CIPS
Center for Indonesian Policy Studies

POLICY BRIEF

March 2021

Policy Brief No. 7

Data Privacy in the Indonesian Personal Data Protection Legislation

by Gliddheo Algifariyano Riyadi

Key Messages

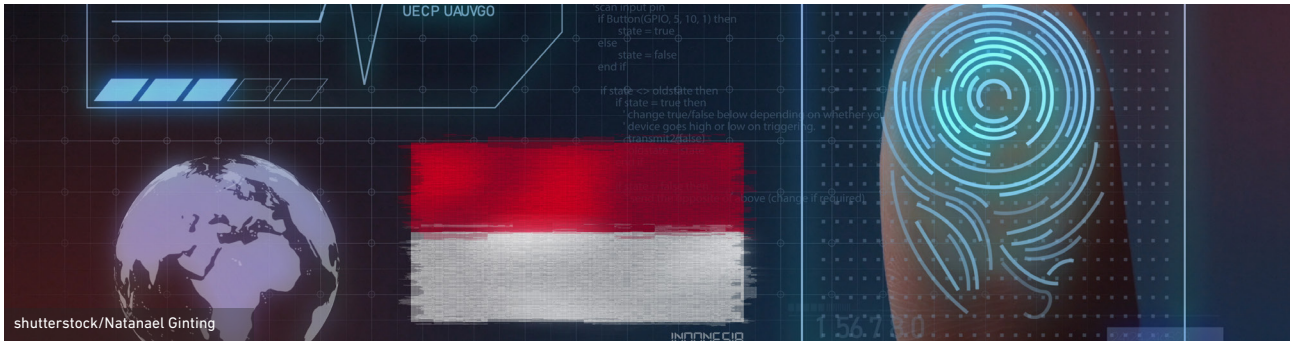
- From e-lending to personalised business recommendations, there is a growing supply of customized digital services that require companies to acquire, process and store personal data. Meanwhile, these data remain the property of individuals and their owners have the right to control and manage their own data.
- The Indonesian House of Representatives is deliberating a Personal Data Protection Bill initiated by the Ministry of Communication and Informatics (MOCI). The draft Bill grants data owners a full range of rights to control and manage their personal data. It makes companies responsible for demonstrating compliance.
- The Bill suspends the rights of data owners in case their data are needed for national defense and security, law enforcement, state administration, supervision of the financial or monetary sector, payment systems, or financial system stability. These exemptions provide the government with unrestrained access to personal data. There should be specific definitions and limitations to government access, mandating transparency on the purpose of the exemption and the period of data storage.

- The PDP Bill should follow a risk-based approach. High risk areas should be those involving systematic and extensive activities to profile individuals, to process special categories of data, and to monitor publicly accessible areas. Those who plan to engage in these activities should have to consult with the supervisory authority in Indonesia before conducting the activity. They need to conduct a detailed privacy impact assessment and notify potentially affected individuals in the case of a data breach.

- The supervisor authority for data privacy should rest with an independent commission. The draft PDP Bill, however, foresees the supervisory function by a government line ministry, which can cause conflicts of interest.

- Since digital service companies constantly need to innovate, they often face uncertainties whether they are in breach of data privacy regulations. To mitigate this risk, the government should consider implementing a regulatory sandbox to facilitate the compliance of new technologies with existing data privacy regulations, and to co-create new policies similar to the Singaporean Personal Data Protection Commission (PDPC) when it tested and amended Singapore's PDP Act.

The Importance of Personal Data Protection



There is a substantial difference between data security and data privacy. Data security refers to keeping private and sensitive data safe from intrusion, hackers or malicious insiders (SNIA, 2019). Data privacy involves specific approval and notification procedures as well as other regulatory obligations in data management. It protects the right to privacy of individual consumers and companies (Petter, 2019). Both data protection and privacy are considered parts of personal data protection.

Personal data privacy is a right of individual data subjects. It refers to the purpose of data collection and processing, privacy preferences and the way organizations manage personal data. National regulations on data privacy usually focus on how to collect, process, share, archive and delete data (Ameed & Natgunanathan, 2016).

As a right owned by everyone without exception, personal data privacy allows individuals to determine the use of their personal data. Data owners have the right to allow data managers to process and use their data. When doing so, data owners need to have the legal right to request information about their own digital identity, the purpose of requesting and using their personal data, and the organisation that is requesting the data (Tourkochoriti, 2016). The EU General Data Protection Regulation (EU GDPR) 2016/679 also stipulates that only adequate and relevant data should be processed by data managers, while the amount of data should be limited to what is necessary for the purpose that was initially agreed with the data owner (Drake, 2016).

As a new international benchmark for personal data privacy, EU GDPR defines personal data in Art. 4 (1) as any information that is related to an identified or identifiable natural person. They allow the identification of these natural persons by their name, an identification number, location data, or an online identifier. Personal data

also include information that reveals the physical, physiological, genetic, mental, commercial, cultural or social identity of a data owner. Among these general categories there are particularly sensitive personal data. They receive a higher level of protection in EU GDPR Art. 9 because of their importance for the data owners. Sensitive personal data include genetic, biometric and health data, information about racial and ethnic origins, political opinions, religious or ideological convictions, as well as their engagement in public affairs (GDPR, 2018).

The ownership of personal data is crucial in the digital era. Every individual is requested to submit personal data when using online services, buying products online, registering an email account, making a doctor's appointment, paying taxes, signing a contract etc. These personal data are often collected without the knowledge of the individual and by companies or agencies that do not interact directly with that person (Privacy International, 2013). Their data can then be used without allowing owners to hold those parties accountable and for processes that data owners have not explicitly agreed to. Consent in every data sharing activity is a crucial feature of data privacy (Jiska, 2016).

The exponential growth of the digital economy in Indonesia increases the urgency to legally protect the privacy of data. By 2025, the digital economy is expected to contribute USD 100 billion to the national economy and to become the largest digital economy power in ASEAN (Rosadi, 2018).

This growth should be accompanied by the protection of the privacy of personal data. While this would increase the trust in the digital economy (Butarbutar, 2019), it does not appear to influence the behavior of digital consumers. A survey by Mastel and APJII in 2017 found that 79% of respondents in Indonesia objected to having their personal data transferred without permission and 98% supported the passing of a Personal Data Protection Law (UU PDP). In practice, however, Indonesian consumers seem little concerned with the use of their personal data. A study found that users fail to study or understand the privacy policy of companies whose services they use, including the terms and conditions that relate to the use of their personal data (Reynaldi & Tifana, 2020).

While European companies operating in Indonesia ought to comply with EU GDPR, because it includes the activities of European companies outside the EU, many Indonesian companies inadequately protect personal data in their internal policies and procedures (Reynaldi & Tifana, 2020). Many of them also maintain a low understanding of the concept of data privacy and consumer data protection.

Meanwhile, Indonesia does not yet have a consistent legal framework for data privacy. Rules and obligations are currently scattered in at least 32 different laws and regulations (Aprilianti, 2020). Discrepancies between those regulations impede their enforcement (Nugroho, 2020). The Electronic Information and Transactions (EIT) Law No. 19/2016 and the Population Administration Law No. 24/2013, for example, have contradicting classifications of general and sensitive data.

The Indonesian Constitution protects the citizens' right to privacy in Article 28 G (1). However, this constitutional guarantee has yet to be properly regulated in a law (Djafar, Sumigar, & all, 2016). The Indonesian House of Representatives (DPR) is currently deliberating a Bill on Personal Data Protection (PDP Bill) in order to effectively protect personal data of Indonesian citizens, and because other countries require the protection of data in their trade relations with Indonesia (Djafar & Wahyudi, 2020).

The Ministry of Communication and Informatics (MOCI) started drafting the PDP Bill in 2014 and submitted it to parliament in 2020 (Karunian, 2020). There were at least four dialogue sessions in 2020 between the parliament and academics, the Indonesian e-commerce association (idEA), the Indonesian Financial Technology Association (AFTECH), the PDP Advocacy Coalition, and MOCI (Rizkinaswara, 2020). In those sessions and hearings, the government attempted to accommodate the views of the industry and other stakeholders in the drafting process. The PDP Bill was included in the 2020 National Legislative Agenda and originally targeted for completion in November 2020. At the end of that year deliberations had not been concluded and the DPR was not able to pass it into law.

Contentious Items of the PDP Bill Drafted by MOCI and the DPR

Several parts of the PDP Bill remained contentious and prevented the passing of the PDP Bill into law.

- The draft PDP Bill opens government access to personal data
- The PDP bill provides exceptions where consent of data owners is not required to access their personal data:
    - national defence and security
    - law enforcement processes
    - supervision of the financial services sector
    - stability of the monetary order, payment and financial systems
    - public interest in the administration of the country

The government is required to provide clear reasons when it wants to access personal data. In matters of national defense and security, there needs to be an urgency for the government to access the data. If courts grant their permission, the government also has the right to access personal data in law enforcement processes.

Allowing the government to access personal data of citizens bears the risk of data being used for political and even economic interests (Greenleaf, 2017). This may not happen during the current administration but it opens opportunities for future administrations that can extract information about individuals without their consent.

In this context, a new regulation by Statistics Indonesia (BPS) on Governing Data Collection is also of importance. At the beginning of 2021, the draft regulation mandated that companies must provide data to BPS as a government agency. BPS does not collect any personal data and therefore the authority of BPS to collect data was also not listed among the consent exemptions in the PDP Bill. Instead, the regulation authorises BPS to collect data, such as company identity (name, license, etc.), number of users (aggregate and per region), number of employees, revenues, transaction values, and payment methods. The BPS Regulation is scheduled to be published and take effect in February 2021. It needs to remain clearly understood that BPS, as the key government data center, will only have access to general corporate data. Data privacy needs to be protected and BPS should refrain from collecting personal data of corporate customers. Companies should retain the right of refusing to submit such data.

Similar to the PDP Bill, Article 23 of the EU GDPR also includes special purposes for which governments of EU member states can pass laws that allow government agencies to access personal data. Under the restriction that a law "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" a national law can void the right to data privacy in matters such as national defence and public security, law enforcement, monetary, budgetary and taxation matters, public health and social security. However, the same article of the EU GDPR also clearly states that such laws must specify the purpose of the data processing, the categories of data accessed, the scope of restrictions, the safeguards to prevent abuse of unlawful access or transfer of data, the storage periods of the data, the right of the data owner to be informed about the restriction etc. (GDPR, 2018).

In the case of the Indonesian PDP Bill there needs to be a guarantee that, after the government has accessed personal data, these data will not be used for any other than the specified purposes and are not leaked to the public. Governments of many countries struggle to protect the privacy of personal data. In Indonesia, personal data of the Directorate General of Population and Civil Registry of the Ministry of Home Affairs (Dukcapil) were sold

at various prices and in tailor-made packages on the website friendmarketing.com. According to news reports, the arrested perpetrator was found with data from 50,854 families, including 1,162,864 Single Identify Numbers (NIK), 761,435 cell phone numbers, 129,421 credit card numbers and 64,164 account numbers (VOI, 2020).

A risk-based approach needs to be applied to the protection of data privacy

Sanctions in the PDP Bill fall into administrative and criminal categories. Administrative sanctions start with a written warning, followed by a temporary suspension, compensation for the mishandling of personal data, and administrative fines. Criminal provisions in the PDP Bill make violators of data privacy subject to criminal prosecution.

The imposition of sanctions in the PDP Bill follows after it has been determined that an individual person or an institution has violated the privacy of personal data. However, adjustments need to be made to the draft PDP Bill to specify the level of supervision and the severity of the sanctions depending on the volume of data violated and the harm done by the non-compliance.

Following the practice of the French data protection authority, CNIL, the PDP Bill should request from those who plan to manage personal data to first identify the harm that can potentially occur from processing the data. Controllers then need to evaluate the severity of the harm and assess the vulnerabilities of their systems and operations. According to a white paper by the International Association of Privacy Professionals (IAPP), the EU GDPR also follows a risk-based approach to compliance. It may not be explicitly stated in the regulation, but the concept determines the criteria for the assessment of penalties for non-compliance that causes physical, material or moral damage to data owners. Harmful consequences are considered particularly grave when data owners experience "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage." (Maldoff, 2016).

Following the example of the EU GDPR, the PDP Bill also needs to distinguish between the levels of risk emanating from data processing activities. High risk areas should be those involving systematic and extensive activities to profile individuals, to process special categories of data, and to monitor publicly accessible areas. Those who plan to engage in these activities should have to consult with the supervisory authority in Indonesia before conducting the activity. They need to conduct a detailed privacy impact assessment and notify potentially affected individuals in the case of a data breach.

PDP Bill put supervisory authority to a government line ministry

The PDP Bill foresees the establishment of a supervisory authority for data privacy. Articles 58 and 59 state that this role will be carried out by the government through the Ministry of Communications and Informatics (MOCI). This is regarded as controversial because MOCI is a public institution that will be subject to this law because it processes personal data. If MOCI oversees the enforcement of data privacy, its regulatory and supervisory authorities may potentially conflict with interests related to its own management of personal data.

The PDP Bill should, instead, establish an independent authority for personal data protection, which acts as the supervisory authority in the process of implementing the PDP Bill. Singapore, for instance, has established an independent institution that oversees PDP affairs in accordance with the applicable law is Singapore. The Personal Data Protection Commission (PDPC) acts independently when overseeing personal data management of government and private institutions. The United Kingdom has also assigned duties and powers to oversee data privacy to an independent institution. The Information Commissioner's Office is a non-departmental public body that reports directly to the UK Parliament (Information Commissioner's Office, 2018a).

Innovative Ways to Develop An Adequate Data Privacy Law

In the fast-evolving digital economy, companies are under constant pressure to innovate. They need to update their products and services, their user interface and their interaction with their customers. Modern management techniques, like agile and scrum, are indicative of the need for companies in the digital economy to respond faster and more effectively to the changing marketplace. The fear of missing out and succumbing to their competition is accompanied by the risk that new data processing tools and applications are in breach of data privacy regulations. It is therefore necessary to develop data privacy policies and regulations that do not hold companies back from innovating.

A suitable tool is a regulatory sandbox, which helps liaising between government regulators and private sector actors in creating an appropriate regulatory framework that is open to innovation. Originally developed in the financial sector, regulatory sandboxes enable firms to test innovative products, services or business models while being exempted from some regulatory obligations. The relevant authorities waive the application of certain administrative provisions and apply their discretionary power with the intention to enhance innovation. This allows firms to test their innovations and comprehend supervisory expectations, while government authorities gain insights into new technologies during the testing stage so they can swiftly adjust their regulatory supervision (Taylor Wessing LLP, 2020). Indonesia does have some experience applying regulatory sandboxes. Bank Indonesia (BI) issued BI Regulation No. 22/23/PBI/2020 on Payment Systems that provides the framework for the role of BI in stimulating innovation through regulatory sandboxes to test regulations and policies governing new innovations (Suleiman, 2021).

The Information Commissioner's Office in the UK applied a regulatory sandbox to the protection of personal data privacy. The so-called beta phase of its technology strategy 2018- 21 planned to invite around 10 organisations from the private and public sectors to support data privacy and innovation. From July 2019 to September 2020, these organisations were meant to address the use of personal data in emerging or developing technology, complex data sharing, building good user experience and public trust by ensuring transparency and clarity of data use, and other specific data protection challenges (Information Commissioner's Office, 2018b). The pharmaceutical company Novartis, for example, participated in the sandbox to identify data privacy risks when using voice applications in a clinical setting, and what they are supposed to undertake to address those risks (Business at OECD, 2020).

Closer to home, from an Indonesian perspective, Singapore applied a regulatory sandbox when it revised the country's PDP Act (Monetary Authority of Singapore, 2019). Singapore's Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) involved six data contributors in testing and validating concepts that involved the sharing of public and private data. Under a Trusted Data Sharing Framework, the regulatory sandbox started with an engagement phase where companies provided their plans to innovate involving the use of data. If this phase could not give them the needed assurance that they were compliant with existing regulations, then IMDA/PDCP provided guidance to reduce the uncertainty regarding the innovation. Finally, if those concerns were still not adequately addressed, then regulators and companies engaged in the co-creation of new guidance or a new policy as an amendment to the law. As Singapore was updating its Personal Data Protection Act and drafted relevant guidelines, Facebook collaborated with IMDA in a regulatory sandbox project. As part of the Facebook Accelerator - Singapore project, the sandbox sought the guidance from regulators and industry experts when working with startups to co-create new ways how notice and dynamic consent can be implemented in innovative products and services (Business at OECD, 2020).

Experiences in Singapore and the UK provide lessons for the process of drafting data privacy regulations and the PDP Bill in Indonesia.

References

Ameed, M., & Natgunanathan. (2016). Protection of big data privacy. *IEEE access*, 1821-1834.

Aprilianti, I. (2020). *Protecting People: Promoting Digital Consumer Rights*. Retrieved from: https://www.cips-indonesia.org/digital-consumer-rights-pp27

Butarbutar, R. (2019). Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia. *3rd International Conference on Law and Governance* , 154-163.

Business at OECD (BIAC). (2020). Regulatory Sandboxes for Privacy Analytical Report, November 2020. Retrieved from: https://biac.org/wp-content/uploads/2021/01/Final-Business-at-OECD-Analytical-Paper-Regulatory-Sandboxes-for-Privacy-1.pdf

Central Bank of Indonesia. (2017). Frequently Asked Questions: Peraturan Anggota Dewan Gubernur No.19/14/-ADG/2017 tentang Ruang Uji Coba Terbatas (Regulatory Sandbox). Retrieved from: https://www.bi.go.id/elicensing/helps/FAQ%20REGSAND.pdf

Desy, S. (2020). MOEC Denies 1.3 Million Employee Data Leaks. Retrieved from: https://katadata.co.id/desysetyowati/digital/5ece8096d6625/kemendikbud-bantah-1-3-juta-data-pegawainya-bocor

Djafar, W., Sumigar, F., & all, e. (2016). *Perlindungan Data Pribadi di Indonesia: Ulasan Pelembagaan Dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM Press.

Drake, G. (2016). Navigating the Atlantic: understanding EU data privacy compliance amidst a sea of uncertainty. *S. Cal. L. Rev., 91*, 116-128.

GDPR. (2018). Regulation (EU) 2016/679 (General Data Protection Regulation) version OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. Retrieved from: https://gdpr-info.eu

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Indonesia and Turkey*, 10-13.

Information Commissioner's Office. (2018a). About Information Commisioners Officers. Retrieved from: https://ico.org.uk/about-the-ico/

Information Commissioner Office. (2018b). *Sandbox beta phase: Discussion Paper*. Retrieved from: https://ico.org.uk/media/2614219/sandbox-discussion-paper-20190130.pdf

Jiska, C. (2016). The spy next door: Eavesdropping on high throughput visible light communications. *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*.

Karunian. (2020). *Kawal Pembahasan RUU Pelindungan Data Pribadi, Koalisi Advokasi RUU PDP serahkan usulan DIM Alternatif kepada DPR RI*. Retrieved from: https://elsam.or.id/kawal-pembahasan-ruu-pelindungan-data-pribadi-koalisi-advokasi-ruu-pdp-serahkan-usulan-dim-alternatif-

Maldoff, Gabriel. (2016). The Risk-Based Approach in the GDPR: Interpretation and Implications. *White Paper by the International Association of Privacy Professionals (IAPP)*. Retrieved from: https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

Monetary Authority of Singapore. (2019). *Overview of Regulatory Sandbox*. Retrieved from: https://www.mas.gov.sg/development/fintech/regulatory-sandbox

Nugroho, A. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding* 7.7, 183-189.

Petter, J. (2019). *Data Privacy Guide: Definitions, Explanations and Legislation*. Retrieved from: https://www.varonis.com/blog/data-privacy/

Privacy International. (2013). *A Guide for Policy Engagement: Part 1 Data Protection Explained*. Retrieved from https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf

Reynaldi, F., & Tifana, N. (2020). *Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Perlindungan Data Pribadi.* Universitas Padjajaran Press.

Rizkinaswara, R. (2020). *DPR telah Adakan Rapat Dengar Pendapat Umum terkait RUU PDP*. Retrieved from: https://aptika.kominfo.go.id/2020/07/dpr-telah-adakan-rapat-denger-pendapat-umum-terkait-ruu-pdp/

Rosadi, S. (2018). Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia.". *Brawijaya Law Journal 5.1* , 143-157.

SNIA. (2019). *What is Data Privacy?* Retrieved from: https://www.snia.org/education/what-is-data-privacy

Suleiman, A. (2021). Improving consumer protection for low-income costumers protection in P2P lending. *Center for Indonesian Policy Studies Policy Paper*. Retrieved from: cips-indonesia.org/publication

Taylor Wessing LLP. (2020). Regulatory Sandboxes. Retrieved from https://www.lexology.com/library/detail.aspx?g=419b7b84-bde0-4c29-bb63-41df2aa3d0b1

Tourkochoriti, I. (2016). The Snowden revelations, the Transatlantic Trade and Investment Partnership and the divide between US-EU in data privacy protection. *University of Arkansas at Little Rock Law Review 36*, 161-176.

VOI. (2020). *We are Personal Data That is Sold and Purchased, 4 Aug 2020*. Retrieved from: https://voi.id/en/tulisan-seri/10237/we-are-personal-data-that-is-sold-and-purchased

ABOUT THE AUTHOR

Gliddheo Algifariyano Riyadi was a research trainee in CIPS' Emerging Policy Leaders Program. He currently works as an Organization and Governance Analyst at National Public Procurement Agency (LKPP). Prior to joining CIPS' program, Gliddheo worked as Research and Policy Analyst at Regional Autonomy Watch (KPPOD). He graduated with a bachelor's degree in Political science from the University of Indonesia in 2019.

CIPS
Center for Indonesian Policy Studies

The Center for Indonesian Policy Studies (CIPS) is dedicated to providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

As a strictly non-partisan and non-profit think tank, CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allow Indonesia to prosper.

Center for Indonesian Policy Studies

contact@cips-indonesia.org

Jalan Terogong Raya No. 6B Cilandak,
Jakarta Selatan 12430, Indonesia

www.cips-indonesia.org

Our works relies on your support. Visit **www.cips-indonesia.org/donate** to support CIPS.