Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022
ISSN: 2747-2604
Volume 7 No. 4, December 2025

The Urgency of Establishing a Personal Data Protection Agency in Indonesia (Adopting the South Korean Personal Data Protection Agency Model)

Lubna Tabriz Sulthanah[1)] & Rasji[2)]
[1)]Faculty of Law, Universitas Tarumanagara, Indonesia, E-mail: lubna.207231020@stu.untar.ac.id
[2)] Faculty of Law, Universitas Tarumanagara, Indonesia, E-mail: rasji@fh.untar.ac.id

Abstract. *Countries under the constitution have a responsibility to protect the privacy of every citizen, one of which is through the protection of personal data. Indonesia has not yet had its own institution tasked with realizing the implementation of the protection of personal data in an integrated manner. Indonesia, when compared to several countries in the Southeast Asia and Asia region, can be said to be lagging behind in terms of having the PDP Law, including the absence of a Personal Data Protection Institution. As a policy study material to see the form of the Personal Data Protection Agency, the researcher will examine the Personal Information Protection Commission (PIPC), which is a personal data protection institution in South Korea. The selection of the country is based on the fact that South Korea is one of the countries in Asia that is considered to meet the equality standards of data protection laws. The type of research used is a normative legal research method supported by empirical legal research methods. The data collection technique was carried out by literature study supported by interviews with parties involved in the research. The main problem that will be raised in this study is how the Personal Data Protection Institutions in Indonesia and South Korea are similar and different. In addition, what is the urgency of establishing a Personal Data Protection Agency in Indonesia that adopts PIPC in South Korea. The adoption in question does not mean plagiarizing in a complete way, but adaptation by considering constitutional conditions, capacity, and specific needs.*

Keywords: *Agency; Data; Personal; Protection; Urgency.*

1. Introduction

The increasingly widespread use of Information and Communication Technology (ICT) will bring transformation in fulfilling the social life of the community. The presence of Information and Communication Technology (ICT) has eliminated

restrictions in accessing various resources through the internet. The lack of interaction between public space and personal life causes certain individuals or groups of people to use it to seek profit through the internet (Fauzi & Alif RS, 2022). The data that has been collected, will be easily misused such as manipulated, stolen or even sold to irresponsible third parties. Situations like this are difficult to avoid because almost every activity in life in this digital era uses personal data. The increasing use of technology or the growing number of internet users, this will be in line with the increasing frequency of cyber attacks that may occur.

Article 28G Paragraph 1 of the Constitution of the Republic of Indonesia 1945 (UUD NRI 1945) states that, "everyone has the right to the protection of personal self, family, honor, dignity, and property under his or her power, and has the right to a sense of security and protection from threats or fear to do or not do something that is a human right". The provision does not explicitly mention the right to privacy, but explains that the state under the constitution has a responsibility to protect the privacy of every citizen, one of which is through the protection of personal data. The concept of privacy is related to the protection of privacy data, which aims to maintain the integrity and dignity of each individual (Djafar & Komarudin, 2014).

Based on the results of the report by the State Cyber and Cryptography Agency (BSSN) in the Indonesian Cyber Security Landscape Document prepared by the Directorate of Cyber Security Operations, it was said that during the 2024 period, BSSN has recorded the results of detection of 241 alleged data leak incidents. Comprehensive regulations are needed to minimize cybercrime and ensure full protection of personal data. Several previous regulations have addressed the issue of personal data, but none have specifically explained the implementation of personal data protection. The discussion of the draft Personal Data Protection Bill began on January 24, 2020, then the draft was passed into Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and began to be promulgated on October 17, 2022 which is fully effective on October 17, 2024.

Indonesia has not yet had its own institution tasked with realizing the implementation of the protection of personal data in an integrated manner. The existence of this Personal Data Protection Institution is regulated in Articles 58 to 61 of the PDP Law which covers the duties, functions, and procedures of the institution, while until now regarding personal data protection has been charged to the Ministry of Communication and Digital (Komdigi). The Personal Data Protection Agency is the key in enforcing compliance standards and personal data protection obligations, from data processor controllers. This means that without a strong Personal Data Protection Institution, it is difficult for the PDP Law to be implemented effectively. The existence of the Personal Data Protection Agency

will ensure that the law enforcement process related to the protection of personal data will be carried out independently. This is important, because the object of the PDP Law is not only people but also the public legal entity sector, including in the legislative, executive and judicial realms (Mahardika, 2021).

Indonesia, when compared to several countries in the Southeast Asia and Asia region, can be said to be lagging behind in terms of having the PDP Law, including the absence of a Personal Data Protection Institution. As a policy study material to see the form of the Personal Data Protection Agency, the researcher will examine the Personal Information Protection Commission (PIPC), which is a personal data protection institution in South Korea. The selection of the country is based on the fact that South Korea is one of the countries in Asia that is considered to meet the equality standards of data protection laws.

Based on this background, some of the main problems that will be raised in this study are, how are the similarities and differences between the Personal Data Protection Institutions in Indonesia and South Korea. In addition, what is the urgency of establishing a Personal Data Protection Agency in Indonesia that adopts PIPC in South Korea.

2. Research Methods

Legal research involves a thorough examination of legal facts whose ultimate goal is to find solutions to problems that arise (Muhaimin, 2020). The type of research used is a normative legal research method supported by empirical legal research methods. The nature of the research uses descriptive research. The type of data used in this study is secondary data supported by primary data sourced from informants using data collection techniques in the form of interviews. The data collection technique was carried out by literature study supported by interviews with parties involved with the problems in the research. The approach in this study is to use a statute *approach* and a *conceptual approach*.

3. Results and Discussion

3.1. Similarities and Differences between Personal Data Protection Institutions in Indonesia and PIPC South Korea

Article 1 paragraph (1) of the PDP Law explains that Personal Data is data about an individual who is identified or can be identified separately or combined with other information either directly or indirectly through electronic or non-electronic systems. Personal data with respect to a person's characteristics, name, age, gender, education, occupation, address, and position in the family. Another definition of personal data is data in the form of a person's identity, code, symbol,

letter, or personal marker number that is private and confidential (Latumahina, 2014).

After the enactment of Permenkomdigi 1/2025, the implementation of government affairs in the field of communication and information, including the protection of personal data, is under the authority of Komdigi. Based on the results of an interview with Mr. Eryk Budi Pratama as a cybersecurity and data privacy practitioner, it was found that the biggest obstacle to the implementation of the PDP Law in Indonesia lies in the unpreparedness of the derivative regulatory ecosystem, where the Presidential Regulation on Personal Data Protection Institutions has not yet been passed. Looking at the design side of the regulation, Mr. Eryk Budi Pratama said that the PDP Law that applies in Indonesia is optimal because it regulates principles, data subject rights, the obligations of controllers and processors of personal data, and sanctions. However, its implementation has not been optimal because of 3 (three) main obstacles, namely: 1) The absence of a fully functioning independent supervisory institution; 2) There is no technical standard for the implementation of Personal Data Protection such as the ROPA (Record of Processing Activities), DPIA (Data Protection Impact Assessment) template, breach notification; 3) Some areas still need clarification such as large-scale determination, PDP risk criteria, and cross-border transfer mechanisms.

Specifically, based on the provisions of Article 144 of Permenkomdigi 1/2025, the Directorate General of Digital Space Supervision has the task of formulating and implementing policies in the field of digital space supervision and personal data protection. Based on an in-depth evaluation from the perspective of practitioners, Komdigi as an incubator of the Personal Data Protection Agency has a very broad national digitalization mandate with a limited number of human resources, so the focus on personal data protection is not optimal. The Komdigi is not designed to be an independent supervisory authority, and its investigative and audit capacity is still limited. The concentration of the personal data protection function under the Directorate General of Digital Space Supervision of Komdigi, which has been burdened with extensive tasks and has the potential to experience conflicts of interest to strengthen this vital function, cannot be carried out in a focused, optimal, and free manner from intervention. Therefore, the establishment of a special independent institution, in accordance with the mandate of Article 58 of the PDP Law, is not only a necessity, but also an urgent need to realize effective personal data protection, choose public trust, and ensure legal certainty in Indonesia's digital ecosystem.

South Korea has obtained adequacy status from the European Commission on December 17, 2021 through the Commission Implementing Decision, which recognizes the level of personal data protection under the Personal Information Protection Act (PIPA) of 2011 to be equivalent to the European Union's GDPR

standard. As the implementer of this regulation, South Korea then established PIPC as an independent authority that specifically handles the protection of personal data. Although structurally PIPC is under the Office of the President as stipulated in Article 7 (1) of PIPA, this institution has the independent authority to carry out the function of deliberation and resolution related to data protection issues.

The establishment of PIPC in South Korea was motivated by escalation of concerns about the potential for sensitive data leaks and the increasing number of identity theft cases (Zubaidy et.al, 2022). This institution has a strategic mandate to improve the legal framework related to the protection of personal information, formulate and implement systemic policies, develop a welfare direction plan, as well as conduct investigations and legal handling of various forms of violations of privacy rights that occur. Based on the applicable legal framework, PIPC is formed as an independent entity where its commissioners are appointed directly by the President to carry out the mandate of comprehensive personal data protection in accordance with the provisions of the Law.

In addition to the legal aspects used to protect data and provide sanctions for violators, the success of personal data protection in a country is also supported by public awareness and education as a form of creating a society that is side by side in the digital era to create a safe and trusted digital environment (Tsaniyah & Juliana, 2019).

According to Mr. Eryk Budi Pratama, he confirmed that the South Korean PIPA is often used as a reference in other Asian countries, even the South Korean PIPC is considered to have run effectively and optimally because it has strong investigative authority, enforcement, and imposition of fines, has a clear commissioner structure and operates directly under the President of South Korea, and leads the harmonization of regulations across sectors. This avoids overlapping regulations and conflicts of authority between different government agencies.

The similarities between the Personal Data Protection Institution in Indonesia and PIPC South Korea are as follows:

a. The institution was established under a special law on the Protection of Personal Data;
b. The institution functions as a regulatory, supervisory, educational, and dispute resolution authority; and
c. The Personal Data Protection Law is the main reference in the national personal data protection policy.

Meanwhile, the differences are described in the form of a table as follows:

Table 1. The Difference Between the Indonesian Personal Data Protection Agency and the South Korean PIPC

Comparative Aspects	Indonesia	South Korea
Legal Basis	Law No. 27 of 2022 concerning Personal Data Protection (PDP Law)	Personal Information Protection Act (PIPA)
Status and Independence of the Institution	Indonesia does not yet have an independent institution and is still under the structure of the Kemenkomdigi	It already has an independent institution. Operates directly under the President of South Korea with a clear commissioner structure
Law Enforcement Authority	It is not optimal and limited because the definitive institution does not include full audit authority and the incident is coordinated	Complete and powerful. Have investigative power, law enforcement, and effective fines
Functions and Roles	As a regulatory, supervisory, educational, and dispute resolution authority (in the incubation stage)	As an authority for regulation, supervision, education, and optimal dispute resolution
Cross-Sector Surveillance	It is not fully integrated. There is still a potential for overlap of authority with other sectoral institutions	Integrated and centralized (one-stop authority). Leading the harmonization of regulations across sectors, thereby avoiding overlap.
Position in National Policy	Become the main reference in the national personal data protection policy	Become the main reference in the national personal data protection policy
Administrative Sanctions	It is regulated in the PDP Law, but its effectiveness is still limited	More progressive, in the form of fines based on the percentage of revenue to increase the deterrent
Technical Terms Considered Superior	Not yet fully implemented or still in the setup stage	• Personal Data Protection Audits are mandatory for large organizations • Stricter data minimums & purpose limitations • Pseudonymization obligation for analytical data • Mandatory data security certification system for critical sectors • Privacy by Design Certification

The philosophical foundation of the existence of an independent protection institution in the personal data protection system is the need to create an entity that is able to act objectively and free from all forms of political pressure or economic interests. South Korea in this context has built a model that can be considered a *best practice* through PIPC. PIPC is not only formed based on the mandate of the law, namely PIPA, but is also placed in a strategic position in the constitutional structure. The clause stating that this commission will carry out its functions independently is a constitutional guarantee that allows PIPC to make decisions based on law and evidence, without being influenced by the agenda of the ruling government.

The PIPC's leadership structure consisting of commissioners appointed by the President provides a high level of accountability, while protecting the commissioners from technical intervention from other ministries. This model ensures that PIPC is not an extension of the government bureaucracy, but a state authority that has full autonomy in carrying out its mandate. Looking at law enforcement, PIPC has very varied sanctions and has a significant impact. PIPC can not only impose administrative sanctions in the form of financial fines, but can also order the cessation of data processing, restrictions on data transfers abroad, and the destruction of illegally obtained data. The function of PIPC as *a one-stop authority* ensures the efficiency and consistency of regulations. By concentrating all data protection-related authority in a single institution, South Korea eliminates the potential for overlapping authority and regulatory confusion that often occurs if such authority is fragmented across multiple ministries or institutions.

3.2. The Urgency of Establishing a Personal Data Protection Institution in Indonesia by Adopting South Korea's PIPC

Looking at the provisions in the PDP Law, it actually regulates the authority and duties of the Personal Data Protection Institution listed in Articles 58 to 60 of the PDP Law which has resembled the minimum standards for the regulation of Personal Data Protection Institutions internationally. Although normatively Indonesia through the PDP Law has mandated the establishment of similar independent institutions in accordance with international standards, in practice the process of handling the law and implementing sanctions for various failures to protect personal data is still under the authority of the Ministry of Communication and Commerce, considering that until now a special institution for personal data protection has not been formed.

While South Korea has come a long way with its PIPC model, Indonesia is still entangled in a *status quo* full of uncertainty and limitations. The ratification of the PDP Law in October 2022 had given hope for the birth of a new era of data protection in Indonesia. The PDP Law expressly mandates the establishment of a special institution tasked with implementing personal data protection, however, almost three years after the ratification of the PDP Law, the mandate to establish this independent institution has still not been realized. The absence of a Presidential Regulation mandated by Article 58 paragraph (5) of the PDP Law to further regulate the institution has created *an alarming* vacuum of authority.

The function of supervision and enforcement of personal data protection laws while carried out by the Ministry of Communication and Communications is precisely under the Directorate General of Digital Space Supervision and more specifically under the Directorate of Digital Space Supervision Strategy and Policy. The placement of the function of personal data protection in the bureaucratic

structure of the ministry creates at least two fundamental problems. First, Komdigi has a very broad portfolio of tasks, in this context, personal data protection is only one of many tasks, so it has the potential to not receive adequate attention and resource allocation. This divided focus risks making the supervisory function run suboptimally. Second, Komdigi is part of the executive government. The government is one of the largest controllers of personal data through various *e-government* programs, population databases, tax systems, and so on. Placing the data protection oversight function within the government creates an inevitable conflict of interest. This is contrary to the fundamental principle of law enforcement, which is *nemo iudex in causa sua*, which means that no one should be a judge in his own affairs. Such a model has the potential to undermine objectivity and neutrality in supervision.

The structural limitations of the Komdigi have direct implications for the weak law enforcement capacity. In contrast to PIPC, which has clear and strong investigative authority, the authority of the Komdigi to conduct audits and examinations of personal data controllers is considered incomplete and still limited. In addition, although the PDP Law has regulated administrative sanctions, the mechanism for imposing such sanctions is not optimal considering that a definitive institution, in this case an independent PDP Institution, has not yet been formed. The absence of authority to impose sanctions that are direct, firm, and have a deterrent effect makes the Ministry of Communication and Communication not have sufficient power to discipline violators.

Fragmentation of authority is another complex issue in the governance of personal data protection in Indonesia. The supervisory function is not fully centralized at the Komdigi. BSSN has a role in handling cybersecurity incidents, including those that lead to data leaks. The Financial Services Authority (OJK) regulates data protection in the financial services sector, while the Ministry of Health has an interest in health data. Multi-regulator conditions have the potential to create overlapping standards and confusion for data controllers. This has the potential to weaken the overall effectiveness of data protection. This model is in stark contrast to *the one-stop authority* implemented by PIPC in South Korea.

The inconsistency between the legal design in the PDP Law and its implementation further clarifies the gap between Indonesia and South Korea. The PDP Act has been designed quite comprehensively, adopting many international principles and providing a strong mandate for the establishment of independent institutions. When it is implemented, the mandate has not been realized. As a result, there is a dissonance between legal expectations (*law in the books*) and laws that live in practice (*law in action*).

An analysis of the status quo of Indonesia and South Korea's PIPC has revealed a wide gap in the effectiveness of personal data protection. This gap is not only technical-operational, but touches on fundamental aspects in fulfilling citizens' constitutional rights and the nation's competitiveness in the digital era. Therefore, discussing the urgency of establishing an independent personal data protection institution by adopting the South Korean PIPC model is a must. This urgency must be reviewed from at least four interrelated perspectives: legal and constitutional perspectives, digital economy perspectives, national security and data sovereignty perspectives, and social and human rights (HAM) perspectives.

Based on a legal and constitutional point of view, the urgency of establishing an independent institution stems from the existence *of a vacuum of authority* created by the inconsistency between the mandate of the PDP Law and the reality of its implementation. The PDP Law clearly mandates the establishment of a special institution in Article 58. Furthermore, Articles 59 and 60 detail the duties and authorities of the institution. However, this constitutional right cannot be realized optimally and does not have an effective enforcement mechanism because the institution mandated to guarantee it has not yet been established. In legal theory, this condition can be categorized as *legislative neglect*, where the lawmaker is considered negligent because he did not realize the mandate that he has set himself. This creates uncertainty regarding the *legal standing* of the Ministry of Communication and Tourism in carrying out functions that should be the authority of independent institutions. This uncertainty creates legal vulnerabilities both for data subjects whose rights are violated, as well as for data controllers who need certainty in carrying out their compliance obligations.

The urgency from the perspective of the digital economy is perhaps the most concrete and easily measurable argument for impact. Indonesia's digital ecosystem is growing rapidly, driven by the boom of the creative economy. This growth relies heavily on a smooth and legal flow of cross-border data. Countries with internationally recognized levels of data protection, such as South Korea, which have obtained *adequacy status* from the European Union, enjoy significant ease in transferring data to these jurisdictions. On the contrary, the absence of a credible and independent supervisory institution in Indonesia is a major obstacle to obtaining similar recognition. This clearly reduces Indonesia's competitiveness in attracting investment and becoming part of the global value chain.

Based on a national security and data sovereignty perspective, the ability to respond to incidents quickly, coordinated, and have strong law enforcement authority is imperative. The current institutional model, where the handling is spread between the Komdigi, BSSN, and the police, has proven to be suboptimal. An independent agency focused on data protection would be a more effective spearhead in mitigating these threats and upholding Indonesia's data sovereignty.

The urgency from a social and human rights perspective, the establishment of independent institutions lies in its function as a guardian of citizens' constitutional rights. Article 28G paragraph (1) of the 1945 Constitution explicitly recognizes everyone's right to personal protection. The personal protection has extended to include the protection of personal data. An independent institution serves as an *institutional guarantee* for this constitutional right. The institution is a place for citizens to complain and seek solutions when their rights are violated. The absence of institutions that can provide real and responsive protection has the potential to cause public disappointment and a lack of trust in the state. If citizens do not believe that their data will be protected by the state, they will be reluctant to participate fully in the digital ecosystem. This will ultimately hamper the government's efforts to digitize various public services. The establishment of credible independent institutions is a key step to restoring and maintaining this public trust.

Adoption does not mean plagiarizing it completely, but rather adapting by taking into account constitutional conditions, capacity, and specific needs. Based on the analysis of the advantages of PIPC, there are six main pillars that must be adopted :

a. Adoption of the principle of full independence at the level of state institutions. The ideal model would be to place it directly under the President, as PIPC. This position provides the highest political legitimacy while breaking the chain of intervention from the ministry's sectoral interests.
b. Institutions must be equipped with strong and independent investigative power. Authority includes the right to summon relevant parties, request access to electronic systems and documents, conduct on-site inspections, and request expert testimony.
c. Institutions must have effective administrative law enforcement authority, with a diversified and deterrent sanctions portfolio. Of particular importance is the revenue-based fine model for serious violations, as implemented by PIPC.
d. Indonesia needs to adopt a mandatory privacy audit mechanism for sectors that are considered high-risk, such as the financial services, healthcare, and technology sectors which are required to undergo periodic data protection compliance audits conducted by independent auditors approved by the Personal Data Protection Agency.
e. Consistent implementation of the principle of one-stop authority. The Personal Data Protection Agency shall be the sole authority authorized to handle all cross-sectoral personal data protection matters. This will eliminate the overlap of authority. Then for highly-regulated sectors such as banking, the Personal Data Protection Agency can coordinate to issue joint technical guidelines, but the authority for supervision and law

enforcement must still be in the hands of the Personal Data Protection Agency.

f. The development of technical standards and for critical sectors should be a priority. The Personal Data Protection Agency must actively certify the application of data protection principles from the design stage of technology systems and products. The adoption of these standards will shift the paradigm from simply reactive responding to incidents to preventive by building a culture of compliance early on.

4. Conclusion

There are similarities between the form of the Personal Data Protection Institution in Indonesia that has been mandated in the PDP Law and the PIPC in South Korea, such as the two institutions were formed based on the special law on Personal Data Protection and function as regulatory, supervision, education, and dispute resolution authorities, as well as being the main reference in national personal data protection policies. Although there are differences in various aspects such as the legal basis, the status and independence of institutions, functions and roles. The existence of PIPC in South Korea has given meaning that the country has shown seriousness in protecting its people. South Korea's PIPC model can be ensured to be able to account for the accurate, complete, and correct use of personal data, thus providing assurance that the personal data managed is well maintained. The urgency of establishing a Personal Data Protection Institution must be reviewed from at least four interrelated perspectives: legal and constitutional perspectives, digital economy perspectives, national security and data sovereignty perspectives, and social and human rights perspectives. Seeing this, the function of the incubator at the Ministry of Communication and Tourism needs to be transferred to an independent institution that focuses on personal data protection. Any delay will only increase national vulnerability, and reduce Indonesia's competitiveness on the global stage. Adopting these principles and adapting them to the Indonesian context, the establishment of this institution is expected to be a turning point in realizing Indonesia's ideals that are not only digital, but also sovereign and protect the rights of its citizens.

5. References

Journals:

Afif Zaid. (2018). Konsep Negara Hukum Rule of Law dalam Sistem Ketatanegaraan Indonesia. *Jurnal Pionir LPPM Universitas Asahan*. Vol. 2, No.5 : p.59

Aryani, Christina. 2021. Reformulasi Sistem Pembentukan Peraturan Perundang-Undangan Melalui Penerapan Omnibus Law. *Jurnal USM Law Review*. Vol. 4, No.1 : p.6

Az-Zahra, Firdausi. (2024). Regulas Perlindungan Data Pribadi : Tinjauan Komparatif Indonesia dan Korea Selatan. *Jurnal Alternatif*. Vol.15, No.2 : p.86

Fauzi, Elfian dan Nabila Alif RS. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Lex Renaissance*. Vol.3, No.3 : p.5

Jazuly, Syukron. (2015). Independent Agencies dalam Struktur Ketatanegaraan Indonesia. Jurnal Supremasi Hukum, Vol.4, No. 1 : p.220

Kusnadi, S.A & Andy U.W. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *Jurnal Ilmu Hukum*. Vol.2, No.1 : p.4

Latumahina, Rosalina Elsina. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita*. Vol.3, No.2 : p.16

Mahardika, Ahmad Gelora. (2021). Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi dalam Sistem Ketatanegaraan Indonesia. *Jurnal Hukum Unissula*, Vol. 37, No.2 : p.4

Mahiar, et.al. (2020). Consumer Protection System (CPS) : Site Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*. Vol.3, No.2 : p.287-302

Mardiana, Nela. (2023). Urgensi Perlindungan Data Pribadi dalam Perspektif Hak Asasi Manusia. *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia*. Vol.5, No.1 : p.18

Porta, R.La. (2000). Investor Protection and Corporate Governance. *Jurnal of Financial Economics*. Vol.58, No.1 : p.90

Tsaniyah, Naimatus & Kannisa A.J. (2019). Literasi Digital sebagai Upaya Menangkal Hoaks di Era Disrupsi. *Al Balagh:Jurnal Dakwah dan Komunikasi*. Vol.4, No.1 : p.121

Suari, K.R.A & I Made Sarjana. (2023). Menjaga Privasi di Era Digital : Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*. Vol.6, No.1 : p.135

Zubaidy, Anang., et.al. (2022). Menggagas Pembentukan Komisi Perlindungan Data Pribadi (Studi Komisi Perlindungan Informasi Pribadi di Korea Selatan dan Peluang Formulasinya di Indonesia). *Prosiding Simposium Nasional Hukum Tata Negara*, Yogyakarta : April 2022 : p.220

Books:

Djafar, W., & Asep, K. (2014). *Perlindungan Hak Atas Privasi di Internet – Beberapa Penjelasan Kunci*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM)

Manggalatung, A. S. (2016). *Desain Kelembagaan Negara Pasca Amandemen UUD 1945*. Bekasi : Gramata Publishing

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram : University Press

Raharjo, Satjipto. (2014). *Ilmu Hukum*. Bandung : PT Citra Aditya Bakti

Rosadi, Shinta Dewi. (2015). *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung : Refika Aditama

Soekanto, Soerjono. (1983). *Tata Cara Penyusunan Karya Tulis Ilmiah Bidang Hukum*. Jakarta : Ghalia Indonesia

_____. (2019). *Faktor- Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta : Rajawali Press

Regulation:

The 1945 Constitution of the Republic of Indonesia

Law No. 27 of 2022 concerning Pelindungan Data Pribadi

Personal Information Protection Act (Act No. 16930). 2020 (S. Korea)

Interview:

Interview with Mr.Eryk Budi Pratama as cybersecurity and data privacy practitioner on November 19, 2025