ISEAS YUSOF ISHAK INSTITUTE

ISSUE: 2023 No. 75

ISSN 2335-6677

PERSPECTIVE

RESEARCHERS AT ISEAS – YUSOF ISHAK INSTITUTE ANALYSE CURRENT EVENTS

Singapore | 22 September 2023

What Can We Expect of Indonesia's PDP Law?

*Yanuar Nugroho and Sofie Syarief**

This picture taken on 4 April 2023 shows a woman watching a livestream on social media offering merchandise for sale in Jakarta. Photo: Bay Ismodo/AFP).

** Yanuar Nugroho is Visiting Senior Fellow at the Indonesia Studies Programme (ISP) and Regional Economic Studies (RES) at ISEAS-Yusof Ishak Institute Singapore and Senior Lecturer at Driyarkara School of Philosophy Jakarta. Sofie Syarief is former Visiting Fellow at the Media, Technology and Society at ISEAS-Yusof Ishak Institute Singapore and a PhD student at Goldsmiths, University of London, UK.*

ISSUE: 2023 No. 75
ISSN 2335-6677

EXECUTIVE SUMMARY

- The Personal Data Protection (PDP) Law was ratified by the Indonesian House of Representatives at the end of 2022. Although seen as a move in reaction to some data leakage incidents, this marks an important step in the country's journey towards digital transformation.

- However, the enactment of this law near the end of Jokowi's terms makes it look like mere lip service since it can be implemented only after all derivative regulations are in place. Till today, none of them is ready, which means that implementation of the law will be delayed.

- There are some serious challenges in the law. First, the accountability of the government in handling and managing citizens' personal data is not clearly defined. Second, the mandate to establish the Personal Data Protection Authority is difficult to operationalise because the chain of command involving various government entities is unclear. Third, there is a risk of journalistic work being stifled by indiscriminate use of the law by those in power.

- Policymakers must carefully identify, anticipate and mitigate potential unintended consequences of the law.

ISSUE: 2023 No. 75
ISSN 2335-6677

INTRODUCTION

On 20 September 2022, Indonesia's House of Representatives (DPR) ratified the PDP Law (Personal Data Protection, or *UU Perlindungan Data Pribadi*),[1] which was first initiated in 2016. The ratification happened during the 'Bjorka havoc' when a hacker penetrated and stole data from national online applications such as the Covid-19 tracing app, *PeduliLindungi*, operated by the Ministry of Health (MOH) and the *MyPertamina* app belonging to the state-run oil and gas company Pertamina.[2] Not long after the incident, 1.3 billion SIM card registration data were stolen, exposing personal ID details.[3] In the latest case, in early July 2023, 34 million passport numbers and immigration IDs were leaked.[4] All these data leaks involving governmental bodies were usually met with denial or excuses, the most popular being that the leaked data are obsolete[5] although ID numbers are valid for life.[6]

The PDP Law's ratification is seen as a reactive move to the cases of data leakage. It marked an important point in the country's journey towards digital transformation.[7] The government has been slow in developing its digital capacity, especially in protecting citizens' personal data. Indonesia has passed the Law on Information and Electronic Transactions (UU ITE, or ITE Law). This law is seen as an 'elastic' regulation which, instead of providing convenience and ease of service to the public, suppresses democratic and civic space in Indonesia by introducing an extended range of vague and imprecise offences, and with draconian penalties that can be abused.[8]

The calls for more serious policies concerning data governance resurfaced when Bjorka publicly leaked several supposedly confidential datasets.[9]

Politically, the enactment of the PDP Law coming near the end of Jokowi's term makes it look like mere lip service because it cannot be implemented until the derivative regulations are ready. These regulations are impossible to complete within less than a year. The issue of personal data and data protection is understood differently by the government – even among government bodies— and by the citizens. The logical implication is the occurrence of bias and multiple interpretations when the policy is implemented. This essay highlights some key issues related to data governance and the PDP Law. It will also discuss implementation challenges.

GOVERNMENT'S ACCOUNTABILITY, OR THE LACK THEREOF

At the heart of the PDP Law is the crucial 'accountability principle' requiring all organisations operating in Indonesia to be responsible for managing data.[10] Yet, there is still very little assurance of accountability when government bodies mishandle data.[11]

Government accountability on data mishandling was shown to be even more crucial a mere two months after the PDP Law was passed when another data leak occurred, in November 2022.[12] The breach was met with a firm denial from the Minister of Health[13] after the ministry (as the data controller) failed to inform the public (as the data owner) that data protection failure had occurred, as required in the PDP Law. The minister's denial stopped further investigations within the ministry.

The response to the data leak incident illustrates the government's ineptitude and reluctance in taking data breaches seriously. Arguably, it shows how the government has yet to understand that personal data protection is part of citizens' rights to privacy as stipulated in the Constitution. During the abovementioned massive data breach, the president and several ministers were targeted for doxxing—an act to intentionally reveal a person's private information online without their consent, often with malicious intent. Rather than seeing it as cause for alarm, Coordinating Minister for Political, Legal, and Security Affairs Mahfud MD — who himself was doxxed[14] — responded with a statement that showed a lack of sensibility in personal data protection. He tweeted, "*I'm not bothered, and I don't want to know. Because my personal data is not confidential. It can be taken from and seen on Wikipedia (Google), on the back covers of my books, at the LHKPN KPK (State Officials' Asset Report of Corruption Eradication Commission). My personal data is open, no need to leak it.*"[15]

In a show of privilege, the former Minister of Communications and Informatics (Menkominfo) Johnny G Plate, opted to use an American phone number after his private data was doxxed.[16] Rather than acknowledging how harmful private data breaches can be or showing care in securing the public's data which his own ministry had harvested, he asked journalists not to make a fuss about his decision.[17]

Unfortunately, the responses from both ministers largely represent the government's lax stance in regard to data protection.[18] The inadequate responses are compounded by half-heartedness in acknowledging the root cause, which is poor data protection governance. In handling the Bjorka hacking incident, rather than take measures to improve the nation's cyber security system, the government opted to block sites or accounts used to hack the system. At the same time, several relevant agencies, including Kemenkominfo and the National Cyber and Crypto Agency (BSSN), shifted the blame onto the other.[19] These responses ignited public scepticism: How can the government protect citizens' data if the authorities keep buck-passing and no one takes responsibility?

CHALLENGES TO PERSONAL DATA PROTECTION

The PDP Law stipulates two types of personal data: specific and general.[20] In public services, data are further classified into personal or individual data, aggregate or group data, and demographic data. Based on the Civil Registry (Administrasi Kependudukan/Adminduk) Law No. 24/2013 revising Law No. 23/2006, *personal data* are stored, managed, and protected confidentially, whereas *aggregate data* refer to a group of data on characteristics or events, or groupings of individual populations such as demographic events, age groups and occupations. *Demographic data* are used by citizens to access public services, while the government uses them as a basis to carry out development planning, budget allocation, and law enforcement.[21] These data are sourced by and are under the responsibility of government agencies.

Such a complex classification of data, especially if protection is not well managed, is prone to leakages and breaches. Poor data security or user negligence can lead to data leakage. Data breach occurs when the system is broken into.[22] Between 2019 to 2021, there were many cases of data breaches in Indonesia. Based on BSSN (2021), there were 290.3 million cyberattacks in 2019. This would increase by 41%, reaching 495.3 million cases in 2020. Understandably,

as data flows exponentially increase, so does the risk of cyberattacks. From 2019 to 2020, ransomware attacks alone increased 105%.[23]

Official responses to data security problems may have shown a lack of goodwill and evasion, judging from excuses given by some individuals. One example is the statement that a particular hack involved old, outdated data[24] – implying the hacked data were not important. Another example is the claim that the system was still safe despite a hack.[25] Nevertheless, these cases have multi-dimensional impacts, not only for the individual data owners but also for data management institutions, especially when the data are managed by government agencies. For individuals, hacking of their personal data may cause material and non-material losses, for instance, when the hacked data are used for doxing, fraud, or breaking into digital assets in the form of currency and other digital products. For data management institutions, such cases reduce public confidence in their performance and may decrease service quality or cause a decline in their reputation, and potentially lead to lawsuits.

The government is hence obliged to secure data as a strategic resource. There is an urgent need for better personal data governance, both for Indonesia's public and private sectors. The government must take full responsibility for protection of existing personal data. Indeed, it is for this reason that the PDP Law was proposed and passed.

PDP LAW AND ITS (PROBLEMATIC) SUBSTANCE

Consisting of 16 chapters and 76 articles, this law substantially covers at least four aspects, that is, data categorisation, the rights of data subjects,[26] the obligations of data controllers,[27] and the establishment of Personal Data Protection Authority (PDPA).[28]

The table below describes a juridical review of the substance of the PDP Law and the technocratic implications in its implementation, both concerning derivative regulations and the duties and responsibility of relevant institutions.

No	Sub-Material of the PDP Law	Derivative Regulations	Time Period	Leading Sector-Ministry/Agency
1	1. Chp 3 - Types of Personal Data 2. Chp 4 - Rights of Personal Data subjects 3. Chp 5 - Processing of Personal Data 4. Chp 6 - Obligations for Control of Personal Data and Personal Data Processors in the Processing of Personal Data 5. Chp 7 - Transfer of Personal Data	Existing regulations: ● Regulation of Menkes No 24/2022 on Medical Records ● Regulation of Menkes No 18/2022 on One Health Data ● Financial Services Authority Regulation (POJK) No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector ● Central Bank Regulation Number 22/20/PBI/2020 on Consumer Protection ● Regulation of Menkominfo No 20/2016 on Protection of Personal Data in Electronic Systems ● Regulation of Mendagri No 102/2019 on Granting Right to Access and Use of Population Data ● Regulation of Mendagri No 57/2021 on Information Security Management Systems and Population Administration Regulations to improve: ● Government regulations regarding filing objections from data subjects on decision-making actions during automatic processing of personal data and actions that cause legal consequences or impact data subjects. (From Article 10 paragraph 1) ● Government regulations regarding procedures for compensation for personal data processing violations. (From Article 12 paragraph 1)	Two years	● Ministry of Communications and Informatics (Kemenkominfo) ● Cyber and Crypto Agency (BSSN) ● Ministry of Home Affairs (Kemendagri) ● Ministry of Health (Kemenkes) ● Ministry of Finance (Kemenkeu) ● Financial Service Authority (OJK) ● Central Bank
2	Chp 9 – Institutions	● Presidential Regulation on the establishment of non-structural institutions at the level of the ministry/institution that administers personal data protection that is responsible to the president. (Upcoming, from Article 58) ● Government Regulation on the authority of data protection institutions. (From Articles 59 and 60)	Two years	● President ● New non-structural institutions at the ministry level ● Ministry of State Secretariat (Kemsetneg) ● Executive Office of the President (KSP) ● Kemenkominfo
3	Chp 10 - International Cooperation Chp 11 - Community Participation	● Government Regulation or Ministerial Regulation ● Regional Regulation	Two years	● Kemenkominfo ● Ministry of Foreign Affairs (Kemenlu)
4	Chp 8 - Administrative Sanctions Chp 12 - Dispute Resolution and Procedural Law Chp 13 - Prohibition on the Use of Personal Data Chp 14 - Criminal Provisions	● Sanctions: will be further regulated in a Government Regulation (Upcoming)	Two years	● Kemenkominfo ● Ministry of Law and Human Rights (Kemenkumham) ● Personal data protection agency

Source: Compiled by authors

Several articles in the PDP Law have legal implications and loopholes that need to be investigated. For instance, there are around 15 authorities that have not been listed — PDPA included — in resolving disputes through non-litigation adjudication mechanisms and issuing mediation decisions regarding compensation. There is a legitimate concern that the law can threaten the work of Indonesia's press,[29] including criminalisation of it.[30] The law also regulates criminal sanctions without providing definite limits on the meaning of each element,[31] and is therefore somewhat more inclined towards imposing sanctions than raising awareness.

In particular, the establishment of the PDPA under the President begs the question of its independence since its role is to oversee the implementation of the law by all stakeholders. Another loophole are the provisions that require companies or providers to comply with requests for deletion without delay within 3 x 24 hours from the date the request was submitted.[32] These are technically problematic because in practice, companies would need a longer time to delete data, perhaps even weeks. Further, the obligation for data controllers to have a Data Protection Officer (DPO) and parameters related to the terms of the fulfilment of the rights of Personal Data Owners[33] is difficult for medium to smaller businesses to fulfil.

IMPLEMENTATION CHALLENGES

There are two fundamental challenges to overcome for the PDP Law to be fully implemented: (i) Preparing derivative regulations and (ii) Establishing the PDPA Board.

The formulation of derivative regulations requires a fairly long time and is a complicated process. The PDP Law mandates that nine Government Regulations (Peraturan Pemerintah, or PP) and one Presidential Regulation (Peraturan Presiden, or Perpres), and subsequent Ministerial Regulations, be produced. So far, the passage of various PP and Perpres has taken significant amounts of time, mostly around six months or even a year from draft to law. If these regulations are the priority of the President – like the Omnibus Law on Job Creation (UU Ciptaker, Law No. 11 of 2020) and State Capital Law (UU IKN, Law No. 3 of 2022), they could be formulated quickly. Arguably, the completion of derivative regulations of PDP Law has so far not been the government's priority.[34]

The government organised a public consultation in February 2023 involving some 200 participants from the banking, health, education, IT, e-commerce, hospitality, transport, and public sectors.[35] So far, there is still no clear time horizon as to when the implementing regulations will be completed. Again, this signals that the issue of PDP is not seen as a priority.

Chapter 9 of the PDP Law mandates the need for a Perpres to establish a ministerial level non-structural body (PDPA) that reports to the President[36] and a PP on the authority of this institution as a data protector.[37] However, the institutional form of the PDPA is also unclear, even though the law explicitly stated it as being fully and directly responsible to the President (Article 58 para 4). There is a question of its independence. Although the law applies to both corporations and the government, the regulation delegates the establishment of the PDPA to the President, virtually rendering it no different from other executive institutions. Conflicts of interest may arise when there is no clear division of responsibility or authority regarding supervision and enforcement. Unclear regulations regarding the position and institutional structure of the PDPA will also leave its formation—including how vast its authoritative reach will be—heavily dependent on the President's "good will".[38]

The ways in which the PDPA will be established entails at least two significant problems. First, inequality of sanctions may occur in response to a failure in data protection. Any violations of data protection may be subjected to varying sanctions, from mere administrative sanctions to fines.[39] However, criminal penalties[40] are also looming, with specific penalties towards corporations.[41] Not only are governmental bodies not regarded as economic institutions that

amass annual income and cannot therefore be subjected to sanctions more profound than the administrative ones, the nature of the PDPA—not being independent from the executive bodies they are supposed to regulate— opens the possibility for unfair judgments and ineffective supervision.

Second, the PDPA being an institution on par with the governmental bodies it is meant to regulate poses a serious challenge. For example, it might do very little to determine which ministry or agency is responsible for any breach of a civil registry, especially for ID numbers, and put in place measures to secure the data created and harvested under government policies. The supervision of the PDPA should hence rest with an independent commission rather than with a government ministry.

The process for establishing the PDPA will likely take a long time, and there is no guarantee that it will start work immediately after it is formed. One is reminded of the National Research and Innovation Agency (BRIN), whose full organisational structure and governance remain unfinalised more than two years after its formation.[42] These lessons indicate that the institutional aspect is more urgent than the implementation of the PDP Law or the establishment of PDPA, and should be prioritised accordingly.

With such challenges, what may the implications of the enactment of the PDP Law be?

LACK OF AWARENESS OF DATA PROTECTION

The long list of sanctions against private data protection violations might force public entities and private corporations to channel their resources towards obeying the PDP Law. However, as much as sanctions are necessary, punitive actions towards citizens might be problematic if imposed before any meaningful measures to raise public awareness on protecting private data are taken.

According to a 2021 survey conducted by the Ministry of Communication and Information Technology, Indonesia's overall digital safety index—including the safety to not share any private data via social media—is quite low, i.e., 3.1 on a scale of 1-5.[43] This reflects general ignorance towards personal data protection or that of other people; this opens possibilities for unintentional breaches, which stem not from malicious intent but from the lack of adequate awareness of private data and the importance of protecting them—evidenced by how Minister Mahfud reacted to the personal data breach against him.

With this background in mind, the law might lead to misuse and overcriminalisation,[44] like the ITE Law. In essence, it threatens criminal action against anyone unlawfully disclosing other people's personal data. However, there is neither sufficient definition nor legal limitation on what constitutes 'unlawful' (Article 65 para 2) hence opening possibility for abuse. Equally, without adequate knowledge and conceptual awareness of data protection, the public is prone to unintended offence. For instance, teachers sharing students' daily activities could potentially be a violation[45] especially because the Law categorises children's data as 'specific' data,[46] implying different and more stringent legal repercussions.[47] It is therefore crucial to ensure overall awareness of personal data protection if the fundamental aim is to protect the public.

CURBING PRESS FREEDOM

In a continuation of the trend in curbing press freedom,[48] the PDP Law also has its own articles which may stifle journalism. Among the varieties of specific data that should not be disseminated, "criminal record" is included (Article 4 para 2). Within the bill, "criminal record" is elaborated as a written account of past unlawful acts and present judicial proceedings, police records and immigration records for travel ban issuance. The fact that all kinds of criminal records—including ongoing judicial proceedings—are regarded as specific data, implying offence for anyone publishing them, will potentially threaten journalistic work in reporting.[49]

Exclusions for the disclosure of specific data are also found in the Law (Article 15 para 1). However, these are limited to governmental undertaking and academic research. Journalistic works and the public's legitimate interests are disregarded. As mentioned, the term 'unlawful' can also be problematic for journalistic works. There is no legal definition and limitation regarding unlawful dissemination of personal data — or even specific data — rendering the term obscure yet broad.

As such, some articles of the PDP Law can be used in an unchecked manner by certain groups, especially those in power, to restrict and criminalise journalistic works. The possible outcome is journalist reports such as exposing public officials' history of corruption or other crimes—which are of legitimate public interest, and paramount since Indonesia is anticipating a national executive and parliamentary election in 2024— can be subjected to punishment. Not only do these articles contradict Indonesia's Press Law (Law No. 40 of 1999)[50] which mandates the press to professionally fulfil the public's rights to know without coercion and interference, they further question the country's commitment to democracy.

CONCLUSION

There are several aspects within the PDP Law that must be revisited and attended to when it comes implementation. These aspects, including unclear institutional set-up and articles that have ambiguous or conflicting ideas, foreshadow unintended consequences affecting the actual protection of Indonesians' data. Such consequences must be identified, anticipated and mitigated when they happen. Reflecting on the consequences and putting them in the bigger picture takes us to another reflection: Beyond the PDP Law lies a more fundamental need for a digital strategy at the country level. Without a strategy to provide firm ground for digital transformation, Jokowi's vision of Pemerintahan Dilan, a digital government that serves the people, will never be realised.

ENDNOTES

[1] https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf
[2] https://id.techinasia.com/data-pedulilindungi-diduga-bocor
[3] https://tekno.kompas.com/read/2022/09/01/13450037/13-miliar-data-registrasi-kartu-sim-diduga-bocor-pengamat-sebut-datanya-valid?page=all
[4] https://www.bbc.com/indonesia/articles/c9e7e9grjmko

[5] https://teknologi.bisnis.com/read/20230710/101/1673421/kemenkominfo-duga-data-paspor-yang-bocor-adalah-data-2020
[6] https://nasional.tempo.co/read/1637576/peretas-meki-unggah-kebocoran-26-juta-data-polridivisi-humas-data-usang
[7] During the 2019 Presidential Candidate Debate, Joko Widodo campaigned for what he called *Pemerintahan Dilan* which stood for *Pemerintahan Digital Melayani* or 'a serving digital government'. By this, he referred to four orientations for public service reform, i.e., e-government, simplification of public institutions, improvement of state apparatus quality, and governance reform. https://menpan.go.id/site/berita-terkini/dilan-dia-adalah-pemerintahan-digital-melayani-tahun-2025
[8] https://www.lowyinstitute.org/the-interpreter/are-indonesia-s-rubber-laws-limiting-freedom-speech
[9] https://id.techinasia.com/data-pedulilindungi-diduga-bocor
[10] https://www.thejakartapost.com/opinion/2022/12/21/indonesias-data-privacy-law-avoids-costly-and-misguided-localization-.html
[11] One such mishandling is the previously mentioned SIM card registration policy. In essence, Indonesians are obliged to register their personal data—including identity number and family card number—before being able to use any services from Indonesian telecommunication providers. The 1.3 billion SIM card registration data leak proved that the policy does not come with the utmost data safety, yet SIM card users have no other option, and no changes in the registration process have been made since.
[12] https://www.thejakartapost.com/paper/2022/11/22/care-and-protect-apparent-govt-health-app-breach-raises-deeper-data-concerns.html
[13] https://www.merdeka.com/peristiwa/menkes-bantah-data-pedulilindungi-bocor-apakah-itu-untuk-popularitas-hot-issue.html
[14] https://news.detik.com/berita/d-6289436/reaksi-pejabat-di-spill-bjorka-anies-sebut-data-salah-mahfud-md-santai
[15] Authors' translation from source: https://twitter.com/mohmahfudmd/status/1569501565152821248).
[16] https://en.tempo.co/read/1635136/kominfo-minister-admits-to-changing-phone-number-due-to-cyber-attack
[17] https://nasional.kontan.co.id/news/ini-alasan-menkominfo-johnny-plate-ganti-nomor-ponsel-pakai-nomor-amerika-serikat
[18] Widiatedja, I. G. N. P., & Mishra, N. (2022). Establishing an independent data protection authority in Indonesia: a future–forward perspective. International Review of Law, Computers & Technology, 1-22 https://doi.org/10.1080/13600869.2022.2155793
[19] https://nasional.kompas.com/read/2022/11/18/05230361/data-pedulilindungi-bocor-pemerintah-diminta-tak-saling-lempar-tanggung
[20] Specific personal data include information such as health, biometrics (like fingerprints and retina scans), genetics, children, personal finances, crime records, political views, and life/sexual orientation, etc., while general personal data include for instance full name, nationality, gender, religion, and marital status. See PDP Law Article 4
[21] Civil Registry Law Article 58 verse (3)
[22] https://commercial.acerid.com/support/articles/kebocoran-data-data-leakage-kenali-penyebab-dan-dampaknya/
[23] https://www.kominfo.go.id/content/detail/43363/siaran-pers-no-306hmkominfo072022-tentang-tantangan-keamanan-siber-makin-besar-indonesia-dorong-tata-kelola-data-lintas-negara/0/siaran_pers
[24] https://nasional.tempo.co/read/1637576/peretas-meki-unggah-kebocoran-26-juta-data-polridivisi-humas-data-usang
[25] https://www.cnnindonesia.com/teknologi/20210831113819-185-687743/data-diduga-bocor-kemenkes-minta-warga-hapus-ehac-versi-lama

[26] Data subject is defined as an individual with all related personal data. See PDP Law Article 1 verse (6).
[27] Data controller is defined as an individual or public institution or international organization which act individually or together in deciding the objective and control of personal data processing. See PDP Law Article 1 verse (4)
[28] *Rights of Data Subjects* include access to and copies of personal data, clarity of identity, as well as the basis of legal interests, approval-revocation-suspension and restrictions on data processing, filing and filing of objections to the use of personal data, as well as the right to compensation for violations of data processing.
Obligations of the Data Controller include proving approval of the data subject, personal data management, guarantee of protection and security, as well as conveying the legality, purpose, and relevance of personal data processing.
Persnal Data Protection Authority (PDPA) is granted with authority and tasked with formulating and establishing policies in personal data protection, supervising compliance of personal data controllers, and imposing administrative sanctions for violations of Personal Data Protection.
[29] See https://www.hukumonline.com/berita/a/penerapan-uu-pdp--potensi-kriminalisasi-hingga-hambat-kerja-kerja-pers-lt6329eb04dd0f3/?page=2
[30] PDP Law Article 4 para 2.
[31] PDP Law Article 65 para 2 and Article 67 para 2.
[32] PDP Law Article 41 para 1.
[33] PDP Law Article 53.
[34] Since the UU Ciptaker was ratified on 2 November 2020, it took only three months to issue the implementing regulations: 45 PP and 4 Perpres. UU IKN was adopted on 15 February 2022 and two months later one PP and four Perpres were issued. Whereas for PDP Law, even until today, 11 months after ratification, not a single derivative regulation has been completed. See https://news.detik.com/berita/d-5396256/ini-daftar-45-pp-dan-4-perpres-turunan-uu-cipta-kerja and https://mediaindonesia.com/politik-dan-hukum/490432/pemerintah-rampungkan-lima-aturan-turunan-uu-ikn.
[35] See https://aptika.kominfo.go.id/2023/02/siapkan-aturan-pelaksana-uu-pdp-kominfo-libatkan-publik/
[36] PDP Law Article 58.
[37] PDP Law Articles 59 and 60.
[38] https://elsam.or.id/siaran-pers/pengesahan-ruu-pelindungan-data-pribadi-terancam-menjadi-macan-kertas
[39] PDP Law Article 57.
[40] PDP Law Articles 67, 68, and 69,
[41] PDP Law Article 70.
[42] At least three deputies, the agency secretary, and quite several directors are not yet definitively appointed https://brin.go.id/page/profil-pejabat
[43] https://cdn1.katadata.co.id/media/microsites/litdik/Status_Literasi_Digital_diIndonesia%20_2021_190122.pdf
[44] https://tirto.id/ketika-uu-pdp-berpotensi-jadi-pasal-karet-ancam-kebebasan-pers-gwsK
[45] https://magdalene.co/story/apa-isi-uu-perlindungan-data-pribadi
[46] Article 4 para 2
[47] Articles 34 and 53
[48] https://www.thejakartapost.com/opinion/2022/05/04/indonesian-law-systematically-stifles-journalists.html
[49] https://tirto.id/ketika-uu-pdp-berpotensi-jadi-pasal-karet-ancam-kebebasan-pers-gwsK
[50] https://www.pwi.or.id/detail/633/UU-Pers

ISSN 2335-6677

ISEAS Perspective is published electronically by:
ISEAS - Yusof Ishak Institute

30 Heng Mui Keng Terrace
Singapore 119614
Main Tel: (65) 6778 0955
Main Fax: (65) 6778 1735

Get Involved with ISEAS. Please click here:
https://www.iseas.edu.sg/support/get-involved-with-iseas/