Indonesia's Personal Data Protection Law: Highlights and Challenges to the Businesses and Society

Unggul Sagena, Technology and Society Researcher
University of Indonesia

Introduction

On 20th September 2022, Indonesia's house of representatives officially passed the Personal Data Protection bill (PDP Law No. 27/2022) [1] [2] which become Indonesia's first comprehensive law to specifically deal with the issue of data privacy. Indonesia is the 5th country in Southeast Asia after Singapore, Malaysia, Thailand and the Philippines to have regulations on PDP [3]. Based on the European Union General Data Protection Regulation (EU GDPR), the PDP Law is expected to better regulate and protect personal data, especially in the current situation where massive data leaks of users on business platforms [4] and personal data are intentionally leaked to the public on social media [5]. The digital economy industry will change, align and adapt to the provisions of the PDP Law which is the main standard for managing and processing personal data in Indonesia. Several issues related to data and the digital economy will impact business practices and challenge the whole of Indonesia's digital society.

Contents Highlights

PDP Law provides a universal primary regulation to maintain and regulate the protection of the personal data of the Indonesian people, wherever their data is located. The definition of personal data according to the PDP Law is "data about individuals who are identified or can be identified separately or in combination with other information, either directly or through electronic or non-electronic systems" [6]. This law, which consists of 16 chapters and 76 articles, regulates matters relating to individual personal data. What is regulated, among others, are the rights of each individual to whom personal data is attached, provisions for processing personal data and the obligations of the controllers of such personal data, institutions in the form of supervisors/personal data protection authorities, as well as the implementation of prohibitions and sanctions.

According to the PDP Law, there are 4 parties to the processing of personal data, which is adapted from the EU GDPR [7]. First, personal data subject; an individual to whom personal data is attached. Second, personal data processor; any person, public body, and international organization acting individually or jointly in processing personal data with/on behalf of the personal data controller, Third, personal data controller; any person, public body and international organization acting individually or jointly in determining the objectives and exercising control over the processing of personal data. Processing of personal data can be carried out by 2 (two) or more personal data controllers but must meet the minimum requirements, such as; there is an agreement, there are interrelated

objectives, and/or there is a jointly appointed contact person. Fourth, personal data supervisory body/authority. Different from the EU GDPR which has an independent data protection authority, the government will establish a personal data protection authority directly under the President [8].

In terms of processing data, a lawful ground added to the consent bases should be expressed explicitly, either in writing or recorded, manually or electronically. PDP Law recognises lawful grounds for processing personal data, namely for (i) fulfilment of contractual obligation, (ii) fulfilment of the legal obligation of the controller, (iii) protection of vital interest of the data subject, (iv) conduct of duty for public interest, public service or lawful authority of the controller as well as (v) the fulfilment of other lawful interest(s).

Challenges to Business and Society

As impacts, there are challenges for businesses and society after the enactment of the PDP Law that can be noted. First, PDP Law mandates data protection officers (DPO) and the implementation of a data protection impact assessment (DPIA). Businesses should appoint a DPO whenever personal data is processed for public interest, any systemic monitoring of personal data on a large scale and any large-scale processing of specific and/or crime-related personal data [9]. Mitigation of data privacy breaches makes businesses have to invest more in digital security resources. DPIA should be implemented and assisted by DPO to ensure any 'high risk' processing of personal data. However, it is not clear which scale is “high-risk” and how DPO is important in every business. DPO and DPIA should be clarified in the following implementing regulation issued by the government, to ensure the requirements and conditions to implement the necessity of DPO and DPIA. This is a serious challenge for MSMEs and startups that have limited resources because the PDP Law does not clearly distinguish the scale of business entities.

Second, the “extraterritorial” policy [10] and data transfer policy require companies and institutions holding data for Indonesian citizens based abroad to comply with all the rules of the PDP Law. This policy, particularly related to data storage will attract more foreign companies to enter potential Indonesia's consumer market. Before the PDP law, foreign companies were required to have a data centre located in Indonesia. Foreign companies now can settle their business in Indonesia while maintaining abroad data centres, which can be established in a lower operating costs country. This incentive facilitates the entry of goods and services from abroad through digital services belonging to foreign companies. With a more competitive environment of business, the Indonesian business community needs to be more vigilant.

The data transfer policy of the PDP Law also has the potential to further liberalize Indonesia's data governance. Similar to EU GDPR, cross-border transfer of personal data must comply with requirements such as the receiving country of the personal data has a similar or higher level of personal data protection, or if it is not, the data can be transferred offshore by the assurance of legally binding instrument to protect personal data, or data controller has obtained consent from the data subject. PDP Law allows for personal data

transfer by a controller within and outside the Indonesian territory. Especially for cross-border personal data transfer, the personal data controller must ensure that the receiving party's country has an equal or better personal data protection standard. If not, then the personal data controller must ensure an adequate and binding effort for personal data protection. If both conditions are not met, then the controller must obtain consent from the relevant personal data subjects. Companies should carefully manage their digital security more than before because the sanctions are not only administrative but also criminal. Data breach, if occurs should be notified as written notice within 72 hours to the data subject (users of company services) and the data protection authority.

Third, administrative and criminal sanctions. The PDP Law enforce strict action against companies that fail to comply with the PDP Law. On that account, companies operating in Indonesia or dealing with Indonesian residents' data should adopt a proactive approach to identifying and resolving any potential challenges to comply with the PDP Law. In contrast to the EU GDPR, PDP Law specifies administrative and criminal sanctions, depending on the type of violation. The administrative fine is a maximum of 2 per cent of the annual income or annual revenue for the violation variable [11].

For businesses, the only punishment that can be imposed on the corporation is a fine sanction which is a maximum of 10 (ten) times the maximum penalty imposed. In addition to being sentenced to a fine, companies may be subject to additional penalties in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts; freezing of all or part of the company's business; permanent prohibition from performing certain actions; closing all or part of the place of business and/or activities of the company; carry out obligations that have been neglected; payment of compensation; license revocation; and/or dissolution of the company [12]. However, every person in charge of the company can also be subject to criminal charges. Criminal sanction is imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp. 6,000,000,000.00 (six billion rupiah). As well as the seizure of profits, payment of damages and other sanctions against corporations violating the PDP Law provisions [13].

Fourth, the absence of distinction between types of companies causes every business entity including Micro, Small, and medium enterprises (MSMEs) and startups that have a low understanding of personal data protection to be subject to heavy fines. The PDP Law is also a law that creates high-cost consequences for companies doing business. Human capital investment in digital security, recruitment of DPOs and efforts to purchase technology for data security require financial resources. Although the rules regarding data centres can be circumvented by streamlining infrastructure networks abroad, not all companies have the same capacity.

Fifth, The PDP Law specifically regulates the processing of personal data of children and persons with disabilities. However, there are no details on the implementation of child data processing specifically. In addition, civil society highlighted the exclusion of sexual orientation and political views from the categorization of specific personal data in the PDP Law, which has the potential to cause discrimination against gender minority groups in Indonesia and the use of data for political purposes ahead of the general election in 2024.

Children's data is also categorized as specific data [14], where explicit consent is required, while children are still in the hands of the parents.

Sixth, civil society urged the PDP Law to be revised to address at least 10 criticisms raised by NGOs who are members of the Personal Data Protection Advocacy Coalition (KA-PDP) [15]. Including the concern over the lack of “independent” data protection authority because DPA is directly under the President and will be established at maximum 6 months from the enactment of the PDP law.

Conclusion

Even though PDP law has major impacts on business and society, the existence of the PDP Law is very important. It is a legal guideline for the protection of personal data in the digital ecosystem. Business and socio-cultural practices in the context of the digital era will then pay attention to the context of data protection due to various consequences. Criticism of several regulatory aspects of this law should be accommodated and used as inputs in making government regulation a technical derivative of the PDP law provisions, and also a major consideration for future revisions. Government regulation that will follow the law must clarify the details of how businesses and society further comply with the PDP law.

The challenging transitional period of 2 years after the PDP law enactment provides space and time for all stakeholders to comply and align with the PDP law. Within a given period, the government must focus on ensuring companies and public bodies comply with PDP Law. Companies must also conduct an internal assessment of their data protection compliance and adjust their relevant practices/policies to adapt within the transitional period given. In parallel, government and civil society organizations must ensure that all levels of society understand the changing behaviour requirement to adapt to the PDP law. Society’s current digital culture which lacks awareness of children's data-sharing, and lacks education about the importance of protecting own data, may inadvertently violate this law in the future.

References

[1] https://www.reuters.com/world/asia-pacific/indonesia-parliament-passes-long-awaited-data-protection-bill-2022-09-20/
[2] https://opengovasia.com/indonesia-approves-personal-data-re7gulations/
[3] https://conventuslaw.com/report/key-changes-in-data-privacy-and-cyber-security-laws-across-southeast-asia-in-2022/
[4] https://restofworld.org/2022/indonesia-hacked-sim-bjorka/
[5] https://safenet.or.id/2021/06/the-rise-and-challenges-of-doxing-in-indonesia/
[6] Article 1, paragraph 1, PDP Law No 27/2002
[7] https://gdpr.eu/what-is-gdpr/
[8] https://teknologi.bisnis.com/read/20220921/84/1579773/ini-tugas-lembaga-pengawas-perlindungan-data-pribadi-di-bawah-presiden
[9] https://www.nortonrosefulbright.com/en/knowledge/publications/31bce8f0/highlights-of-indonesias-personal-data-protection-law
[10] Article 2, paragraph 1, PDP Law No 27/2022
[11] Article 57 paragraph 3, PDP Law 27/2022
[12] https://www.hukumonline.com/berita/a/ancaman-sanksi-administratif-hingga-pidana-dalam-uu-pelindungan-data-pribadi-lt633c69ce2de5c?page=2
[13] Article 67-68, PDP Law 27/2022
[14] Article 4, paragraph 2, PDP Law 27/2022
[15]https://www.tifafoundation.id/artikel/siaran-pers-koalisi-advokasi-ruu-pelindungan-data-pribadi-ka-pdp/