WHAT SHOULD INDONESIA LEARN FROM RIGHTS TO DATA PRIVACY UNDER THE GDPR?

Nadine Arieta Ravinka, Fakultas Hukum Universitas Udayana,
e-mail: nadine12ravinka@gmail.com
I Gusti Ngurah Parikesit Widiatedja, Fakultas Hukum Universitas Udayana,
e-mail: parikesit_widiatedja@unud.ac.id

doi: https://doi.org/10.24843/KS.2022.v10.i03.p09

ABSTRACT

Right to data privacy is determined as a fundamental right and shall be protected. The increase of data misuse is an urgent need to legitimize the data protection law. Unfortunately, Indonesia still does not have a comprehensive law regulating personal data protection. This article applied normative legal research methods that draw on statutory and comparative approaches. This article aimed to present the comparison between the GDPR and Indonesia's PDP Bill by analysing both provisions on data privacy rights. The article indicated that, in the non-existence of comprehensive personal data protection law, the acts carried by the government are not enough to safeguard the data privacy of Indonesia's citizens. Moreover, there are some deficiencies of the PDP Bill compared to the GDPR. It lacks the substance of the fundamental principles of data protection. This article recommends, in order to strengthen and harmonise personal data protection, the government should take proper measures to legalize the personal data protection law immediately which comprises data protection principles in line with international standards.

Keywords: Data Privacy, Right to Privacy, Personal Data Protection Law.

1. Introduction

1.1 Background

The advancement of information and communications technology (ICT) today has brought harmony with the media and telecommunications. The utilization of ICT in different fields brings advantages to civilization, but on the other side, it also presents an adverse impact when it comes to law enactment. Personal data privacy breach is one of the issues that arise due to ICT usage. Various services in electronic devices in the form of applications, often involve collecting and storing the users' personal data, especially when registering an account. The impact of digitalisation perceived by users in the terms of contracts which are standard clauses that must be agreed upon before using the platforms. The contract approval process is not conventionally anymore because there is an advanced standard terms and conditions (T&C) of the contract which is often inequitable, it leads to an imbalance between the company's obligations and user's rights. In addition, most users ignore the privacy policy on the platforms before approving the contract.[1] Nevertheless, most applications

[1] Millencia Ang, "Consumer's Data Protection and Standard Clause in Privacy Policy in E-Commerce: A Comparative Analysis on Indonesia and Singapore Law". *The Lawpreneurship Journal* 1, no. 1 (2021): 100-113. https://journal.prasetiyamulya.ac.id/journal/index.php/TLJ/article/view/523, 101.

might not provide sufficient protection around the data they collect, leaving users with less privacy which may threaten user privacy.

Right to privacy is owned by a person which covers personal information that cannot be submitted or possessed by all parties without owner consent.[2] Individuals need to have tools to exercise their right to privacy, restrain harmful data practices, protect their data from abuse and data exploitation. Especially that we are now heavily relying on digital services, it is getting harder to keep our data secure. Since data volume is growing exponentially in the digital era and data leaks happen more frequently than ever before.[3] It is requisite to provide a sufficient legal framework to assure individuals have strong rights with their data and mitigate interferences to the right of privacy. A strong data protection law shall provide a legal framework to empower individuals rights to know how their personal data being processed and used, by whom, when, and why, to gain details on which data is stored, for what purpose and to request the removal in case the purpose is not given anymore.[4]

There have been significant increases in most countries around the world that have stipulated regulations of data protection. For instance, the European Union (EU) countries have the General Data Protection Regulation (*hereinafter* GDPR), which is one of the toughest privacy and personal data protection law that reflected the new digital era and has also become the world's benchmark for regulation of privacy protection. Meanwhile, by now Indonesia does not yet have regulations specifically regarding personal data. Indonesia personal data protection regulations are dispersed in various regulations under several ministerial regulations. These rules become ineffective because the application of the law could mess up with the overlap of the existent rules.[5] The major issue with the weakness of personal data protection laws is that there is no legal protection to handle the legal problems related to personal data abuse. Nevertheless, the Indonesian Government has initiated Indonesia's Personal Data Protection (hereinafter PDP) Bill since 2016 which has prepared by the Ministry of Communication and Information (MoCI) and it is still being finalized by the House of Representatives.

The PDP Bill is introducing new key roles, data ownership rights, data transfer rules and other serious changes for Indonesia data protection legislation. The PDP Bill will become the first comprehensive personal data protection law in Indonesia, not only through electronic systems but also non-electronically. However, the bill's provisions are still inadequate especially in the aspect of the right to data privacy protection. Therefore, the PDP Bill is urgently needed because data is a commodity in this digital era. It might help to ensure legal certainty to the evolving technological and economic conditions in this era of digitalization. Moreover, the PDP Bill is also

---

[2] Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia". Fiat Justitia Jurnal Ilmu Hukum 12, no. 3 (2018): 206-223. https://doi.org/10.25041/fiatjustisia.v12no3.1312, p 207.

[3] Long Cheng, dkk, "Enterprise data breach: causes, challenges, prevention, and future directions". *John Wiley & Sons, Ltd,* (2017): 1-14. https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1211, p 1.

[4] Privacy International. "The Keys to Data Protection, A Guide for Policy Engagement on Data Protection," 2018, https://privacyinternational.org/.

[5] Fenty U Puluhulawa, dkk, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (2020): 182-200, https://doi.org/10.33756/jlr.v2i2.6847, p 186.

necessary to be revised in adjusting with international standards in personal data privacy protection.

1.2 Problems

The first issue to be discussed in this article is the comparison between Indonesia's PDP Bill and the GDPR concerning data privacy as known to be a fundamental right. The second issue is, what measures should the Indonesian Government undertake in protecting individuals' data privacy rights?

1.3 Purpose

This article is aimed to analyse the comparison between the GDPR and Indonesia's PDP Bill by analysing both provisions concerning data privacy rights. In addition, it will analyse the potential measures by which the Government of Indonesia should undertake in strengthening personal data privacy protection.

2. Method

This article was the normative legal research that relied on statutory and comparative approaches. The statutory approach is used to review and analyze relevant legal instruments while the comparative approach is used to examine and compare regulations relating to personal data protection specifically the GDPR and Indonesia's PDP Bill. This article uses various sources of law that consist of primary and secondary sources. The technique of collecting legal materials is through the literary study will be based upon both national and international legal instruments, textbooks, journals, and online websites.

3. Result and Analysis

3.1. The Significant of Personal Data Protection as a Fundamental Right

3.1.1. How Does the Protection of Data Privacy Become a Fundamental Right?

According to Warren and Brandeis in the article "The Right to Privacy" published in the 1890 Harvard Law Review, privacy was defined as the right to be alone and the right to enjoy life and this legal development was inevitable and required legal recognition. Daniel Solove in his book entitled "Understanding Privacy", opines there are six common types of privacy, which are limited access to the self; the right to be alone; control over personal information; secrecy; intimacy; and personhood.[6] In view of the extensive use and exploitation of personal data create situations wherein personal data can simply become a vast public consumption. The problem of personal data protection happens to be a significant concern and becomes crucial. The protection of personal information is continuously more essential since personal data might be misused and also may harm data owners' rights.[7]

The protection of privacy has been recognized as a fundamental aspect to protect an individual's freedom, freedom of expression, privacy and personal dignity. The concept of data protection came from the right to privacy which is often linked and

---

[6] Kristopher A. Nelson, "Daniel Solove's Six General Types of Privacy." 2011, https://inpropriapersona.com/daniel-soloves-six-general-types-of-privacy/.

[7] Shinta Hadiyantina, dkk. "The Indonesia Government Authority of Privileged Access the Personal Data Protection in Digital Era, Personal Data Protection in Digital Era", p. 101. https://hukum.ub.ac.id/wp-content/uploads/2018/09/Conference-SHT.pdf.

both are instrumental in safeguarding and supporting fundamental rights.[8] Personal data privacy is a right of the individual as a data subject. It allows individuals to determine their use of personal data and to protect information and prevent it from being disseminated. Therefore, law enforcement is needed to robust personal data protection in legal form that makes certain safety in the use of the electronic systems on digital platforms. Comprehensive data protection law is essentials for protecting human rights in this digital age, mostly the right to privacy.[9] The legal order must guarantee respect for personal dignity. Data protection law seeks in protecting personal data by providing individuals on how to exercise data protection rights and require the public or private sector that perform the processing of their data to respect these rights.[10]

3.1.2. International Legal Frameworks of Privacy Rights and Personal Data Protection

Freedom of privacy in international instruments is known as a fundamental right inherent to all human beings. Right to privacy is stipulated in the Universal Declaration of Human Rights (UDHR), which provides the legal basis for its members with regard to the state's commitment to respecting and protecting the rights of individuals.[11] Article 12 of the UDHR proclaims that "No one will be subjected to interferences arbitrarily with his privacy, family, home, or correspondence, nor to assaults upon his honour and reputation. Every person has entitled to the law protection towards attacks or interferences." The International Covenant on Civil and Political Rights (ICCPR) has been established as the basis of the major international human rights treaties by the UDHR, which provides for enhanced protection of human rights. In Article 17, it proclaims that no one shall be treated unlawfully or arbitrarily in intervention with personal matters, home, family, or correspondence, nor to unlawful attacks upon his or her reputation and honour. While the UDHR is not legally binding, the ICCPR presents as a normative ground for the development of domestic laws by giving authority to each country to create legal instruments to protect their nation.[12]

There are a few international instruments of personal data protection are created with agreed-upon codes, decisions, practices, policy instruments and recommendations, examples are: (1) CETS 108, its purposes are to protect individuals and regulate the personal data cross border-flow; (2) The OECD Privacy Guidelines, that aims to promote respect for privacy as a foundational value and simultaneously create safeguards guidelines to enable personal data across borders' flow. It establishes data protection principles, those are data quality, use limitation, collection limitation, purpose specification, openness, accountability, security safeguards, individual participation; (3) The Asia-Pacific Economic Cooperation Privacy Framework. It covers principles of data protection consisting of integrity preventing harm, collection limitation, choice, notice, personal information usage, personal information integrity, accountability, security safeguards, access and correction. Moreover, it presents

---

[8] European Data Protection Supervisor. Data Protection. https://edps.europa.eu/data-protection_en.

[9] Human Rights Watch. "The EU General Data Protection Regulation." 2018, https://www.hrw.org/news/.

[10] European Data Protection Supervisor, loc.cit.

[11] Rudi Natamiharja, *Op.Cit*, 208-209.

[12] Rudi Natamiharja & Stefany Mindoria, "Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN", LPPM UNILA, (2019). http://repository.lppm.unila.ac.id/10613/, p 8.

implementation guidelines to set the effectiveness of privacy protections, ensure economic growth and continue trade in the Asia Pacific.

3.1.3. The General Data Protection Regulation (GDPR)

Europe is consistently at the forefront of privacy standard settings worldwide. The GDPR is a regulation established in the EU regulating provisions regarding data privacy compliance requirements for organisations which located inside and outside the EU. It has been enforced since 25 May 2018 and replaced the EU Directive 1995. It marked the third generation of data protection and it has had a direct effect on all the EU states.[13] The establishment of the GDPR was an emphasis from the EU Charter of Fundamental Rights, determining that all EU citizens have personal data protection rights.[14] It specifically seeks to enhance personal data protection across the EU, strengthen current challenges concerning privacy rights and personal data, and encourage the digital economy of the EU. The GDPR aims to limit abusive interference with individuals' data privacy, which in the end will protect several other human rights.[15]

The GDPR territorial scope requires organisations worldwide that perform personal data processing of the EU citizens to comply with its provisions, whether the processing occurs in the Union or not.[16] It also provides two conditions for non-EU companies that might be subject to this law. First, when the processing of personal data is related to individuals in the EU and concerned with the offering of services or goods to the EU citizens, whether that offers free or paid. Second is when a non-EU company monitors the behaviour of the EU citizens in the EU territory.[17] For example, if there is an organization located outside the EU that stores and processes personal data of the EU citizens, then those activities remain subject to the GDPR.[18] However, if the entity is not located in the EU, does not provide services or goods to the EU citizens, and does not control the behaviour of the EU citizens, then, it will not comply with the GDPR.[19]

3.1.4. Processing of Personal Data

Personal data in the GDPR is described as all information related to identifiable or an identified natural person especially with reference to an identifier, for example, name, identification number, online identifier, location data, to one or more aspects specific to the genetic, mental, economic, physical, cultural or social identity of this natural person.[20] Moreover, the GDPR differentiates kinds of personal data that consists of (1) General personal data, including personal data for instance name, phone

---

13 Haristya, S., dkk. *Preliminary Study: A Comparison of Indonesia's Personal Data Protection Bill with Europe's Convention 108+ and General Data Protection Regulation* (Jakarta, Tifa Foundation, 2020), p 9.

14 Ori Setianto, dkk. "Legal Application of the Right to Data Portability in Peer to Peer (P2P) Lending in Indonesia." *Jurnal Legalitas* 13 no. 2 (2020): 103-114. https://doi.org/10.33756/jelta.v13i2.8476, p. 108.

15 Human Rights Watch, *loc.cit.*

16 The GDPR, Art. 3 (1).

17 *Ibid,* Art. 3(2).

18 Ori Setianto, dkk. *loc.cit.*

19 Edward S. Dove, "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era." *The Journal of Law Medicine & Ethics* 46, no. 4 (2018): 1013-1030. https://doi.org/10.1177%2F1073110518822003, p 1019.

20 The GDPR, Art. 4(1).

number, home address, email address, IP address, location data and personal data that are combined for identification. They are factual information that is often publicly available; (2) Specific personal data is personal data requiring special protection, relating to information and health data, genetic data, biometric data, financial data, criminal record, political orientation, life or sexual orientation, child data, and any other data in compliance with the prevalent laws. These types of data are very sensitive and confidential, hence need to be more protected and guarded. Further, the GDPR establishes that personal data inclusive of special categories are allowed to be processed for the public interest. However, these exceptions come with several safeguards to ensure the protection of data subject, because processing specific categories of sensitive data are very tightly regulated.[21]

The definition of personal data processing is all activities cover the collection, storage, recording, structuring, use, transfer, dissemination, disclosure, restriction, and destruction or deletion of personal data. To fulfill its provisions, the GDPR has tightened the rules on the liabilities of both controller and processor. Personal Data Controller (PDC) is a public entity, legal person, or other body whether, alone or jointly with others, who makes decisions on the purpose of personal data in compliance with the laws of the Member States.[22] When a controller processes personal data, it must take appropriate actions so the data subjects' rights are fulfilled. The GDPR also complements further mechanisms to assure the controller takes action in responding to the data subject's request.[23] The GDPR emphasizes the controllers' obligation to deliver information to data subjects, including to notify any personal data breach to their national supervisor authority. Furthermore, Personal Data Processor (PDPr) is a public authority, a legal person, or other organization that processes personal data in the name of the controller.

3.1.5. Data Protection Principles

The GDPR is underpinned by data protection principles to provide the liabilities that organisations must comply with when they collect, manage, and process the personal data of individual and achieve its compliance. Article 5 establishes data protection principles that consist of (1) Lawfulness, fairness, and transparency, defines the processing of personal data shall be in a lawful, fair and transparent way; (2) Purpose limitation, personal data shall be stored only for a certain, legitimate, and explicit purpose for as long as it is needed to accomplish the purpose; (3) Data minimisation, the collection of personal data shall be precise, relevant and not excessive to what's needed to fulfil a specific purpose; (4) Data accuracy, refers to personal data shall be kept current, accurately, correctly and not misleading; (5) Storage limitation, the maintenance of personal data shall be in the form that authorizes data subjects identification for the necessary purpose of the processing of personal data; (6) Integrity and confidentiality, the processing of personal data shall be in a way of ensuring appropriate protection, inclusive of protection towards unlawful or unauthorized processing and accidental loss, damage or destruction, applying proper technical measures; (7) Accountability, the controller shall have the responsibility to provide records and give a demonstration of compliance with data protection principles.

[21] *Ibid*, Art. 9.
[22] *Ibid,* Art. 4(7).
[23] Haristya, S., dkk, *op.cit*, 16.

3.1.6. Data Subject's Rights

The GDPR regulates the processing activities for the benefit of data subjects explained in chapter 3. The fundamental of data subjects rights under the GDPR are: (1) Right to be informed, refers to individuals have entitled to be informed of the storing and processing of personal information in clear language, understandable and accessible form; (2) Right of access defines the data subjects have right to acquire and receive information of the personal data being processed by the controller; (3) Right of rectification, individuals reserve the right to request the rectification of incorrect or incomplete personal information; (4) Right to erasure, refers to the right of data subjects to request the deletion of their personal information on certain circumstances without undue delay, for instance, the data is no longer needed or the data is processed unlawfully; (5) Right to restriction, data subjects have entitled to ask the controller to limit the processing of personal data; (6) Right to data portability, individuals reserve the right to reuse their personal data through various services safely and securely without any obstacle that affects its usability; (7) Right to object, data subjects have entitled to oppose their personal information being processed and to ask the controller not to process them at all; (8) Rights related to automated decision-making that includes profiling, data subjects have entitled not to be the subject of any decision-making, without human involvement, such as profiling.

3.2. Domestic Regulations of the Privacy Rights and Personal Data Protection

The idea of personal data protection in Indonesia implicitly is originated on Article 28G paragraph (1) of the Constitution of the Republic of Indonesia 1945, stating that every person shall have the right to protection of themselves, honour, family, dignity, and property, have the right to feel safe against and receive protection from the threat to do or not do something that is a human right. Apart from constitutional protection, Indonesia has ratified the ICCPR within Law No. 12 of 2005, which also emphasizes the Indonesian Government's obligation to protecting the personal and data privacy of its citizens. Conforming to Law No. 39 of 1999 regarding Human Rights, Article 29 stipulates the admission of everyone's rights to protect personal, family, opinion, honour, property, and dignity rights wherever they are.

Other existing regulations in Indonesia regulate the personal data protection to prevent data abuse that might infringe upon data owner and may cause losses such as defamation. In the information and telecommunication field, several laws regulate personal data protection related to personal information confidentiality. For instance, Law No. 36 of 1999 (Telecommunications Law) in Article 40 stipulates that any individual shall not conduct an unlawful interception of information channelled through telecommunications networks in any form. Another provision in the electronic systems is Law No. 19 of 2016 on Electronic Information and Transactions (EIT Law). Referring to Article 26 paragraph (1) any transfer of an individual's personal data must obtain the data owner's approval first due to the prohibition of personal data arbitrary transfer.

Based on the EIT Law, the Government of Indonesia has enacted the Government Regulation (GR) No. 71 of 2019 on the Implementation of Electronic System and Transactions. It involves stronger stipulations of personal data protection information and website authentication. It also affirms the necessity for the government to prohibit any disadvantage to public interests through the misapplication of transactions and

electronic information and the need to develop a national cybersecurity strategy.[24] GR No 71 of 2019 adds more provisions concerning personal data processing, which is the right to be forgotten. The purposes are to remove certain electronic information and electronic document that is deemed irrelevant from search engines. However, GR No 71 of 2019 only covers cyber-crimes related to electronic transactions, such as data abuse, the spread of malicious viruses and codes, and unauthorised electronic signatures.

MOCI Regulation No. 20 of 2016 on Personal Data Protection, provides measures to safeguard the personal information use in electronic systems. It establishes that personal data is specific personal information kept, maintained, protected by its secrecy, and safeguarded by the truth (Article 1). Moreover, Article 2 paragraph (1) determines that personal data protection in electronic systems include protection of the collection, acquisition, storage, appearance, processing, announcement, analysis, transmission, destruction and dissemination of personal data. It also regulates data owners' rights which consist of the confidentiality of their data, the right to complain, allowed to access and acquire personal data historical and right in requesting the destruction of their specific personal data (Article 26).

3.3. The Progress of Indonesia's Regulations on Data Protection and Privacy

3.3.1 General Review of Indonesia's Personal Data Protection Bill

The Government of Indonesia has been preparing the draft of the Personal Data Protection Bill, which its materials are more or less adopted from the GDPR. The PDP Bill consists of 15 chapters and 72 articles, regulating a large range of matters from general provisions, personal data types, data owners' rights, data collection and storage, data processing, controllers and processors responsibilities, the appointment of data protection officer, acknowledging stakeholder's rights and obligations, community role, international cooperations, transitional provisions, exclusion towards personal data protection, resolution of the dispute, closings provisions, administrative and criminal sanctions, and more. It aims to protect all personal data belonging to Indonesian citizens, processed both electronically and manually. The range of subjects' cover individuals, corporations, or institutions under Indonesia's legal jurisdiction, where their actions are outcome in legal consequences in Indonesia's territory or affect Indonesian citizens whether inside and outside of Indonesia territory. The scope will follow the extraterritorial jurisdiction principle, which applies to every person, public institution or organization that performs legal actions as stipulated in this law and has legal consequences whether within inside or outside of Indonesia's jurisdiction.[25]

The PDP Bill defines personal data as all data related to identifiable natural person, which can be identified directly or indirectly through electronic systems and non-electronic or in combination with other information. This definition mirrors the definition in the GDPR. In this Bill, personal data is divided into: (1) General personal data consisting of full name, citizenship, religion, gender and any personal data that combine to enable identification; (2) Specific personal data is personal data that involves special protection, including health data, sexual orientation, genetic data, political orientation, biometric data, child data, criminal records, financial data, and

[24] Noor Halimah Anjani, "Cybersecurity Protection in Indonesia". Centre for Indonesian Policy Studies, Policy Brief No. 9, (2021). https://www.cips-indonesia.org/, p 4.

[25] The Draft Personal Data Protection Bill of Indonesia 2020 (the Draft of PDP bill), Art. 2.

other data that complies with applicable regulations and laws. [26] However, the Bill defines people as persons or corporations, which does not specifically distinguish people as a person or an individual under the law, because people might be persons or corporations. This definition requires more explicit criteria of personal or individual categories and a clear division of scope to distinguish between household data processing activities with other and commercial data processing activities. This unclear distinction would potentially put individuals who retain or process data for personal purposes or household activities under the law's purview.[27]

There are four parties regulated in the PDP Bill, consisting of (1) Personal Data Owner (PDO), is data subjects who have personal data attached to them; (2) Personal Data Controller (PDC), is a public entity that establishes the purpose and supervises the personal data processing; (3) Personal Data Processor (PDPr) is an individual, public entity, as well as an organisation that processes personal data under the PDC's responsibility; (4) Third-party consists of each person, public entity, or any other party whose obtained authorization from PDC or PDPr for processing personal data. The PDP Bill grants PDO a full extent of rights to be in charge of their personal data. Those rights include the right to request access; right to be informed; right to rectification in incomplete and inaccurate personal data; right to erasure; right to withdraw consent; right to choose or not choose to process based on pseudonymization; right not to be subject to a decision based on profiling or automated individual decision-making; right to delay or limit processing; right to sue and request compensation in any case of infringement of personal data under the law. Both PDC and PDPr will be required to observe and respect these rights. Hence, the PDP Bill outlines the obligations of PDC and PDPr specifying the necessary information and mechanisms for the workability from the data subject's consent.

The PDP Bill establishes the processing activities that PDC must undertake, as follows: notify the PDO of any changes to the information declared in the consent without undue delay; maintain record, update, correct inaccuracies or errors in personal data in 24 hours after receiving the request; supervise processor and ensure the processing is in line with the consented purpose; accountability for processing activities in compliance with the regulations; personal data processing termination by 3x4 hours after the request is received; breach notification to the PDO and MoCI by 3x24 hours of the occurrence takes place.[28] Conversely, the PDPr has a legal duty for any data processing activities, on the condition that the PDPr performs under the instructions of the PDC and complies with the requirements of the Bill.[29] Other obligations of the PDPr are the rectification, accuracy, and alignment of personal data processing with the purpose agreed by the data owner; providing the confidentiality and consistency of personal data; keeping a record of the processing; preventing unauthorized processing and invalid access of personal data; supervising all relevant parties; notify the offence of personal data to the data owner and the MoCI; show compliance and exemptions to the liabilities of the processor.[30]

---

[26] *Ibid,* Art. 3.

[27] Haristya, S., dkk, *op.cit*, 12.

[28] The Draft of PDP Bill, Art. 24 – 42.

[29] *Ibid*, Art. 43.

[30] Yohanes Hermanto Sirait, "General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa." *Gorontalo Law Review* 2 no. 2 (2019): 60-71. https://doi.org/10.32662/golrev.v2i2.704, p 68.

3.3.2 The Urgency of Indonesia's Personal Data Privacy and Protection Law

Regulations on the GDPR and Indonesia's PDP Bill does have resemblances since the GDPR is one of the references to personal data protection. Indonesia is leaning toward the GDPR's objective approach due to the non-existence of law in Indonesia that particularly protects individuals' personal data privacy. Indonesia personal data protection regulations burst apart responsibilities across different ministries which remain ineffective in overcoming data breaches and data abuses. Those ministerial regulations are still beneath the law whereas many regulations that establish personal data protection are designed in the legislation form. Other than the existing ministerial rules, however, there is still an urgent need for the enactment of law at the legislation level especially in personal data protection and privacy to ensure legal certainty, justice, and expediency.[31]

Indonesia Personal Data Protection Bill aims to regulate personal data processing in Indonesia. It is expected to establish data security and sovereignty as fundamental for data protection and to acquaint important obligations whether for the owners or users.[32] Despite that, the Bill is still unclear when it will be issued and promulgated as law. As a result, the measures carried by the Indonesian Government are not enough to prevent personal data abuse. Many of the Bill's provisions lack sufficient details, particularly on data subjects' rights, data protection principles, international data transfers and also, it does not include the fundamental data protection principles which are data protection by design, by default and data protection impact assessment (DPIA), therefore it is not specific enough concerning the liabilities of data controllers and processors.[33] Those principles require PDC and PDPr to take appropriate actions to ensure personal data protection since those principles are seen as necessary to safeguard data processing. Therefore, the Bill contains significant gaps compared to the GDPR in the lack of data protection by design, by default and DPIA, which are fundamental to ensuring that privacy and data protection is a core of data collection and use, including in digital innovation technologies.[34]

Moreover, the Bill lacks providing clarity details of the Data Protection Authority (DPA) to enforce the law. The Bill has not established an independent authority, organization, or regulatory institution in charge of protecting personal information based on applicable law. The Bill only stipulates the enforcement of personal data protection that will be executed by the government through MoCI without further explanation of its roles, competencies, tasks, or powers.[35] This is considered controversial as the MoCI is a public body that will be subject to this law. It could potentially cause conflict with interests related to its management of personal data.[36] Due to this absence, it brings up the question of how to monitor the enforcement of the law when it is enacted.[37] Thus, the supervisory authority should rest with an independent commission. The absence of clarity on the powers and roles of the DPA, might bring serious implications on its capabilities to ensure the controllers and processors are held accountable. For instance, the authority must be able to verify data

---

[31] Fenty U Puluhulawa, dkk, op.cit, 197.
[32] Onetrust DataGuidance. "Indonesia Data Protection Overview." (2020). https://www.dataguidance.com/.
[33] Haristya, S., dkk, *op.cit*, 3.
[34] *Ibid*, 19.
[35] *Ibid*, 22.
[36] *Ibid.*
[37] *Ibid*, 10.

controllers' and processors' consent mechanisms, security of processing, the activities record of processing, and protection of data subject's rights are all in accordance with Bill's provisions. Further, the law is likely to be inadequately enforced, with the risk that it will be ignored by both controllers and processors.

Even though an essential feature to ensure legal certainty and consistency in data protection is the creation of an independent DPA. The effective implementation of data protection rules depends on oversight and enforcement by DPA. The DPA's decision-making must be independent of any direct or indirect external influences. Its presence can help to strengthen the position of individuals in fundamental rights. It might also gain citizens' trust and provide an accessible point of contact to answer individual queries and handle their complaints without having lengthy and costly proceedings.[38] In the absence of the DPAs roles on monitoring data processing, however, there are several authorities in specific sectors such as Bank of Indonesia whose monitors data protection in the banking sector, Financial Services Authority (OJK) controls personal data regarding financial, the Ministry of Health maintains personal data concerning medical record, and etc.[39]

3.3.3 The Measures of the Indonesian Government Should Undertake

Before the PDP Bill is legitimized, the Indonesian government shall carry out proper measures to ensure the enactment of comprehensive data protection law within policies and practices in international legal standards on privacy and data protection, review legislation and improve the privacy rights protection in compliance with international human rights standards. The PDP Bill needs to be revised distinctly define and delineate the roles, responsibilities, and authorities of relevant institutions in handling personal data processing. In addition, the Bill should give more extensive obligations on data controller and processor by recognising the principles of data protection by design, by default and DPIA to ensure the entities in monitoring data processing effectively.

Furthermore, The Government of Indonesia must consider the establishment of an independent DPA who acts to perform as a supervisor in performing the PDP law, that could lead the enforcement efforts, to conduct investigations, act on complaints, follow up on reports and execute administrative sanctions if they detect violations of the law.[40] Last but not least, The Government of Indonesia should socialize, provide knowledge and raise understanding about the importance of privacy and data protection to citizens also understandings the potential risks and the right to protect the privacy of personal data, also empower all citizens to comply with the law when it is enacted. Law enforcement will rely on the knowledge and active role of individuals to protect their data. It would help Indonesia to thrive in the era of digital transformation and economic growth along with protecting the rights of individuals as it is fundamental.

---

[38] Antoine Schweitzer-Chaput, "Independent Data Protection Authority Matters." The Jakarta Post. 2021. https://www.thejakartapost.com/.

[39] Arfi Azahri, "Legal Review of Consumer Law Protection on Personal Data on Digital Platform." *Indonesian Private Law Review* 2, no. 1 (2021): 59-71, https://doi.org/10.25041/iplr.v2i1.2189, p 69.

[40] Rudi Natamiharja, *op.cit*, 220-221.

4. Conclusion

Based on Indonesia's existing personal data regulations, it proves that Indonesia lacks comprehensive regulations on the protection of personal data. Too many rules on data protection make those regulations ineffective and inefficient because it has no comprehensive law which protects its citizen from data misuse. As data usage and processing becomes more widespread, there is an increasing urgency to push the finalization of comprehensive personal data protection to ensure legal certainty. Comprehensive and consistent data protection regulation is a key tool for both governments and companies in today's world, as a part of the protection against cyber risk, and to answer the growing concerns of citizens. However, Indonesia's PDP Bill has not entirely enough referred to the personal data protection principles. Compared to the GDPR, the Bill contains significant gaps due to the lack of data protection by design, by default and DPIA, which are fundamental for ensuring that privacy and data protection is a core of data collection and use, including in digital era. As well, the deficiency of clarity upon provisions concerning the authority of supervisory. In the absence of data protection authority, the law may potentially not be sufficient and might affect the implementation that causes risks. The details of fundamental data protection principles, accompanied by, sufficient data protection requirements are needed to be added. Moreover, there need to be further provisions to ensure fair, transparent, and lawful data processing with the fulfilment of data controller and processor liabilities under the compliance, and the obligation to manage the personal data confidentiality. Finally, the most important thing is to raise public awareness to disseminate information and improve knowledge of how important is data privacy.

REFERENCES

Books

Haristya, S., dkk. *Preliminary Study: A Comparison of Indonesia's Personal Data Protection Bill with Europe's Convention 108+ and General Data Protection Regulation*. Jakarta: Tifa Foundation, 2020.

Journals

Ang, M. "Consumer's Data Protection and Standard Clause in Privacy Policy in E-Commerce: A Comparative Analysis on Indonesia and Singapore Law." *The Lawpreneurship Journal* 1 no. 1 (2021).

Azahri, A. "Legal Review of Consumer Law Protection on Personal Data on Digital Platform." *Indonesian Private Law Review* 2 no. 1 (2021).

Dove, E. S. "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era." *The Journal of Law Medicine & Ethics* 46. (2018).

Long Cheng, dkk, "Enterprise data breach: causes, challenges, prevention, and future directions". *John Wiley & Sons, Ltd,* (2017).

Natamiharja, R. "A Case Study on Facebook Data Theft in Indonesia." *Fiat Justitia Jurnal Ilmu Hukum* 12 no. 3 (2018).

Puluhulawa, F. U., dkk. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2 no. 2 (2020).

Sirait, Y. M. "General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa." *Gorontalo Law Review* 2 no. 2 (2019).

Setianto, O., dkk. "Legal Application of the Right to Data Portability in Peer to Peer (P2P) Lending in Indonesia." *Jurnal Legalitas* 13 no. 2 (2020).

Articles

Anjani, N. H. "Cybersecurity Protection in Indonesia." Policy Brief No. 9, Centre for Indonesian Policy Studies. (2021). https://www.cips-indonesia.org/

Hadiyantina S, dkk. "The Indonesia Government Authority of Privileged Access the Personal Data Protection in Digital Era." Personal Data Protection in Digital Era. https://hukum.ub.ac.id/wp-content/uploads/2018/09/Conference-SHT.pdf

Natamiharja, R. & Mindoria, S. "Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN." LPPM UNILA. (2019). http://repository.lppm.unila.ac.id/10613/

Privacy International. "The Keys to Data Protection, A Guide for Policy Engagement on Data Protection." (2018). https://privacyinternational.org/

Website:

Schweitzer-Chaput, A. Independent Data Protection Authority Matters. The Jakarta Post. https://www.thejakartapost.com/academia/2021/06/08/independent-data-protection-authority-matters.html, the Jakarta Post, 2021. Accessed September 15, 2021.

Human Rights Watch. The EU General Data Protection Regulation. https://www.hrw.org/news/, 2018. Accessed October 12, 2021.

European Data Protection Supervisor. Data Protection. https://edps.europa.eu/data-protection_en.

Nelson, K. Daniel Solove's Six General Types of Privacy. https://inpropriapersona.com/daniel-soloves-six-general-types-of-privacy, in propria persona, 2011. Accessed August 20, 2021.

Yuriutomo, I. D. Indonesia Data Protection Overview. https://www.dataguidance.com/. OneTrust DataGuidance, 2020. Accessed September 14, 2021.

International Instruments

Universal Declaration of Human Rights
International Covenant on Civil and Political Rights
The European Union General Data Protection Regulation

National Legal Instruments

The 1945 Constitution of the Republic of Indonesia
Law of the Republic of Indonesia No. 39 of 1999 regarding Human Rights
Law of the Republic of Indonesia No. 36 of 1999 regarding Telecommunications
Law of the Republic of Indonesia No. 19 of 2016 regarding Electronic Information and Transactions
Regulation of Minister of Communications and Informatics of the Republic of Indonesia No. 20 of 2016 on Personal Data Protection