privacy and individual rights, has led to a shift in societal needs. Therefore, there is a need for legal protection to maintain privacy boundaries and prevent the exploitation of personal data.

Third, the juridical foundation is reflected in Indonesia's legal system, which includes the constitution and various other regulations. Indonesia's constitution recognizes human rights, one of which includes the right to privacy, including personal data protection. As stated in Article 28 G, paragraph (1) of the 1945 Constitution, every person has the right to be treated fairly and without discrimination, which also includes the protection of their personal data. The application of privacy protection is explicitly regulated in the Personal Data Protection Law (UU PDP). Article 1, number 1 of the UU PDP defines personal data as data related to an individual that can be identified, either directly or indirectly, through the use of other information. This article also emphasizes that personal data can be processed in both electronic and non-electronic forms. Meanwhile, Article 4 regulates the types of personal data, which are categorized into two main groups: specific personal data and general personal data. Specific personal data carries a higher risk for the data subject, such as in cases of discrimination or harm, while general personal data includes information such as full name, gender, nationality, religion, and marital status.

One of the key principles regulated in the Personal Data Protection Law (UU PDP) is the consent for the processing of personal data. According to Article 22, consent for the processing of personal data must be given in writing or recorded, either electronically or non-electronically, and must have the same legal effect. This consent must also contain clear information about the purpose of the processing, in a format that is easy to understand and access. If the consent does not meet these requirements, it may be considered null and void by law.

Furthermore, the UU PDP also imposes strict penalties on parties that violate the provisions regarding the processing of personal data. Article 67 stipulates that anyone who deliberately and unlawfully acquires or discloses another person's personal data may face imprisonment and significant fines. Violations of personal data also include the misuse of personal data for personal gain or for

the benefit of others, which may harm the data subject, as outlined in Article 68, which imposes criminal sanctions on those who deliberately create or falsify personal data for harmful purposes.

Having discussed the protection of personal data from the perspective of national law, this section will also examine the Protection of Personal Data in Other Countries, where the author will attempt to compare the regulation of personal data protection in Indonesia with that in Malaysia. The Malaysian Personal Data Protection Act 2010 (PDPA) contains several key principles. There are 7 principles of personal data protection that must be adhered to, as outlined in Section 5(1) of the Personal Data Protection Act 2010. These principles include the integrity of personal data: the processing of personal data by a data user shall comply with the following Personal Data Protection Principles:¹⁷

- a) The General Principle (prinsip umum);
- b) The Notice and Choice Principle (prinsip pemberitahuan dan pilihan);
- c) The Disclosure Principle (prinsip pengungkapan);
- d) The Security Principle (prinsip keamanan);
- e) The Retention Principle (prinsip retensi);
- f) The Data Integrity Principle (prinsip integritas data); and
- g) The Access Principle (prinsip akses)

In the section above regarding personal data protection, the principles must be fulfilled to ensure that data users feel safe and their personal data is protected. If the provisions mentioned above are violated, a fine of three hundred thousand ringgit or imprisonment for up to two years will be imposed.¹⁸

Additionally, the Personal Data Protection Act 2010 contains provisions regarding the application for registration as specified in Section 16(1), which states: "A person who belongs to the class of data users as specified in the order made under subsection 14(1) shall submit an application for registration to the commissioner in the manner and form as determined by the commissioner."

This provision requires business operators or data users to register their applications with the commissioner, who will then issue a certificate for data management. If business operators or data users process personal data without having this certificate, they will be subject to a fine of five hundred thousand ringgit or imprisonment for up to three years. This regulation provides greater security for individuals who wish to share their personal data, as they can first verify whether the data management process is certified.

¹⁷ Ali Alibeigi and Abu Bakar Munir, "Malaysian Personal Data Protection Act, a Mysterious Application," *University of Bologna Law Review* 5, no. 2 (2020), <https://doi.org/10.6092/ISSN.2531-6133/12441>.

¹⁸ Ida Madieha Azmi, "Bioinformatics and Genetic Privacy: The Impact of the Personal Data Protection Act 2010," *Computer Law and Security Review* 27, no. 4 (2011), <https://doi.org/10.1016/j.clsr.2011.05.008>.

With the enactment of the Personal Data Protection Act 2010, individuals are granted new rights, such as the right to be informed about their personal data, as well as the right to access, correct, and control the processing or use of their personal data by other parties. The Act also regulates cross-border personal data transfer. The Personal Data Protection Act 2010 stipulates that no transfer of personal data outside of Malaysia can occur unless designated by the Minister of Information, Culture, and Communication. Moreover, the destination country where the personal data is transferred must provide an adequate level of protection, at least equivalent to the protection provided by the Personal Data Protection Act 2010 of Malaysia.¹⁹

Furthermore, the Personal Data Protection Act 2010 regulates cross-border data transfer in Section 129(1), which states: "A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette."²⁰

Based on the data protection regulations in Indonesia, it can be analyzed that both Indonesia and Malaysia have similar regulations in place to protect personal data, including the rights of data subjects, the obligations of data controllers, and the implementation of the consent principle. However, differences exist in the structure of oversight, the regulation of sanctions, and the way these regulations are implemented in both countries.

3.2. The Principle of Due Process of Law and Its Implementation in the Legal Certainty of Personal Data Protection in Case No. 46/Pid.Sus/2023/PN.Slt

In this section, the researcher will first provide an overview of the concept of due process of law, which is closely related to the historical struggle for human rights. In England, it is known through the Magna Carta (1215), followed by the Bill of Rights (1689), the Declaration of the Rights of Man and Citizen (1789), the Declaration of Independence (1776), and the Universal Declaration of Human Rights (1948). The principle of due process of law is reflected in the provisions of the Indonesian Criminal Procedure Code (KUHAP). Due process of law emphasizes that every enforcement and application of criminal law must comply with constitutional requirements and adhere to the law. Due process of

¹⁹ Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia," *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018), <https://doi.org/10.24815/kanun.v20i2.11159>.

²⁰ Fadhilah Abdul Ghani et al., "An Overview of the Personal Data Protection Act 2010 (PDPA) : Problems and Solutions," *Global Business and Management Research : An International Journal* 12, no. 4 (2020).

law does not allow violations of certain provisions of the law under the pretext of enforcing other legal provisions.²¹

In order to ensure the achievement of due process of law in its implementation, law enforcement officials must adhere to, recognize, respect, and protect the doctrine of incorporation, which encompasses various rights, including some that are outlined in Chapter IV of the Indonesian Criminal Procedure Code (KUHAP) concerning investigators and public prosecutors:²²

- a. No one may be compelled to be a witness against themselves in a criminal offense (the right of self-incrimination).
- b. No one may be deprived of or denied the right to life, liberty, or property without due process of law.
- c. Every person must be guaranteed the right to personal security, domicile, and the examination and seizure of documents without just cause.
- d. The right to confront, in the form of cross-examination, with the accuser.
- e. The right to a speedy trial.
- f. The right to equal protection and equal treatment under the law. The principle of equal protection must be upheld in handling similar cases. Providing different protections or treatments is a discriminatory act.
- g. The right to legal counsel assistance in self-defense. This right is a principle outlined in Article 56, paragraph (1) of the KUHAP.

The application of the principle of presumption of innocence, along with the development of the Miranda Rule, which has also been adopted in the KUHAP, includes prohibiting investigators from using brutal practices to coerce confessions and prohibiting psychological intimidation as part of Article 56, paragraph (1) of the KUHAP. It stipulates that if a suspect or defendant is charged with a crime punishable by the death penalty or a sentence of fifteen years or more and does not have legal counsel, the relevant authorities at all stages of the judicial process must appoint legal counsel for them. In other words, in line with the principle of due process of law, law enforcement officials should inform and explain the constitutional rights of the suspect (warning of his constitutional rights).²³

²¹ Dewi Bella Juniarti, "Fulfillment of Defendant's Rights in PERMA Number 4 of 2020 Reviewed from the Principle of Due Process of Law," *Lex Scientia Law Review* 5, no. 2 (2021), <https://doi.org/10.15294/lesrev.v5i2.50385>.

²² John V. Orth, *Due Process of Law : A Brief History*, *Due Process of Law : A Brief History*, 2003.

²³ Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law and Security Review* 42 (2021), <https://doi.org/10.1016/j.clsr.2021.105575>.

Due process of law in personal data protection provides legal certainty for individuals regarding the collection, processing, storage, and distribution of their personal data, in the following ways:²⁴

- a. Data Collection Transparency: The due process principle requires that individuals be clearly and transparently informed about the purpose, types of data being collected, and how this data will be used. In personal data protection, this means that any organization collecting personal data must disclose clear processes related to data collection and usage, including the individuals' rights to access or correct their personal data.
- b. Right to Notification and Consent for Data: Individuals have the inherent right to be informed about and to give consent for the collection and processing of their personal data. The data collection process must be conducted with informed consent, meaning individuals should be given the opportunity to understand what will happen to their data and make decisions based on the information available.
- c. Access and Correction of Personal Data: Due process also involves the right of individuals to access their personal data stored by organizations and provides an opportunity to correct inaccurate or incomplete data. This ensures that no personal data is misused or improperly handled by those responsible for processing the data.
- d. Fairness in Data Processing: The due process principle also requires that the personal data processing be conducted in a fair and proportional manner. This includes limiting data collection to legitimate purposes, avoiding discrimination, and ensuring that personal data is not used excessively or misused.
- e. Protection from Data Misuse: Due process provides protection against potential misuse of personal data by unauthorized parties. Any action taken regarding personal data must comply with legal procedures and be accountable. This includes the obligation to ensure personal data is securely stored and not accessed by unauthorized individuals.
- f. Right to Resolve Disputes: An important aspect of due process is the individual's right to resolve legal disputes related to the use of their personal data. In the context of personal data protection, this includes the right to file complaints or take legal action if their rights are violated, for example, through data protection bodies or courts.
- g. Development of Clear Policies and Regulations: Due process also mandates clear policies and regulations regarding the processing of personal data. Governments or data supervisory bodies must ensure that laws are in place governing the collection and processing of personal data and that these regulations are strictly and fairly enforced.

The discussion will next focus on the analysis of the implementation of due process of law in ensuring legal certainty in the protection of personal data in case No. 46/Pid.Sus/2023/PN.Slt, where the authority of investigators in

²⁴ Khafidah Puspita, "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia," *Jurisprudensi : Jurnal Ilmu Syariah, Perundangan-Undangan Dan Ekonomi Islam* 15, no. 1 (2023), <https://doi.org/10.32505/jurisprudensi.v15i1.5478>.

finding and determining 'initial evidence,' 'sufficient initial evidence,' and 'sufficient evidence,' as regulated in Article 1, point 14, Article 17, and Article 21 paragraph (1) of the Indonesian Criminal Procedure Code (KUHP), can prevent arbitrary actions. The Indonesian National Police Regulation Number 6 of 2019 on Criminal Investigations, Section 5, Article 25 states that in the determination of a suspect: (1) The determination of a suspect must be based on at least two pieces of evidence supported by physical evidence; (2) The determination of a suspect as referred to in paragraph (1) must be carried out through a case examination mechanism, unless the suspect is caught in the act.

Due process of law in the enforcement of law prioritizes the supremacy of law (the law is supreme), which emphasizes that investigators, law enforcement officers, and public prosecutors must adhere firmly to the provisions of criminal procedural law, which in this case is the KUHP. Article 183 of the KUHP emphasizes, "A judge may not impose a sentence on an individual unless there is at least two pieces of evidence...and so on."

As procedural law, the KUHP plays a crucial role in material law. The existence of procedural law is essential for the execution of material law. As stated by Professor H.A.S. Natabaya, "Procedural law (formal law/*formeel recht*) is the lifeblood of material law (*materiël recht*) as a guide for the implementation of material law." Therefore, it guarantees legal certainty for all parties involved in the effort to uphold law and justice and prevents arbitrary actions (*eigenrichting*).²⁵

Gustav Radbruch stated that legal certainty is the essence of law itself. The implementation of legal certainty is manifested as the application of law, especially in relation to legislation. According to Radbruch, law should encompass three fundamental core values: first, the value of justice related to philosophical aspects; second, the value of certainty focused on juridical aspects; and third, the value of utility from a sociological perspective. Legal certainty reflects justice in judicial decisions, where judges are required to explore, follow, and understand the values and sense of justice that live within society. Judges have the authority to establish the law through *Rechtsvinding*, or legal discovery, which is carried out through methods of interpretation. The judge's examination of a case is performed through methods of interpretation. When judges face legal gaps in examining a case, they engage in legal discovery. The judicial system functions as a mechanism that aligns with the theory of a legal system, in which the elements—substance of law, structure of law, and legal culture—complement and influence each other.

²⁵ M.Kn Wibowo T. Tunardy, S.H., "Sumber Hukum Materiil Dan Sumber Hukum Formil," *Jurnal Hukum*, 2020.

In the Salatiga District Court case No. 46/Pid.Sus/2023/PN.Slt, a verdict was issued in a criminal case, as outlined in the judge's considerations, including: "Considering that based on the facts, the Defendant knowingly used someone else's population data, which was intentionally purchased from Mr. BY (DPO), and this act was deliberate and intentional by the Defendant"; "...Considering that the Defendant registered a new SIM card using someone else's NIK and KK as if the registrant was the legitimate owner of the NIK and KK. The Defendant manipulated the use of someone else's NIK and KK to register the new SIM card as if it were being used by the rightful owner, with the purpose of obtaining personal benefits, such as a bonus from the company"; "...Considering that the NIK and KK are population data that can be accessed electronically. In registering the new SIM card, the Defendant used electronic registration by sending an SMS to number 4444"; "...Considering that the Defendant used the NIK and KK without the consent of the rightful owner to register the new SIM card. The data used for registration made it appear as though the legitimate owner or authentic holder of the data was registering the card, thus allowing the new SIM card to be activated"; etc. "Taking into account Article 51 paragraph (1) of Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and Law No. 8 of 1981 on the Criminal Procedure Code, as well as other relevant laws and regulations."

Subsequently, the Judge issued the following verdict :

1. *Declares that the Defendant, EY bin Guntiono, has been proven beyond a reasonable doubt to be guilty of committing the criminal offense of "Knowingly, without rights and unlawfully, manipulating electronic information with the intent that such electronic information is considered as if it were authentic data," as stated in the first alternative indictment of the Public Prosecutor;*
2. *Imposes a sentence of 6 (six) months of imprisonment and a fine of IDR 50,000,000 (fifty million rupiahs), with the provision that if the fine is not paid, it shall be replaced with a prison sentence of 2 (two) months;*
3. *Orders that the period of arrest and detention already served by the Defendant be deducted in full from the imposed sentence;*
4. *Orders that the Defendant remains in detention;*
5. *Orders the following evidence to be confiscated :*
 - 1 (one) purchase receipt issued by the Singa Kota Counter;
 - 1 (one) SIM card from Smartfren with the number 088813981569;
 - 1 (one) INFINIX brand mobile phone.

The considerations and the verdict of the Judge are as follows: (1) The proper process for SIM card registration must use the data of the customer who will use the SIM card, not the identity data of someone else who is not using the SIM card; (2) Manipulation using someone else's electronic information is not prohibited, but when coupled with other elements such as being without rights and without the permission of the information's rightful owner, it becomes unlawful. In this case, the data used was made to appear as if it were authentic

data; (3) Manipulation using electronic information is associated with the element of being without rights, without the permission of the rightful owner of the electronic information. In this case, the data used was made to appear as authentic data; (4) The prohibition of using someone else's data for SIM card registration with the intent to prevent it from being used for criminal activities.

Moreover, manipulating electronic information in the registration of a SIM card with the intent that the electronic information and/or electronic documents be considered as if they were authentic data, in order to make it appear as though the user of the SIM card is the person listed on the NIK and KK in the SIM card registration, when in fact the user is someone else, is prohibited. Article 156 of Minister of Communication and Information Regulation No. 05 of 2021 states that the registration of prepaid telecommunications service customers must involve validation and/or verification of the identity of the prospective customer.

The implementation of the Law in accordance with Article 94 in conjunction with Article 77 of Law of the Republic of Indonesia No. 24 of 2013 regarding amendments to Law of the Republic of Indonesia No. 23 of 2006 on Population Administration, Article 94 of Law No. 24 of 2013 states: "Anyone who orders, facilitates, or manipulates population data and/or population data elements as referred to in Article 77 shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to IDR 75,000,000." Article 77 of Law No. 24 of 2013 states: "Everyone is prohibited from ordering, facilitating, or manipulating population data and/or population data elements, as no one shall manipulate, create, alter, delete, or destroy electronic information and/or electronic documents of population data with the intent that such electronic information and/or documents be considered as if they were authentic data."

Population data, as authentic data, is unique or distinctive, singular, and attached to an individual registered as an Indonesian citizen (WNI). Population data consists of personal data and/or aggregate data of the population. Personal data includes: "Family Card Number, Population Identification Number, Full Name; Gender; Place of Birth; Date/Month/Year of Birth; Blood Type; Religion/Belief; Marital Status; Relationship Status within the Family; Physical and/or Mental Disabilities; Last Education; Type of Occupation; Mother's NIK (Identification Number); Mother's Name; Father's NIK; Father's Name; Previous Address; Current Address; Ownership of Birth Certificate/Letter of Birth Acknowledgment; Birth Certificate Number/Letter of Birth Acknowledgment Number; Ownership of Marriage Certificate/Marriage Book; Marriage Certificate Number/Marriage Book Number."

The successful resolution of the case Judgment of Judge in Case No. 46/Pid.Sus/2023/PN.Slt above, the enforcement of criminal law in SIM card registration, the Police (Investigator) applied Model A Report, which is a written report made by a police officer who has experienced, known, or directly discovered an incident. The Model A Police Report is as specified in Article 3, Paragraph (5), Letter (a) of the National Police Regulation No. 6 of 2019 on Criminal Investigation.

Reviewing the success of Law Enforcement Officers in addressing the criminal act of SIM card registration, it is evident that the implementation of Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection (PDP) has not yet been fully realized. Given that the PDP Law was enacted on October 17, 2022, it still requires institutional adjustments to the provisions on Personal Data Processing, which must be completed within 2 (two) years from the enactment of the PDP Law.

Connecting the relevance of the case at hand with the PDP Law, Article 4, Paragraph (3) addresses "general personal data," while Article 22, Paragraph (1) outlines the rules for consent to personal data processing, which must be obtained in writing or recorded. Article 67 includes provisions for criminal penalties, and Article 63 provides opportunities for "community participation." The community can play a role, both directly and indirectly, in supporting the implementation of personal data protection. In alignment with Gustav Radbruch's perspective, which identifies three fundamental core values of law—first, the value of justice in the philosophical aspect; second, the value of certainty in the legal aspect; and third, the value of utility from a sociological perspective—along with Lawrence M. Friedman's view of legal system theory, which emphasizes the interconnected and mutually influencing elements of legal substance, legal structure, and legal culture, legal certainty in personal data protection can be further optimized. The police should not only implement police reports in the Model A format but also establish the Police Report in the Model B format.

4. Closing

4.1. Conclusions

Based on the discussion above, it can be concluded that although both Indonesia and Malaysia have regulations governing personal data protection, each country faces significant challenges and differences in the implementation and enforcement of these regulations. In Indonesia, although the Personal Data Protection Law (UU PDP) was enacted in 2022, Malaysia had already established personal data protection through the Personal Data Protection Act (PDPA), which was enacted in 2010. Regarding the analysis of the due process of law principle in

the context of personal data protection, this principle is closely related to ensuring that individuals whose rights are violated in terms of personal data receive justice through a clear, transparent, and fair legal process. The due process of law demands that any legal action taken by the state in the implementation of personal data protection must be conducted in accordance with appropriate procedures and not arbitrarily, while providing equal opportunity for all parties to defend their rights. In the context of case No. 46/Pid.Sus/2023/PN.Slt, the implementation of due process of law in this case demonstrates the state's efforts to provide legal certainty in the enforcement of personal data protection. However, challenges remain in ensuring that this principle is applied consistently, considering the frequent legal uncertainties that arise in judicial procedures. Legal certainty regarding personal data protection, although beginning to be enforced, requires strengthening in terms of oversight and more assertive law enforcement, both by law enforcement agencies and relevant institutions.

4.2. Suggestions

The government needs to strengthen oversight, enhance public education, ensure the application of the principle of due process of law, and impose strict sanctions in the protection of personal data in order to establish more effective legal certainty in both Indonesia and Malaysia.

REFERENCES

- Alibeigi, Ali, and Abu Bakar Munir. "Malaysian Personal Data Protection Act, a Mysterious Application." *University of Bologna Law Review* 5, no. 2 (2020). <https://doi.org/10.6092/ISSN.2531-6133/12441>.
- Arya Agung, Hasbi Pratama. "Perlindungan Data Pribadi Dalam Proses Pengurusan Perizinan Perusahaan Berbasis Elektronik Online Single Submission (OSS)." *Jurnal Ilmiah Galuh Justisi* 9, no. 1 (2021). <https://doi.org/10.25157/justisi.v9i1.4862>.
- Azmi, Ida Madieha. "Bioinformatics and Genetic Privacy: The Impact of the Personal Data Protection Act 2010." *Computer Law and Security Review* 27, no. 4 (2011). <https://doi.org/10.1016/j.clsr.2011.05.008>.
- Blessing, Moses. "Comparative Analysis of Data Protection Laws : Learning from Global Best Comparative Analysis of Data Protection Laws : Learning from Global Best Practices Author : Moses Blessing Date : 5 Th Oct , 2024 Abstract :," no. October (2024).
- Cahyono, Joko. "JUNCTO : Jurnal Ilmiah Hukum Perlindungan Data Pribadi Di Era Digital Berdasarkan" 6, no. 2 (2024): 330–39. <https://doi.org/10.31289/juncto.v6i2.5443>.

- Fauzi, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Lex Renaissance* 7, no. 3 (2022). <https://doi.org/10.20885/jlr.vol7.iss3.art1>.
- Ghani, Fadhilah Abdul, Syahirah Mohd Shabri, Maizatul Akmar Mohd Rasli, Nurulhuda Ahmad Razali, and Emir Hambali Ahmad Shuffri. "An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions." *Global Business and Management Research: An International Journal* 12, no. 4 (2020).
- Gumilar, Gugum, Eka Budiarto, Maulahikmah Galinium, and Charles Lim. "Personal Data Protection Framework for Web Developers and API Providers under UU PDP." In *2023 International Conference on Informatics, Multimedia, Cyber and Information Systems, ICIMCIS 2023*, 2023. <https://doi.org/10.1109/ICIMCIS60089.2023.10349040>.
- Juniarti, Dewi Bella. "Fulfillment of Defendant's Rights in PERMA Number 4 of 2020 Reviewed from the Principle of Due Process of Law." *Lex Scientia Law Review* 5, no. 2 (2021). <https://doi.org/10.15294/lesrev.v5i2.50385>.
- Kusuma, Aditama Candra, and Ayu Diah Rahmani. "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)." *SUPREMASI: Jurnal Hukum* 5, no. 1 (2022). <https://doi.org/10.36441/supremasi.v5i1.721>.
- Maciej Serda, Fernando Gertum Becker, Michelle Cleary, R M Team, Helge Holtermann, Disclaimer The, National Agenda, et al. "Pengaruh Terpaan Berita Tentang Kebocoran Data Pengguna Tokopedia Dan Aktivitas Word of Mouth Terhadap Tingkat Kepercayaan Dalam Menggunakan Tokopedia." *Interaksi Online* 9, no. 2 (2021).
- Mariani, John F. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia." *The Encyclopedia of American Food and Drink* 3 (2020).
- Niffari, Hanifan. "PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain." *Jurnal Hukum Dan Bisnis (Selisik)* 6, no. 1 (2020). <https://doi.org/10.35814/selisik.v6i1.1699>.
- Orth, John V. *Due Process of Law : A Brief History. Due Process of Law : A Brief History*, 2003.
- Prasetyo, Teguh, and Jamalum Sinambela Sinambela. "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat." *SPEKTRUM HUKUM* 20, no. 1

- (2023). <https://doi.org/10.56444/sh.v20i1.3663>.
- Prayogo⁴, Refaldy Braif Carundeng² Anna S. Wahongan³ Presly. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik." *Lex Privatum* 10, no. 1 (2022).
- Purnama, Thiara Dewi, and Abdurrahman Alhakim. "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *E-Journal Komunitas Yustisia* 4, no. 3 (2021).
- Puspita, Khafidah. "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia." *Jurisprudensi: Jurnal Ilmu Syariah, Perundangan-Undangan Dan Ekonomi Islam* 15, no. 1 (2023). <https://doi.org/10.32505/jurisprudensi.v15i1.5478>.
- S, Anryana, Ahmad Yamin, and Muhammad Nur Fietroh. "Penerapan E-Government Melalui Aplikasi Identitas Kependudukan Digital Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Sumbawa Barat." *JlIP - Jurnal Ilmiah Ilmu Pendidikan* 7, no. 1 (2024). <https://doi.org/10.54371/jiip.v7i1.3619>.
- Saleh, Abd. Rahman. "Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana." *HUKMY: Jurnal Hukum* 1, no. 1 (2021). <https://doi.org/10.35316/hukmy.2021.v1i1.91-108>.
- Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018). <https://doi.org/10.24815/kanun.v20i2.11159>.
- Stoykova, Radina. "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence." *Computer Law and Security Review* 42 (2021). <https://doi.org/10.1016/j.clsr.2021.105575>.
- Suhargon, Rahmat, Ari Dermawan, and Taufiq Hidayah. "URGENSI UU ITE DALAM MENJALANKAN PERAN AKTIF KEDUDUKAN HUKUM BISNIS DI INDONESIA." *Journal of Science and Social Research* 7, no. 1 (2024).
- Wibowo T. Tunardy, S.H., M.Kn. "Sumber Hukum Matreiril Dan Sumber Hukum Formil." *Jurnal Hukum*, 2020.
- Yahya Ziqra. "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online." *Iuris Studia: Jurnal Kajian Hukum*, 2021. <https://doi.org/10.55357/is.v2i2.146>.