LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 6, 2025, pp. 1462-1474
Published by: IHSA Institute (Natural Resources Law Institute)

The Role Of The State Towards Data Protection In The Use Of Artificial Intelligence Through The Cooperation Between Countries In Asean

Yanly Gandawidjaja[1], Petra Bunawan[2], Christian Josua F. X. Purba[3]

[123]Faculty of Law, Universitas Katolik Parahyangan, Bandung, Indonesia

Abstract: Cutting-edge technology, including Artificial Intelligence (AI), is essential for supporting human activities, automating tasks, and processing vast amounts of data. However, the use of AI raises concerns about data security, privacy, and the role of humans in legal decision-making. This study explores Indonesia's role in protecting personal data amidst AI advancements and its efforts to establish cross-border data protection cooperation within ASEAN. Using a normative juridical research method, this study examines legal aspects, literature, and case studies through conceptual, analytical, and case approaches, analyzing the data qualitatively. Indonesia ensures legal certainty in personal data protection through Law No. 27 of 2022 on Personal Data Protection. Additionally, Minister of Communication and Information Circular Letter No. 9 of 2023 on AI Ethics serves as a guideline for electronic system administrators to implement technology responsibly. At the regional level, Indonesia collaborates with ASEAN countries to address cross-border data protection. It participated in the formulation of the "ASEAN Framework on Personal Data Protection," which provides non-binding guidelines for member countries in drafting national regulations. Despite its non-obligatory nature, this framework's principles influence Indonesia's approach to personal data protection and promote regional cooperation. Through bilateral, multilateral, and regional efforts, Indonesia seeks to enhance data protection and address challenges arising from AI integration in daily life.

Keywords: Artificial Intelligence, Personal Data Protection, ASEAN Framework.

1. Introduction

The need for the latest technology is crucial to support work in various aspects of life. Technology that develops from time to time is increasingly unstoppable. Research and development continues to innovate to find the latest breakthroughs that can help human work. The latest innovation today gave birth to artificial intelligence or Artificial Intelligence (hereinafter abbreviated as AI) which is not only in the field of information technology but also penetrates various fields in human life. AI is designed to help human work so that it can do its work automatically. However, along with the times and technology, AI is starting to be designed to replace the role of humans in carrying out important activities. Even some existing professions are in danger of being replaced by AI. AI can perform certain jobs because the system is equipped with databases and information. The data and information are obtained in various ways, such as databases, data research and processing, data entry, and others.

Obtaining so much data is not necessarily safe for those who own the data. Data protection has been legally recognised, both internationally and nationally. Data protection stems from the right to privacy, which has been globally recognised as a fundamental human right enshrined in international conventions, notably Article 12 of the Universal Declaration of Human Rights and Article 17 of the Covenant on Civil and Po-

Correspondence:
Name: Yanly Gandawidjaja
Email: liely@unpar.ac.id

Received: Jan 09, 2025;
Revised: Jan 17 2025;
Accepted: Jan 31, 2025;
Published : Feb 28, 2025;

litical Rights. Widespread data security is a challenge of today's AI use. It is important to understand in detail which parties have the authority to ensure data protection. It is also important to know how data protection can be done so that data security is maintained. Likewise, the role of the government in carrying out its functions in protecting data security.

In the context of Indonesia as a sovereign state, the state has an important role in protecting the personal data of every legal subject in the country. Although fully sovereign, Indonesia needs an effective strategy to maintain data protection, one of which is through cooperation between countries in the Southeast Asian region (ASEAN). Coordination between national regulations, such as Law No. 27 of 2022, and the ASEAN framework on personal data protection is crucial to ensure alignment of data protection policies at the international level. With a complementary relationship, these two regulations play a role in strengthening personal data protection, not only at the Indonesian domestic level, but also in the broader context of cooperation between ASEAN countries, creating an effective and harmonised data protection system at the national and international levels.

The challenges Indonesia faces in integrating AI ethics into data protection regulations include several complex aspects. One of them is ensuring that AI is not used to make decisions that violate individual privacy rights, such as automated decision-making that can affect a person's basic rights without transparency and accountability processes. In addition, there needs to be clear regulation on how personal data is collected, processed, and stored by AI systems, so as not to violate ethical principles such as fairness, non-discrimination, and openness. This also includes stricter oversight of the use of AI in sensitive sectors, such as health and finance, where the potential for misuse of personal data is great. Thus, Indonesia needs to build a more comprehensive legal framework that prioritises the protection of privacy rights and AI ethics to prevent violations that could harm individuals and society.

2. Materials and Methods

This research is a normative juridical research that aims to analyse and examine legal aspects related to the research topic. The normative juridical approach is used to analyse existing regulations related to personal data protection, as well as identify practical challenges in the implementation of these policies. These challenges often arise due to the mismatch between existing rules and the reality of rapidly developing technology, especially in the use of AI technology that processes large amounts of personal data (Kuner, 2020). Therefore, this approach is important to understand how the law can respond to personal data protection needs in a changing context.

The research is conducted through library research, which includes the study of legal regulations, literature, scientific papers, and other library materials. To collect and analyse data, the research combined conceptual, analytical, and case approaches, which made it possible to investigate existing regulations in depth. Campbell and Glasson caution that no one technique is magically 'right' for all problems. However, in normative legal research, the statutory approach remains an integral part. The data obtained will be analysed qualitatively, including principles, concepts, legal doctrines, and relevant legal rules, which are then described systematically (Bygrave, 2014).

Furthermore, the analysis in this research also includes the cross-border impact of AI technology, especially in the context of trade and personal data security. AI technologies enable the flow of data across national borders, which poses new challenges in legal arrangements that can accommodate these global dynamics. Therefore, this research also explores the role of Indonesia in international cooperation, particularly within the ASEAN framework, to protect personal data. It is important to ensure that countries in

the region have a comprehensive agreement on personal data protection that can respond to the challenges of evolving technology (Chen, 2017; ASEAN Secretariat, 2020).

The main points to be known through this research are: (a) What is the role of the Indonesian state in data protection in the use of AI in daily life? (b) What are the efforts of the Indonesian state in implementing data protection through cooperation between countries in ASEAN?

3. Results and Discussion

3.1 Regulation on Artificial Intelligence and Data Protection

a. Definition of Artificial Intelligence

In terminology, the term Artificial Intelligence is constructed from 2 words. Artificial means made or produced to copy something natural; not real, (2) created by people; not happening naturally; Intelligence is interpreted as the ability to learn, understand, and think logically about things; the ability to do this well. In Indonesian, this term is called "artificial intelligence".

A computer scientist from the United States, John McCarthy stated that Artificial Intelligence is a science and technique in creating intelligent machines, especially in creating intelligent computer programs or applications. AI is a step to create a computer, robot, application, or program that works intelligently, just like a human. Another understanding was put forward by Huang and Rust who stated that Artificial intelligence (AI), manifested by machines that exhibit aspects of human intelligence (HI), is increasingly utilized in service and today is a major source of innovation.

Other definitions are contained through laws and regulations in Indonesia. According to the Circular Letter of the Minister of Communication and Information of the Republic of Indonesia Number 9 of 2023 concerning Artificial Intelligence Ethics, Artificial Intelligence is a form of programming on a computer device to perform careful data processing and/or processing.

From the above understanding, it can be concluded that AI is artificial intelligence in the form of a device created by a system or program that can work automatically based on data and information. The application of AI in several areas of life aims to facilitate human work, in this case for problem-solving, decision-making, machine learning, and optimization, among others. From these things, the use of AI that is often encountered includes the use of chatbots in customer service activities, early diagnosis of diseases in the health sector, and helping business actors conduct more massive and effective marketing in the economic sector.

b. Definition of Data Protection

Data protection carried out by the state is certainly closely related to legal protection. Regarding the elements of legal protection, Rikha Yullina Siagian explains that a form of protection can be entitled to legal protection if it fulfills the following elements: (a) Protection from the government for the community. (b) Providing guarantees of legal certainty from the government. (c) It deals with the rights of citizens. (d) There are sanctions or punishments for those who violate them.

Based on these elements, data protection carried out by the state seeks to fulfill protections for the community, guarantee legal certainty, pay attention to the rights of citizens, and provide sanctions for those who violate it.

In the context of personal data protection, two methods are known to protect personal data, namely, first by securing the physical personal data itself. In addition, the second method that can be taken to protect personal data is through regulations that aim to provide privacy guarantees for using personal data.

Regarding the second method, personal data protection was first used in the 1970s in-laws in Germany, Sweden, and France. The protection of personal data in these countries was solely based on the desire to guarantee the right to privacy of each individual's personal data. With the development of information and communication technology, the scope of regulation expanded to aspects of public administration.

Personal data protection is regulated in Law Number 27 of 2022 concerning Personal Data Protection. As stated in Article 1 number 1 of the Personal Data Protection Law, personal data is data about an individual person that is identified or can be identified separately or combined with other information, either directly or indirectly through electronic or non-electronic systems. Then in Article 1 number 2 of the Personal Data Protection Law, it is stated that Personal Data Protection is an overall effort to protect Personal Data in the series of Personal Data processing to ensure the constitutional rights of Personal Data subjects.

c. Relationship between Artificial Intelligence and Data Protection

Just like a car needs gasoline to start and run, AI needs data to run the installed programming. Data is the most crucial thing for the development and use of AI. AI needs data to do its work. Without data, AI has no basis for learning and analysis. Data collected from various sources are put together in a database which will be processed by AI according to what has been programmed. The large amount of data needed is collected from various sources. In Indonesia alone, the AI database is sourced from government agency data, private agency data, and even the personal data of the Indonesian people.

The data obtained by AI will then be processed and studied so that the learning model or AI program system can make decisions. The more data obtained, the more data that can be learned by AI. The more diverse the data types, the more diverse the data recognition by AI in various situations. These things increase the accuracy and validity of the analysis or decisions made by AI.

In addition to capitalizing on the abundance of data, AI also has data that is always up-to-date. This allows AI to adapt to the dynamics of life. Given that a system must be able to keep up with the times. New data also opens up opportunities for correction of previous things that may be wrong or outdated.

AI and data protection are two distinct concepts, but they are closely connected. The relationship between the data used for AI and data protection is significant. It's crucial to recognize this and take action because data security is essential for our society. If data is widely circulated and used irresponsibly, it can harm the data owner. Therefore, the state must actively fight for and safeguard data protection.

The relationship between AI and data protection can be observed from several aspects, including:

a) Regulation

The use of AI in a country needs to be governed by clear and firm regulations. Ideally, the regulation can guarantee security and protection for data owners used by AI; legal certainty; orderly and responsible use of AI, and; sanctions for those who violate the law.

b) Security and Protection

Security and Protection Protection of personal data ownership used by AI is a key focus of regulation. Personal data accessed over the internet is vulnerable to cybercrime. It's important to ensure the security and integrity of the data. Irresponsible tampering or changes to the data can lead to losses and make data owners victims of crimes like fraud.

c) Ethics

The use of data by AI makes it very easy for humans to do their jobs. The increasing freedom in data usage will make human work easier. However, excessive use of personal data can compromise the privacy of the data owner. Therefore, it is necessary to limit the use of AI in an ethical manner to ensure the maintenance of privacy and security for data owners. The three aspects mentioned above will be explained in more detail below.

d. Legal Basis of Personal Data Protection

Internationally, especially in Europe, data protection is regulated Convention No. 108 on Data Protection, the DP Directive, Directive 97/66/EC (processing of personal data and the protection of privacy in the telecommunications sector), and Directive 2002/58/EC (Directive on Privacy and Electronic Communications) which form the legal umbrella for all personal data arrangements within the framework of the right to privacy recognized in Article 8 of the Europe Convention on Human Right (EHCR) and Article 7 of the Charter of the European Union. In this regard, the realization of this personal data protection is then guaranteed by five basic principles that must be complied with by all parties, namely: (a) Principles of lawful data processing; (b) The principle of special purpose and restriction; (c) Data quality principles; (d) Honest processing principle; and (e) The principle of accountability.

In Indonesia, data protection is included in the human rights guaranteed by the constitution. Article 28G of the 1945 Constitution of the Republic of Indonesia reads: "Everyone has the right to protection of himself, family, honor, dignity, and property under his or her power, as well as the right to security and protection from the threat of fear to do or not to do something that is a human right." This becomes the basis for the government in implementing data protection mandated by the constitution.

In the past, data protection by law carried out in Indonesia was still sectoral. There is no law that regulates data protection in general that covers various fields. For example, data protection under Banking Law focuses on bank and customer secrets. Then the Law on the Eradication of the Criminal Acts of Terrorism, which authorizes interested parties to conduct wiretapping and access personal data of citizens suspected of being involved in terrorism crimes.

Reflecting on the previous statement, it is known that the previous personal data regulation was contained in several laws and regulations, so to increase the effectiveness in the implementation of personal data protection, it is necessary to regulate personal data protection in law. Now Indonesia has Law Number 27 of 2022 concerning Personal Data Protection.

Indonesia as a state of law ensures the existence of laws that regulate all the behavior of its people. The consequence is that every citizen is bound and must obey the applicable regulations. The existence of rules and regulations as legal products provides a guideline for performing the legal acts they regulate. However, in reality, there is no law specifically regulating AI. The dynamic development of technology, including AI, forces the government to immediately launch and realize regulations on AI.

Ethical aspects play an important role in the implementation of artificial intelligence. Awareness of the importance of ethics in the development and application of artificial intelligence in Indonesia continues to increase. Business actors and electronic system providers in the private and public spheres, as stakeholders in the implementation of artificial intelligence, seek to regulate the ethical use of artificial intelligence, including in making decisions that affect the wider community. The development of ethical guidelines for artificial intelligence aims to ensure that this technology is used by considering ethical principles, prudence, and safety, and is oriented towards positive impacts. Ethical guidelines for artificial intelligence are needed to support the effective organization of technology-based activities. These

guidelines are needed to mitigate the impacts and losses that can be caused so that the threat of artificial intelligence can be minimized.

In this regard, in 2023 a Circular Letter of the Minister of Communication and Information of the Republic of Indonesia Number 9 of 2023 concerning Artificial Intelligence Ethics was issued. The purpose of the issuance of this Circular Letter is as an ethical guideline in: (a) Create and formulate internal policies of the Company, Public Electronic System Operators, and Private Electronic System Operators regarding data and internal ethics of Artificial Intelligence; and (b) The implementation of consultation, analysis, and programming based on artificial intelligence is in accordance with the provisions of laws and regulations.

3.2 The Efforts and Roles of States in Data Security Protection Through Inter-State Cooperation in ASEAN

a. Data Protection in Indonesia

Personal data protection is related to information and electronic transactions. Indonesia has Law No. 11/2008 on Electronic Information and Transactions which regulates issues arising from the delivery of information, communication, and/or electronic transactions. This law also governs the evidence and sanctions on legal actions through electronic systems. Along with the need to adjust to the times, the Electronic Information and Transaction Law has been updated twice, namely through Law No. 19 of 2016 and Law No. 1 of 2024 concerning Electronic Information and Transactions.

The first amendment in 2016 emphasized and added provisions, among others, regarding the existence and/or electronic information, the obligation to delete irrelevant information and/or electronic documents, adding the role of the Government in preventing the dissemination and use of Electronic Information and/or Electronic Documents that have prohibited content, changing several provisions regarding investigations related to alleged criminal acts in the field of Information Technology and Electronic Transactions.

Then the second amendment to the law in 2024 added provisions regarding electronic evidence, electronic certification, electronic transactions, prohibited acts, the role of the government, and the authority of investigating Civil Servant Officials. In addition, this law also complements the material that has been regulated in the First Amendment to the law. The regulated materials include digital identity in the implementation of electronic certification, child protection in the implementation of electronic systems, international electronic contracts, and the role of the Government in encouraging the creation of a fair, accountable, safe, and innovative digital ecosystem.

In connection with the additional regulation of personal identity, Article 13A of the Electronic Information and Transaction Law of 2024 states the services that can be provided by electronic certification providers, including: (a) Electronic Signature; (b) electronic seal (c) electronic time marker (d) recorded electronic delivery service (e) website authentication (f) preservation of Electronic Signatures and/or electronic seals; (f) digital identity; and/or (g)n other services that use Electronic Certificates.

Of the services mentioned above, there are electronic signature services and digital identity which are part of personal data. The consequences of organizing the electronic system are found in Article 12 of the Electronic Information and Transaction Law which states that everyone involved in Electronic signatures is obliged to provide security for the electronic signatures they use. Then Article 15 paragraph (1) of the Electronic Information administration and national defense and security.

Related to and Transaction Law also emphasizes that every Electronic System Operator must operate the Electronic System reliably and safely and is responsible for

the proper operation of the Electronic System. Then in paragraph (2) it is explained that the Electronic System Operator is responsible for the operation of its electronic system.

However, the provisions in the Electronic Information and Transaction Law focus more on electronic-based activities. The regulation on personal data protection in this regulation is not very in-depth. Therefore, Law No. 27 Year 2022 on Personal Data Protection was issued. The government has issued Law No. 27 of 2022 on Personal Data Protection as a law aimed at streamlining regulations and making the law a reference for the implementation of data protection. The provisions of this Law are the standard for Personal Data Protection in general, whether processed partially or wholly by electronic and non-electronic means. Each sector can implement personal data protection by its objectives, such as protecting and guaranteeing the basic rights of citizens related to self-protection, guaranteeing public services by Corporations, Public Institutions, International Organizations, and the Government, as well as developing the digital economy and the information and communication technology industry, and contributing to increasing domestic industrial competition.

Referring to Article 3 of the Personal Data Protection Law, data protection in Indonesia is carried out based on: the principles of protection; the principle of legal certainty; the principle of public interest; the principle of expediency; the principle of prudence; the principle of balance; the principle of responsibility; and the principle of confidentiality. In line with the elements of legal protection, below will be described the definition of the principle of protection, the principle of legal certainty, and the principle of public interest.

As written in the Explanation of the Law, the principle of protection is that every processing of Personal Data is carried out by providing protection to the Personal Data Subject for his or her Personal Data and the Personal Data from being misused. The principle of Legal Certainty is that every processing of Personal Data is carried out based on the legal basis to realize Personal Data Protection and everything that supports it so that it obtains legal recognition inside and outside the court. Then what is meant by the principle of Public Interest is that nature upholds Personal Data Protection must pay attention to the public interest or society at large. These public interests include the interests of state the supervision of data protection implementation is mandated in Article 58 paragraph (2) of the PDP Law. The institution is established and responsible to the President. The data protection implementing agency has the task of doing: (a) formulation and determination of Personal Data Protection policies and strategies that serve as a guide for Personal Data Subjects, Personal Data Controllers, and Personal Data Processors; (b) supervision of the implementation of Personal Data Protection; (d) administrative law enforcement against violations of this Law; and (e) facilitation of out-of-court dispute resolution.

The circular states that the implementation of supervision is carried out jointly by the Government, electronic system providers, and users to prevent the misuse and/or use of Artificial Intelligence-based technology that deviates from applicable regulations.

To date, there is no institution established by the President specifically in charge of overseeing the implementation of data protection in Indonesia. Since the promulgation of the Personal Data Protection Law in 2022, until June 2024, no personal data protection supervisory agency has been formed. However, the Ministry of Communication and Information Technology (Kominfo) stated that the Personal Data Protection (PDP) supervisory agency will be formed in mid-2024. Director General of Informatics Applications of Communication and Informatics Semuel Abrijani Pangerapan said the establishment of the PDP supervisory body was a mandate from Law Number 27 of 2022 concerning Personal Data Protection (PDP) which was passed by the government and the House of Representatives in 2022. Semuel said the institution would be independent and directly under the President. However, in the early stages, this institution will coordinate with the Ministry of Communication and Informatics.

When it comes to the use of AI and data protection in Indonesia, there is actually no legal umbrella that regulates the two things simultaneously. Therefore, the Minister of Communication and Information of the Republic of Indonesia issued a Circular Letter of the Minister of Communication and Information Number 9 of 2023 concerning Artificial Intelligence Ethics. The issuance of this Ministerial Circular Letter aims to provide a reference for values and ethical principles for business actors, operators of electronic systems in the public sphere, and operators of electronic systems in the private sphere who have programming activities based on artificial intelligence. The implementation of artificial intelligence is based on ethics and codes of ethics that apply to business actors and electronic system operators (PSE). Implementation of programming skills based on Artificial Intelligence as a support for human activities.

Despite the existence of Circular Letters from relevant ministries, Circular Letters are not statutory regulations, as their content is limited to notification of certain urgent matters. When referring to Article 1 point 43 of the Regulation of the Minister of Home Affairs Number 55 of 2010 concerning Office Manuscripts within the Ministry of Home Affairs, it is stated that a Circular Letter is an official document that contains notification, explanation, and/or instructions on how to implement certain matters that are considered important and urgent. A Circular Letter is also not classified as a statutory regulation, nor is it a legal norm of a statutory regulation. Therefore, a Circular Letter cannot be used as a legal basis to revoke a Ministerial Regulation, let alone other hierarchical regulations. So in a Circular Letter, as known from the basis of policy formulation above, and to explain the meaning of policies that belong to statutory regulations, it is clear and should be in a Circular Letter not regulating sanctions.

A circular letter is more suitable to be understood as a cover letter to deliver a policy product whose substance does not change, does not add, does not revoke the accompanying regulations, so that the accompanying regulations do not change and do not have double meanings due to the circular letter.

Every personal data owner and Electronic System Operator has the right to file a complaint to the Minister if there is a problem or failure in personal data protection. This right is mandated in the provisions of Article 29 paragraph (1) of the Minister of Communication and Information Technology Regulation Number 20 Year 2016 on the Protection of Personal Data in Electronic Systems. The Ministerial Regulation is a regulation that protects the personal data of each individual in the electronic system. This means that the protection provided in the Regulation of the Minister of Communication and Informatics No. 20/2016 on the Protection of Personal Data in Electronic Systems is only limited to personal data accessed through electronic media systems by utilizing internet networks (online). So it can be said, the existence of personal data protection is limited to electronic personal data only.

Referring to Article 64 paragraph (1) of the PDP Law, dispute resolution related to personal data protection can be carried out by arbitration mechanism, court, or alternative dispute resolution institution in accordance with the provisions of laws and regulations.

The sanctions that threaten violators of personal data protection can be in the form of administrative sanctions and/or criminal sanctions. Administrative sanctions may be imposed for violations of the obligations of personal data controllers and personal data processors in the processing of personal data. Those who include the Personal Data Controller and the Personal Data Processor are every person, Public Bodies, and International Organizations. The administrative sanctions in question can be in the form of written warnings; temporary suspension of Personal Data processing activities; deletion or destruction of Personal Data; and/or administrative fines.

Criminal sanctions are regulated in Articles 67-73 of the Personal Data Protection Law. From this article, imprisonment and/or fines are given to every person or corporation that deliberately and unlawfully: (a) obtain or collect Personal Data that

does not belong to him to benefit himself or others that may result in the loss of the Personal Data Subject; (b) disclose Personal Data that does not belong to them; (c) use Personal Data that does not belong to him; (d) create false Personal Data or falsify Personal Data with the intention of benefiting yourself or others that may result in losses to others.

Data protection in the use of AI in human activities is expected to run well as envisioned by the state through the existing regulations. Enforcement, supervision, and dispute resolution efforts regulated through positive law are also continuously intensified and improved. However, in reality, data protection in Indonesia has not run optimally. In June 2024, the Indonesian people were shocked by the news that the National Data Center had been hacked.

The State Cyber and Cryptography Agency (BSSN) revealed that the hacking of the Temporary National Data Center (PDNS) 2 in Surabaya began with an attempt to disable the Windows Defender antivirus. Three days later, the system was breached. Previously, PDNS 2 was said to have experienced a disruption since June 20. This paralyzed a number of public services, including immigration. The cyber incident targeting PDNS is confirmed to be a form of a ransomware attack of the LockBit 3.0 variant. Hinsa said this type of ransomware continues to be developed by hackers and BSSN Spokesperson Ariandi Putra said that disruptions to PDNS have started to occur since June 17. "BSSN found that there was an attempt to disable the Windows Defender security feature which occurred starting June 17, 2024 at 23.15 WIB, allowing malicious activities to run," said Ariandi in his statement, Monday, June 24, 2024.

The perpetrators of the hack are said to have asked for a ransom of USD 8 million or around Rp 131 billion at an exchange rate of Rp 16,399 to the Indonesian government. The hackers declared the money as a ransom for 210 pieces of data to be returned. Ironically, The government says that data belonging to ministries, agencies, and governments affected by cyberattacks on the National Data Center (PDN) cannot be restored. Herlan Wijanarko as the Telkom Director of Network and IT Solution explained that his company has tried to handle the impact of the PDN hack, including recovering data affected by the attack. The handling process is carried out together with the State Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (Kemenkominfo), and the Police.

b. Cooperation of ASEAN Countries in Data Protection

Following Article 62 of the Personal Data Protection Law, Indonesia opens opportunities for international cooperation, both with other governments and international organizations. One structure of international data protection collaboration is carried out in the Southeast Asia region. The context of cooperation with countries in the ASEAN region has been sought. There is a framework initiated and agreed upon by several ASEAN member countries called the "ASEAN Framework on Personal Data Protection".

ASEAN Member States recognise the importance of enhancing personal data protection within and among ASEAN Member States in the digital economy. ASEAN Member States share a common desire to foster closer understanding, information sharing, practice comparison, collaboration, and cooperation activities within ASEAN in the area of personal data protection by the domestic laws, policies, and regulations of ASEAN Member States. Therefore, an agreement was reached in the form of an understanding of the “ASEAN Framework on Personal Data Protection” (hereinafter referred to as the Framework). The Framework aims to strengthen personal data protection in the ASEAN region as well as to facilitate cooperation among participants, with a view to contributing to the promotion and growth of regional and global trade and information flows.

This framework has no binding force (unbinding). This is because the framework is not a regulation, treaty, or agreement. As such, the provisions contained in the ASEAN PDP framework are not mandatory for ASEAN member states to implement. Activities on ASEAN PDP so far have revolved more on sharing experiences in drafting and implementing PDP law at the national level. Related to this, there have actually been efforts to increase political awareness about the importance of this agreement, including by taking the issue to the ASEAN Interparliamentary Assembly in 2018, where one of the recommendations was to encourage ASEAN member countries to increase the exchange of ideas on PDP legislation.

In this Framework, there are several working principles that can be adapted by ASEAN member states into their respective positive laws, namely: (a) Consent, Notification and Purpose; (b) Accuracy of Personal Data; (c) Security Safeguards; (d) Access and Correction; (e) Transfers to Another Country or Territory: (f) Retention; (g) Accountability.

c. Data Protection in ASEAN Countries

The framework contained in the ASEAN Framework on Personal Data Protection is being adapted into several national regulations of ASEAN member states. The personal data protection regulated by countries in ASEAN is as follows:

a) Data Protection Regulation in Malaysia

The protection of personal data in Malaysia is regulated in the Personal Data Protection Act 2010, where the regulation adopts the Principles outlined in the OECD Guidelines as a reference in the personal data principles that have been outlined in the Personal Data Protection Act in Malaysia known as the Personal Data Protection Act 2010. This law expressly regulates the protection of the right to privacy of its citizens. It regulates in detail the principles of personal data protection, the rights of data owners, procedures for transferring data, and obligations for parties who store data. It also regulates a complaint mechanism for someone whose personal data has been transferred illegally.

The Personal Data Protection Act sets out the data protection principles that data users must comply with (equivalent to the data controller in the Personal Data Protection Act 2010, namely: The General Principle; The Notice and Choice Principle; The Disclosure Principle; The Security Principle; The Retention Principle; The Data Integrity Principle; (Data Integrity Principles) and; The Access Principle.

Regarding the supervisory institution in accordance with the provisions of Article 47 paragraph (1) of the PDA 2010, the relevant Minister will appoint a commissioner called the "Personal Data Protection Commissioner" for the purpose of carrying out the functions and authorities given to the Commissioner under the Law with such terms and conditions as may be deemed necessary. The Commissioner has the power to carry out inspections of data protection systems under the PDPA. Furthermore, the 2013 Regulations provide that the personal data system must, at all reasonable times, be open to the inspection of the Commissioner or any inspection officer. During this inspection, documents such as consent and notice forms may be requested, as well as the list of third-party disclosures or any other documentation evidencing compliance with standards issued by the Commissioner, or any other information that the Commissioner may request.

b. Data Protection Regulation in Singapore

Singapore has national laws on data protection, namely the Personal Data Protection Act 2012 and the Info-Communications Media Development Authority Act 2016. Outside

of these two laws, there are also other regulations and derivative regulations related to personal data protection.

The Data Protection Act 2012 is an Act to govern the collection, use, and disclosure of personal data by organizations, and to establish the "Do Not Call Register" and provide for its administration, and for matters connected therewith.

Then the Info-Communications Media Development Authority Act 2016 is a law to establish the Information and Communication Media Development Authority and to make provisions for competition and consumer protection in the media industry.

Personal Data Protection Commission (PDPC) to administer and enforce the Personal Data Protection Act (PDPA). On the other hand, PDPC also has the authority to receive public complaints related to personal data protection issues and facilitate alternative dispute resolution. As the party responsible for monitoring the PDPA, the PDPC is also authorized to impose sanctions if there is sufficient evidence to support it as stated in section 56 of the PDPA. In addition, the Singapore government has also established the Singapore Computer Emergency Response Team (SingCERT) to assist in detecting, preventing, and providing resolution to cyberattacks.

c. Data Protection Regulation in the Philippines

The Philippines has Republic Act No. 10173 or known as the Data Privacy Act of 2012 is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected. This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines, or those who maintain an office, branch or agency in the Philippines.

The provisions of this law also regulate in detail the rights of the owner of personal information (data subject), such as the right to be notified if his or her personal information is being processed, and to be asked for prior consent before his personal information is entered into the system. The law also established the National Privacy Commission as a commission to administer and implement the provisions of the Data Protection Act, and to monitor and ensure the country's compliance with international standards set for data protection. The National Privacy Commission falls under the Department of Information and Communications Technology (DICT).

4. Conclusions

The conclusion obtained after summarising the above explanation, Indonesia, as a state of law, ensures legal certainty in personal data protection through Law No. 27 of 2022 on Personal Data Protection. To address the use of Artificial Intelligence (AI) in supporting human activities, the Minister of Communication and Information issued Circular Letter No. 9 of 2023 concerning AI Ethics as a guideline for electronic system providers to enhance the effective implementation of technology. The state seeks to protect personal data through mechanisms of protection, supervision, and sanctions. Although the establishment of an agency to oversee data protection has been suggested, no such agency has been appointed by the President to date. The Personal Data Protection Law provides administrative and criminal sanctions for violations based on the severity of the offense.

Recognizing that data protection extends beyond national borders, Indonesia, as a member of ASEAN, engages in bilateral, multilateral, and regional collaborations. Notably, it contributed to the formulation of the "ASEAN Framework on Personal Data Protection," which, though non-binding, serves as a guideline for ASEAN countries to draft national regulations. These principles, including those adopted by Indonesia, aim to strengthen regional cooperation in safeguarding personal data amidst AI integration.

References

Andayani Citra, M. E., et al. (2023). *Legal Protection of Personal Data in the Digital Economy Era: Opportunities and Challenges (Comparative Study of Indonesia and Malaysia)*. *Saraswati Law Journal (JHS)*, 5(2).

ASEAN Secretariat. (2020). *Framework on Data Protection and Privacy in the ASEAN Region*. ASEAN Secretariat.

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.

Chen, H. (2017). *International Data Protection Law and ASEAN Cooperation*. Cambridge University Press.

Choirul, G., & Nuswardani, N. (2023). Arrangements for the Protection of Non-Electronic Personal Data in Laws and Regulations in Indonesia. *Journal Inicio Legis*, 4(2), November.

CNN Indonesia. (2024, January 29). *Kominfo Says PDP Supervisory Institution Will Be Formed in Mid-2024*. Retrieved from https://www.cnnindonesia.com/teknologi/20240129132212-192-1055704/kominfo-sebut-lembaga-pengawas-pdp-bakal-dibentuk-pertengahan-2024

CNN Indonesia. (2024, June 26). *PDNS 2 Attacked by Hackers, 3 Services Recovered from a Total of 282 Victims*. Retrieved from https://www.cnnindonesia.com/teknologi/20240626015537-192-1114144/pdns-2-diserang-hacker-3-layanan-pulih-dari-total-282-korban

Circular Letter of the Minister of Communication and Information Technology Number 9 of 2023 concerning Artificial Intelligence Ethics.

Data Guidance. (2024, June 28). *Malaysia - Data Protection Overview*. Retrieved from https://www.dataguidance.com/news/malaysia-pdp-announces-appointment-new-data-protection

Efendi, J., & Ibrahim, J. (2016). *Legal Research Methods: Normative and Empirical*. Depok: Prenadamedia Group.

Hukum Online. (2024, June 26). *Definition of Law: Definition, Elements and Examples*. Retrieved from https://www.hukumonline.com/berita/a/perlindungan-hukum-lt61a8a59ce8062/?page=1

Kompas.com. (2024, June 27). *The Government Calls Hacked PDN Data Cannot Be Returned*. Retrieved from https://nasional.kompas.com/read/2024/06/27/10585431/pemerintah-sebut-data-pdn-yang-diretas-tak-bisa-dikembalikan

Kuner, C. (2020). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

Law Number 27 of 2022 concerning Personal Data Protection.

Ministry of Finance of the Republic of Indonesia. (2024, June 20). *The Principle of Lex Superior Derogate Legi Inferiori and the Position of Circular Letters in Legislation*. Retrieved from https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/15099/Asas-lex-superior-derogate-legi-inferiori-dan-Kedudukan-Surat-Edaran-dalam-Perundang-undangan.html

Natalia, S., Kezia, L., & Baasir, H. N. (2023). Consumer Privacy and Data Protection: Policy Perspectives and Comparative Studies. *Nusantara: Journal of Social Sciences*, 10(6).

Oxford Learner's Dictionaries. Retrieved from https://www.oxfordlearnersdictionaries.com/

Philippines Republic Act No. 10173 (Data Privacy Act of 2012).

Tampubolon, T. M., & Ramadhan, R. A. (2020). ASEAN Personal Data Protection (PDP): Realizing Digital Personal Data Security in Southeast Asia. *Padjadjaran Journal of International Relations (PADJIR)*, 1(3), January.

Tempo.co. (2024, June 26). *Facts of the National Data Center Torn apart by Ransomware Hackers: 210 Affected Agencies*. Retrieved from https://bisnis.tempo.co/read/1883963/fakta-fakta-pusat-data-nasional-diobok-obok-hacker-ransomware-210-instansi-terda

mpak

Wahyudi, D., Sumigar, B. R. F., & Setianti, B. L. (2016). *Personal Data Protection: Proposed Policy Institutionalization from the Perspective of Human Rights*. Jakarta: Institute for Community Studies and Advocacy (ELSAM).

Huang, M. H., & Rust, R. T. (2018). Artificial Intelligence in Service. *Sage Journals*, 21(2). Retrieved from https://journals.sagepub.com/doi/full/10.1177/1094670517752459