

# **Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore**

Firsta Rahadatul 'Aisy<sup>a</sup> , Muhammad Azil Maskur<sup>b</sup> ,  
A.M Adzkiya' Amiruddin<sup>c</sup> 

<sup>a</sup> Faculty of Law, The University of Melbourne, Melbourne, Australia

<sup>b</sup> Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

<sup>c</sup> Faculty of Law, Universitas Indonesia, Depok, Indonesia

✉ Corresponding email: [faisy@student.unimelb.edu.au](mailto:faisy@student.unimelb.edu.au)

## **Abstract**

In the digital era, technological advancements have enabled governments and corporations to streamline services and expand market reach, often leading to the collection and transfer of personal data without the knowledge of data subjects. This poses significant risks to constitutional rights. Indonesia's Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) aims to address these risks, yet frequent data breaches indicate ineffective enforcement of administrative sanctions due to the absence of an independent authority. This study analyzes the urgency of establishing a Personal Data Protection Agency in Indonesia, evaluates current sanctions under the PDP Law, and compares the enforcement mechanisms of data protection agencies in Ireland, Australia, and Singapore. Using a normative legal approach with qualitative methods, the research finds that these countries' independent agencies

effectively enforce data protection laws and administrative sanctions. The study reveals significant enforcement shortcomings in Indonesia, underscoring the need for a dedicated authority to prevent violations and protect personal data rights. By adopting best practices from Ireland, Australia, and Singapore, Indonesia can enhance its data protection framework. Immediate action by the President to establish this authority through a Presidential Regulation is crucial for safeguarding personal data in the digital age.

**KEYWORDS** *Personal Data Protection, Administrative Sanctions, Data Breach, Law Enforcement, Personal Data Protection Agency*

## Introduction

Technological advancements have significantly facilitated various aspects of human activity, offering transformative benefits across sectors such as business, healthcare, education, and public services. While these developments warrant recognition and support through the establishment of a robust and inclusive technological ecosystem, their implementation must remain grounded in the principles of human rights. The integration of technology into daily life should not compromise the fundamental rights and freedoms to which individuals are legally entitled. It is, therefore, a core responsibility of the state to safeguard these rights and ensure that the benefits of technological progress are equitably distributed without infringing upon individual liberties.<sup>1</sup>

According to the Preamble of the 1945 Constitution of the Republic of Indonesia, the nation's commitment is to honor all sacrifices made for the country through thorough government action. In addition, the state is dedicated to managing public affairs with a focus on national autonomy, global harmony, and the protection of civil rights. In line with this constitutional mandate, the advancement of technology must be governed in a manner that upholds these core values, ensuring that innovation contributes to, rather than undermines, the realization of justice, equity, and the protection of fundamental freedoms. The state, as the guardian of the people's rights, is entrusted with

---

<sup>1</sup> Howie, Emily. "Protecting the human right to freedom of expression in international law." *International Journal of Speech-Language Pathology* 20, no. 1 (2018): 12-15.

ensuring that technological progress aligns with the nation's constitutional ideals and supports the broader goal of collective welfare.<sup>2</sup>

Over the years, the concept of privacy has gained universal recognition, being upheld by both formal laws and informal ethical standards across various countries.<sup>3</sup> Indonesia's dedication to protecting privacy as a fundamental right for all its citizens is both clear and unequivocal. This commitment is articulated in the Preamble of Human Rights Law Number 39 of 1999, especially in its fourth provision: As a member of the United Nations, the Indonesian people have both moral and legal responsibilities to adhere to and implement the Universal Declaration of Human Rights and other human rights conventions accepted by the Republic of Indonesia.<sup>4</sup> Therefore, the state, as the governing authority, is accountable for its citizens and must ensure their welfare in line with international law. This responsibility extends to ensuring that technological advancements are aligned with the principles of upholding human rights. In essence, the state is primarily responsible for enforcing human rights.<sup>5</sup>

Similar to numerous other nations, Indonesia considers privacy as an integral part of human rights. While the 1945 Indonesian Constitution, which serves as the primary legal framework, does not overtly state privacy or data protection, it does emphasize the protection of human rights. The Preamble of the Constitution states that safeguarding human rights is a national goal, striving to safeguard all citizens and enhance prosperity through peace, social justice, and liberty. Additionally, the concept of data privacy is further explored

---

<sup>2</sup> Changshan, Ma. "The Fourth Generation of Human Rights' Under the Background of Smart Society and Its Protection." *China Legal Science* 5, no. 1 (2019): 5-24.

<sup>3</sup> Banisar, David, and Simon G. Davies. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *John Marshall Journal of Computer & Information Law* 18, no. 1 (1999): 1-15.

<sup>4</sup> Republic of Indonesia, "Law of the Republic of Indonesia No. 39 Year 1999 Concerning Human Rights," Pub. L. No. 39, § preamble (1999).

<sup>5</sup> Suwondo, Denny. "The Legal Protection of Personal Data in the Perspective of Human Rights." *Law Development Journal* 5, no. 4 (2021): 419-429. For further cases, see also Rahim, Erman I., et al. "Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations." *Journal of Law and Legal Reform* 6, no. 3 (2025): 1305-1348; Putra, Tegar Islami, et al. "Critically Reveal the Dimensions of Damage from Unauthorized Use of Personal Data (Study of Decision Number 78/Pid. Sus/2024/PN Tng)." *The Digest: Journal of Jurisprudence and Legisprudence* 5, no. 2 (2024): 231-262; Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?." *Pandecta Research Law Journal* 19, no. 2 (2024): 173-202.

in the amendments to the 1945 Constitution, specifically Articles 28F and 28G. While these provisions do not explicitly address privacy and data protection, they provide a foundation for related regulations. Although these articles have not yet been directly implemented in Indonesian regulations, they clearly reflect a concern for human dignity as a fundamental human right.<sup>6</sup>

The progression of increasingly advanced technology brings forth numerous new challenges, particularly regarding privacy rights. In Indonesia, the rapid growth of data-driven internet technologies impacts various fields, including banking, healthcare, trade, and online transportation, all of which involve the gathering of personal data. This expansion presents considerable difficulties, particularly in safeguarding personal data. In the global economic landscape, Indonesia holds a significant position in electronic transactions, which leads to the greater dissemination of personal data.<sup>7</sup>

Regulating privacy rights related to personal data reflects the acknowledgment and safeguarding of fundamental human rights.<sup>8</sup> As science and technology advance, it is crucial to make sure that privacy rights are safeguarded. While progress is driven by knowledge, privacy rights are crucial for preserving fundamental freedoms. Thus, establishing regulations to protect privacy rights is vital. Furthermore, Indonesia embraces technological progress by implementing legal measures to safeguard citizens' privacy concerning personal data. Law Number 27 of 2022 on Personal Data Protection (PDP Law) serves as a recognition and enactment of the value that protecting personal data is an essential human right, as stated in the 1945 Constitution of the Republic of Indonesia.

The effective operation and execution of human rights in personal data management necessitate the presence of an institution tasked with the legal enforcement of data protection. According to Article 58, Paragraph 2 of Law Number 27 of 2022 on Personal Data Protection, the responsibility for enforcing personal data protection is assigned to a designated institution.<sup>9</sup> This institution, which is selected by and accountable to the President, possesses

<sup>6</sup> Rosadi, Sinta Dewi. "Data Privacy Law in the Application of Smart City in Indonesia." *Journal of Legal, Ethical and Regulatory Issues* 24, no. 4S (2021): 1-9.

<sup>7</sup> Palupy, Heppy Endah. "Privacy and data protection: Indonesia legal framework." *Thesis of Master Program in Law and Technology*, Tilburg: Tilburg University, 2011.

<sup>8</sup> Finck, Michèle, and Frank Pallas. "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law* 10, no. 1 (2020): 11-36.

<sup>9</sup> Republic of Indonesia, Law of the Republic of Indonesia No. 27 Year 2022 on Personal Data Protection (UU PDP)," Pub. L. No. 27 (2022), art. 58(2), [https://jdih.setkab.go.id/PUUdoc/176837/Salinan\\_UU\\_Nomor\\_27\\_Tahun\\_2022.pdf](https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf).

various powers, including the authority to enforce administrative sanctions on data controllers and processors who commit violations.<sup>10</sup>

As of now, despite the establishment of the PDP Law, Indonesia has yet to form a personal data protection institution responsible for enforcing the law and imposing administrative sanctions on violators. Consequently, the enforcement of personal data protection laws remains ineffective and lacks authority, as violations by data controllers and processors have not been addressed or penalized. The development and implementation of personal data protection policies are still incomplete, and oversight of data protection practices has yet to be enforced. Notably, there has been no administrative action taken against violations under the Personal Data Protection Law so far.

One of reasons the institution has not yet been established is that the law does not specify a deadline for its formation. However, setting a maximum deadline for establishing the institution is crucial for legal certainty. The lack of a time frame has resulted in the institution still not being formed to this day.

To assess the effectiveness of administrative sanctions enforcement in Indonesia's Personal Data Protection Law (UU PDP No. 27 of 2022) and the necessity of establishing a dedicated Personal Data Protection Agency (PDPA), this study explores several key research questions. *First*, it examines how Indonesia's current enforcement mechanism function and whether they effectively ensure compliance with data protection regulations. *Second*, it investigates the legal and institutional challenges that hinder the formation of an independent PDPA, particularly in relation to jurisdictional overlaps, regulatory gaps, and resource constraints. *Third*, it evaluates how administrative sanctions are enforced in Ireland, Australia, and Singapore, identifying best practices that Indonesia can adopt. *Finally*, this research aims to provide policy recommendations on strengthening Indonesia's data protection enforcement, including institutional design, capacity-building initiatives, and potential legal reforms to enhance regulatory clarity and enforcement efficiency. Through this analysis, the study seeks to contribute to ongoing discussions on how Indonesia can foster a robust and impactful data protection scheme that aligns with international best practices.

Previous research has explored personal data protection and the enforcement of administrative sanctions, but gaps remain in addressing the role of institutions responsible for enforcing these laws. Rizky Pratama and Evi Retno Wulan highlighted that Indonesia's personal data protection law is

---

<sup>10</sup> Republic of Indonesia, Law of the Republic of Indonesia No. 27 Year 2022 on Personal Data Protection (hereinafter refer as UU PDP 27/2022), art. 58–59.

substantively adequate but lacks effective implementation due to the absence of an oversight institution.<sup>11</sup> However, their study does not address the impact of this absence on administrative sanctions, nor does it offer a comparative analysis of other countries. Similarly, Voss W. Gregory and Heinrich Amadeus Wolff analyzed the effectiveness of GDPR sanctions, but both studies focused primarily on the sanctions themselves without discussing the role of the institutions that enforce them.<sup>12</sup>

I Gusti Ngurah Parikesit Widiatedja and Neha Mishra advocated for the establishment of an independent data protection agency in Indonesia, underscoring its essential role in safeguarding privacy and data protection. They noted that although the PDP Law refers to global best practices, it lacks specific guidelines for establishing an autonomous supervisory body.<sup>13</sup> The absence of a well-defined framework creates uncertainty about the unbiased enforcement of the PDP Law. Unlike this study, their work does not incorporate a comparative analysis of enforcement practices from other jurisdictions but instead concentrates on institutional independence and regulatory capacity.

This study is important because it fills a crucial gap in Indonesia's personal data protection framework. By examining comparative models of data protection institutions in countries like Ireland, Singapore, and Australia, the research provides practical recommendations for the Indonesian government to establish and improve its own data protection authority. This, in turn, aims to bolster the application of the PDP Law and ensure the safeguard of citizens' privacy rights.

This legal research adopts a doctrinal or normative analysis which seeks to uncover specific legal principles or conduct a more nuanced and in-depth examination of legal statements and reasoning<sup>14</sup> related to "*Establishing*

---

<sup>11</sup> Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431-455.

<sup>12</sup> Wolff, Josephine, and Nicole Atallah. "Early GDPR penalties: Analysis of implementation and fines through May 2020." *Journal of Information Policy* 11 (2021): 63-103. *See also* Voss, W. Gregory. "The CCPA and the GDPR are not the same: why you should understand both." *CPI Antitrust Chronicle* 1, no. 1 (2021): 7-12; Voss, W. Gregory. "Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems II." *Colorado Technology Law Journal* 19, no. 2 (2021): 377-427.

<sup>13</sup> Widiatedja, I. Gusti Ngurah Parikesit, and Neha Mishra. "Establishing an independent data protection authority in Indonesia: a future-forward perspective." *International Review of Law, Computers & Technology* 37, no. 3 (2023): 252-273.

<sup>14</sup> Ali, Salim Ibrahim, Zuryati Mohamed Yusoff, and Zainal Amin Ayub. "Legal research of doctrinal and non-doctrinal." *International Journal of Trend in Research and*

*Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore.*" In this study, the legal analysis of the issues will be supported by primary data, a feature commonly associated with empirical legal research (nondoctrinal). However, the utilization of primary data here is restricted to reinforcing the arguments instead shifting the focus of the research. The primary data will not specifically or directly affect to any of the objects being studied.<sup>15</sup> To elaborate, the doctrinal approach involves a thorough review of relevant laws and regulations, including those pertaining to data privacy, while the conceptual approach centers on a detailed examination of fundamental legal concepts, ensuring a robust understanding of both theoretical principles and practical implications in safeguarding individuals' rights in the digital age.<sup>16</sup>

The use of normative legal research methods in this study is driven by their effectiveness in comparing the enforcement of administrative sanctions by personal data protection institutions in Ireland, Australia, and Singapore, providing valuable insights for the establishment of Indonesia's Personal Data Protection Agency. Primary data for this research includes relevant legal texts, such as statutes, regulations, and judicial rulings, alongside documents detailing the judiciary's role in these countries' data protection frameworks. Additionally, the study draws on literature related to environmental protection laws, offering a broader context for understanding regulatory practices. The qualitative approach adopted facilitates a comprehensive examination of how administrative sanctions are applied in the selected jurisdictions, allowing for a detailed comparison that informs the potential design and enforcement mechanisms of Indonesia's own Personal Data Protection Agency.

## Indonesia's Personal Data Protection Law and Enforcement Framework

The Personal Data Protection Law (PDP Law), officially Law Number 27 of 2022, represents a major advancement in Indonesia's legal framework for

---

*Development* 4, no. 1 (2017): 493-495. See also Arifin, Ridwan, et al. "Improving Law Student Ability on Legal Writing through Critical and Logical Thinking by IRAC Method." *Indonesian Journal of Advocacy and Legal Services* 1, no. 1 (2019): 107-128.

<sup>15</sup> Mertokusumo, Sudikno. *Penemuan Hukum: Sebuah Pengantar*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2010.

<sup>16</sup> Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." *Lex Scientia Law Review* 7, no. 2 (2023): 995-1048.

data privacy and protection. It signifies Indonesia's acknowledgment of privacy as a vital human right, in line with global trends and principles found in international agreements such as the GDPR. Despite its progressive provisions, the law encounters significant challenges in its implementation, particularly in terms of establishing a dedicated enforcement institution. This section will explore the core elements of Indonesia's PDP Law, including its foundational principles and key provisions, as well as the institutional shortcomings that impede effective enforcement. It will also draw comparisons with international best practices.

## **A. Overview of Indonesia's Personal Data Protection Law (Law No. 27 of 2022 on Personal Data Protection)**

The Personal Data Protection Law (PDP Law), formally designated as Law Number 27 of 2022, is a significant step forward in Indonesia's legal framework for safeguarding data privacy and protection. It reflects Indonesia's commitment to recognizing privacy as a fundamental human right, consistent with global norms and international agreements like the GDPR. The law seeks to balance the rights and responsibilities between personal data controllers and data subjects, ensuring robust protection for individuals' data. Article 16 of the PDP Law highlights that this balance is vital for data processing, stipulating that personal data controllers must respect the rights of data subjects when acquiring, collecting, processing, or analyzing their data.<sup>17</sup> This includes ensuring that the data is obtained legally and safeguarded in accordance with the purposes and activities for which it is being processed.<sup>18</sup>

In practice, the implementation of personal data protection measures in Indonesia, both physical and non-physical, has been ineffective. Data breaches continue to occur and dissipate without adequate follow-up from relevant authorities or government institutions. The government has not taken significant actions, such as imposing sanctions or penalties, to address these breaches. This lack of action is primarily due to the absence of an established institution tasked with enforcing administrative sanctions for personal data protection violations, despite the mandate outlined in Chapter IX (Articles 58-61) of the PDP Law, which details the institutional framework for data

---

<sup>17</sup> UU PDP 27/2022, art. 16(1).

<sup>18</sup> UU PDP 27/2022, art. 16(2).

protection. Consequently, the enforcement of the law in cases of personal data protection violations remains ineffective, increasing the risk of recurring issues.

According to Article 59 of the PDP Law<sup>19</sup>, 'the personal data protection institution is responsible for:

- a. Developing and implementing policies and strategies for Personal Data Protection to provide guidance for Data Subjects, Data Controllers, and Data Processors;
- b. Supervising the execution of Personal Data Protection measures;
- c. Imposing administrative penalties for breaches of this Law; and
- d. Assisting in resolving disputes through means other than court proceedings.'

Sanctions arise as a response from either individuals or social institutions to a particular action. In sociological terms, they represent a method of law enforcement. Typically, sanctions can be categorized into criminal, civil, and administrative types. Administrative sanctions, which are a form of administrative action, involve the unilateral authority of the administration to decide, impose, and enforce penalties on individuals who breach public order laws.<sup>20</sup> In the context of the PDP Law, administrative sanctions are particularly important, as they empower the designated authorities to ensure compliance with data protection regulations.<sup>21</sup> These sanctions act as a deterrent, encouraging organizations to adopt proper data protection practices and swiftly address any violations that may occur.

The Personal Data Protection Agency (PDPA) needs to ensure that its policies and strategies are comprehensive and practical, offering clear and actionable steps for compliance with the law.<sup>22</sup> These policies must also be flexible enough to address new challenges as technology and data practices evolve. It may involve regular updates to policies in line with international best practices. The agency also needs to ensure that data controllers and processors are following the proper procedures for managing personal data<sup>23</sup>, such as ensuring data security, obtaining consent, and processing data within the

---

<sup>19</sup> UU PDP 27/2022, art. 59.

<sup>20</sup> Saraswati, Retno, Zainal Arifin Hoesein, and Susi Dian Rahayu. "Implementation of Administrative Sanctions in Abuse Law Enforcement Utilization of Green Open Space in Bekasi City." *IOP Conference Series: Earth and Environmental Science*. Vol. 1270. No. 1. IOP Publishing, 2023.

<sup>21</sup> UU PDP 27/2022, art. 57.

<sup>22</sup> UU PDP 27/2022, art. 59(a).

<sup>23</sup> UU PDP 27/2022, art. 59(b).

boundaries set by the law. It may also conduct audits, inspections, or assessments to verify that data protection practices are being followed.<sup>24</sup>

When data protection violations occur, the PDPA has the authority to impose administrative sanctions.<sup>25</sup> This could include sanctions like written warnings, temporary suspension of operations, deletion or destruction of personal data, and fines in cases of serious violations.<sup>26</sup> The fines can reach up to two percent of the annual income or revenue, depending on the specifics of the violation.<sup>27</sup> Furthermore, Article 65 of the PDP Law specifically addresses the misuse of personal data, detailing, among other things<sup>28</sup>:

- 1) Individuals are forbidden from unlawfully acquiring or collecting personal data that is not theirs, whether for personal gain or for others, particularly if such actions could inflict harm on the data subject;
- 2) Any individual is prohibited from revealing personal data that does not belong to them;
- 3) Individuals are barred from generating false personal data or altering existing data for their own or others' benefit, particularly if such actions could potentially cause harm to others.

Administrative sanctions also act as a corrective measure, pushing data controllers and processors to amend their practices if found in violation of the law. The PDPA is responsible for providing alternative dispute resolution mechanisms to settle conflicts related to data protection without necessarily involving the court system.<sup>29</sup> This includes methods like mediation or conciliation to address complaints from data subjects who believe their rights have been violated (e.g., unauthorized access to personal data, misuse of data, etc.).<sup>30</sup> The PDPA helps facilitate negotiations between the data subject and the data controller or processor, aiming to find mutually agreeable solutions.

In addition to its regulatory role, the PDPA is also tasked with promoting public awareness about data protection rights. This includes educating individuals about their rights to privacy and data protection, thereby enhancing

---

<sup>24</sup> UU PDP 27/2022, art. 60(b).

<sup>25</sup> UU PDP 27/2022, art. 60(c).

<sup>26</sup> UU PDP 27/2022, art. 57(2).

<sup>27</sup> UU PDP 27/2022, art. 57(3).

<sup>28</sup> UU PDP 27/2022, art. 65.

<sup>29</sup> UU PDP 27/2022, art. 59(2).

<sup>30</sup> UU PDP 27/2022, *see* explanation of art. 59(d).

the public's understanding of the importance of safeguarding personal data.<sup>31</sup> Other than repressive measures like imposing administrative sanction, the PDPA's enforcement powers also include preventive measures. Preventive measures involve requiring data controllers to submit annual reports on their data processing activities, thereby fostering a culture of transparency.<sup>32</sup>

The lack of a dedicated personal data protection institution has impeded the enforcement of data protection laws. To adequately protect citizens' privacy rights, it is crucial to establish this institution without delay. Enacting a data protection law alone is not enough to manage surveillance effectively; it is essential to have an agency responsible for implementing the law to ensure its practical and effective application.<sup>33</sup> Experts and practitioners alike concur on the necessity for data protection agencies to operate with the highest level of independence allowed by the constitution. However, they should also remain subject to some degree of judicial oversight or accountability.<sup>34</sup>

One important aspect in establishing a personal data protection agency is to ensure its independence by eliminating all political influence. Threats to the independence of this agency could occur if the government politicizes the budget of this agency. In addition, threats to independence could also occur if the government politicizes the recruitment or appointment process of commissioners serving in this agency. The lack of independent supervision raises issues regarding the accountability and transparency of the oversight processes.<sup>35</sup> Therefore, it is important to establish a PDPA with strong independence, free from political interference, to effectively protect individual privacy rights.<sup>36</sup>

---

<sup>31</sup> Budiman, Ahmad. "Otoritas Pengawas Pelindungan Data Pribadi," *Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis* XIII, no. 5 (February 2021): 26, [https://berkas.dpr.go.id/pusaka/files/info\\_singkat/Info%20Singkat-XIII-5-I-P3DI-Maret-2021-181.pdf](https://berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XIII-5-I-P3DI-Maret-2021-181.pdf).

<sup>32</sup> Ayiliani, and Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara."

<sup>33</sup> Flaherty, David H. *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*. North Carolina: UNC Press Books, 2014.

<sup>34</sup> Flaherty, p. 391.

<sup>35</sup> Zhang, Yueming. "Processing of personal data by public authorities in China: assessing equivalence for cross-border transfers from the EU to China." *European Journal of Law and Technology* 14, no. 1 (2023).

<sup>36</sup> Greenleaf, Graham. "Independence of data privacy authorities (Part I): International standards." *Computer Law & Security Review* 28, no. 1 (2012): 3-13.

## B. Existing Enforcement Mechanisms and Jurisdictional Overlaps

In the absence of a functioning Personal Data Protection Agency (PDPA), several existing institutions in Indonesia are responsible for data protection, but they lack the cohesive authority to effectively enforce the PDP Law. These institutions include *Komdigi* (Ministry of Communication and Digital), *BSSN* (National Cyber and Crypto Agency), Ombudsman RI (*Indonesian Ombudsman*), and *Otoritas Jasa Keuangan* (Indonesian Financial Service Authority).

Increasing number of data leaks in recent years has highlighted weaknesses in this fragmented system. High-profile incidents, such as those attributed to the hacker Bjorka, have exposed the vulnerability of the national data protection system. These breaches reportedly involved sensitive data like SIM card registrations, documents from the State Intelligence Agency (BIN), and personal information of state officials, raising serious questions about the preparedness of existing institutions to handle cyber threats.<sup>37</sup>

In 2019, the Jakarta Legal Aid Institute (LBH Jakarta) received over five thousand complaints related to personal data misuse.<sup>38</sup> By 2022, data breaches had increased by 143% in the second quarter alone, according to research by the cybersecurity firm Surfshark.<sup>39</sup> Several personal data breach incidents were reported in 2022, affecting even state-owned enterprises. For example, the State Electricity Company (PLN) experienced a breach involving 17 million customer records, which were leaked to a hacker forum.<sup>40</sup> The exposed data included names, addresses, and billing information. Additionally, the prominent Indonesian internet service provider Indihome faced a data breach

<sup>37</sup> Putri, Riani Sanusi. "Saling Lempar Tanggung Jawab Atasi Kebocoran Data Pribadi," *TEMPO*, accessed March 29, 2025, <https://www.tempo.co/arsip/saling-lempar-tanggung-jawab-atasi-kebocoran-data-pribadi-290025>.

<sup>38</sup> Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, and Moh Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (2020): 182-200.

<sup>39</sup> Surfshark, "Data Breach Statistics Globally," Global data breach statistics, Surfshark, January 28, 2025, <https://surfshark.com/research/data-breach-monitoring>.

<sup>40</sup> Rizkinaswara, Leski. *Data pelanggan PLN bocor, kominfo: Sudah dipanggil dan terus dipantau*, Ditjen Aptika Kominfo (Aug. 22, 2022), <https://aptika.kominfo.go.id/2022/08/data-pelanggan-pln-bocor-kominfo-sudah-dipanggil-dan-terus-dipantau/>

affecting 26 million user accounts, revealing search histories, names, email addresses, and ID numbers.<sup>41</sup>

Pertamina also faced a similar issue, with data of 44 million users being sold by hackers for Bitcoin worth IDR 392 million.<sup>42</sup> Moreover, one of the most frequently used apps during the pandemic, PeduliLindungi, experienced a significant data breach where approximately 3.2 billion records were sold on dark web forums.<sup>43</sup> These breaches highlight the weaknesses in system security and the lax oversight that led to significant losses for data owners.<sup>44</sup>

Not only were apps affected, but there were also allegations of data breaches on government websites, potentially caused by malware or malicious software infections. The site with the highest number of data leaks was *Prakerja*, with 17,331 credentials exposed on [dashboard.prakerja.go.id](https://dashboard.prakerja.go.id). Following this, the Ministry of Education and Culture's sites, [datadik.kemdikbud.go.id](https://datadik.kemdikbud.go.id) and [info.gtk.kemdikbud.go.id](https://info.gtk.kemdikbud.go.id), experienced breaches of 15,729 and 10,761 credentials, respectively. Additionally, the Directorate General of Taxes' website, [djponline.pajak.go.id](https://djponline.pajak.go.id), saw a breach of 10,409 credentials.<sup>45</sup> Data

---

<sup>41</sup> Yolanda, Erlins, and Rugun Romaida Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif." *Journal of Syntax Literate* 8, no. 6 (2023): 4166-4182.

<sup>42</sup> Karina, Dina. "44 Juta Data MyPertamina Diduga Bocor, Pertamina dan Telkom Bakal Investigasi," *Kompas TV*, November 11, 2022, [https://www.kompas.tv/bisnis/347339/44-juta-data-mypertamina-diduga-bocor-pertamina-dan-telkom-bakal-investigasi#google\\_vignette](https://www.kompas.tv/bisnis/347339/44-juta-data-mypertamina-diduga-bocor-pertamina-dan-telkom-bakal-investigasi#google_vignette)

<sup>43</sup> Dirgantara, Adhyasta, and Dani Prabowo, "Data PeduliLindungi Bocor, Pemerintah Diminta Tak Saling Lempar Tanggung Jawab," *KOMPAS*, November 18, 2022, <https://nasional.kompas.com/read/2022/11/18/05230361/data-pedulilindungi-bocor-pemerintah-diminta-tak-saling-lempar-tanggung?page=all>

<sup>44</sup> Yolanda, and Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif." *See also* Lamdayoung, Cindy Thia. "Loss Due to Data Leaks: How is the Legal Protection for Account Owners on Marketplace?." *Journal of Creativity Student* 5, no. 1 (2020): 25-42; Putra, Tegar Islami, et al. "Risks of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites." *Journal of Private and Commercial Law* 8, no. 2 (2024): 110-128; Putra, Tegar Islami, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis. "Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection." *The Indonesian Journal of International Clinical Legal Education* 7, no. 2 (2025): 203-234.

<sup>45</sup> CNN Indonesia, "Ribuan Data Pemerintah Diduga Bocor, Termasuk Prakerja Hingga CPNS," *CNN Indonesia*, April 9, 2022, <https://www.cnnindonesia.com/teknologi/20220408160348-192-782309/ribuan-data-pemerintah-diduga-bocor-termasuk-prakerja-hingga-cpns>.

breaches on government sites can have serious consequences, as the information often includes personal data or other sensitive information.<sup>46</sup>

There has been no significant action taken by the government regarding these violations. Offenders have not faced sanctions and continue to operate their business processes, which inevitably involve storing and managing data. In fact, violations like these should be penalized to ensure deterrence. However, since no such sanctions are in place, there is a high likelihood that these violations could recur. Below explained existing institutions who have handled the enforcement when data breach occurs in Indonesia.

#### 1. Komdigi

*Komdigi* has a broad mandate that includes overseeing the digital landscape in Indonesia, regulating telecommunications, and managing data and information security issues.<sup>47</sup> However, the focus of this ministry is very broad, covering policies in the fields of digital infrastructure, digital government technology, digital ecosystems, digital space supervision, personal data protection, and public communication and media<sup>48</sup>, rather than focusing only on personal data protection, which leads to a reactive rather than proactive approach to data breaches. For instance, in the wake of the Bjorka data leaks involving sensitive information like SIM card registrations and state intelligence documents, *Komdigi* (which was *Kominfo*) emphasized the importance of individual user actions like changing passwords and limiting the sharing of their NIK.<sup>49</sup> However, cybersecurity experts criticized this as insufficient against sophisticated attacks, especially against advanced malware.<sup>50</sup> While *Komdigi* (which was *Kominfo*) can issue guidelines and warnings, it does not have the authority to impose significant penalties or enforce the comprehensive provisions of the PDP Law.

<sup>46</sup> Yolanda, and Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif," p. 4169.

<sup>47</sup> Kementerian Komunikasi dan Digital, "Ruang Lingkup, Tugas, Dan Fungsi," Komdigi, accessed April 7, 2025, <https://www.komdigi.go.id/profil/tugas-fungsi>.

<sup>48</sup> Kementerian Komunikasi dan Digital.

<sup>49</sup> Achmad Hanif Imaduddin, "Dari Jaga NIK Hingga Ganti Password, Berikut Deretan Pernyataan Kontroversial Menkominfo," *tempo.co*, September 8, 2022, <https://www.tempo.co/politik/dari-jaga-nik-hingga-ganti-password-berikut-deretan-pernyataan-kontroversial-menkominfo-293535>.

<sup>50</sup> Widodo Bagiarto, "Pakar Kritik Menkominfo Anggap Tak Penting Pengamanan Siber," *Rmol.id*, accessed April 7, 2025, <https://rmol.id/politik/read/2023/12/03/599796/pakar-kritik-menkominfo-anggap-tak-penting-pengamanan-siber>.

## 2. BSSN

*BSSN* is tasked with managing cybersecurity and protecting the nation's critical infrastructure.<sup>51</sup> It plays a critical role in responding to cybersecurity incidents, such as data breaches caused by hacking.<sup>52</sup> *BSSN* was involved in investigating the data leaks publicized by Bjorka and coordinated with other agencies to mitigate further risks. However, its focus is more on the cybersecurity aspect rather than the data protection rights of individuals, limiting its role in enforcing the PDP Law. The agency also faces challenges such as limited human resources and technology that is not yet optimal for detecting and preventing large-scale data breaches.<sup>53</sup> Moreover, the agency also lacks the authority to enforce penalties against private companies or government bodies that fail to protect personal data effectively.

## 3. Ombudsman RI

The Ombudsman *RI* is responsible for overseeing public services and ensuring that government actions are transparent and just.<sup>54</sup> It can intervene when there are violations of administrative justice<sup>55</sup>, including in cases where personal data is mishandled by public institutions. Based on the Ombudsman's experience, one of personal data protection cases that have been handled according to Public Reports 2018 was the case of Indihome, who faced a data breach affecting 26 million user accounts, revealing search histories, names, email addresses, and ID numbers.<sup>56</sup> Moreover, their Public Report in 2023 also mentioned complaints about government websites that often experience data leaks/problems, making people unsure about providing personal data and email when requested.<sup>57</sup> However, the role of the Indonesian Ombudsman is limited

<sup>51</sup> Badan Siber dan Sandi Negara, "Tentang Kami - Badan Siber dan Sandi Negara," Badan Siber dan Sandi Negara, accessed April 7, 2025, <https://bssn.acaraseru.id/bssn.acaraseru.id>.

<sup>52</sup> Badan Siber dan Sandi Negara.

<sup>53</sup> Salwa, Nikita Dewi Kurnia. "Tantangan & Hambatan Besar Yang Dihadapi CSIRT-BSSN Indonesia," *Computer Security Incident Respond Team Indonesia*, November 18, 2024, <https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn>.

<sup>54</sup> Ombudsman Republik Indonesia, "Tugas Dan Fungsi," Profil Tugas dan Fungsi, accessed April 8, 2025, <https://ombudsman.go.id/profiles/index/pfft>.

<sup>55</sup> Ombudsman Republik Indonesia.

<sup>56</sup> Yolanda and Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif," p. 4169.

<sup>57</sup> Rettob, Krisna. "Perlindungan HAM Di Era Digital Dalam Perspektif Pelayanan Publik," *Online Article*, Ombudsman RI, December 2024, <https://ombudsman.go.id:443/artikel/r/artikel--perlindungan-ham-di-era-digital-dalam-perspektif-pelayanan-publik>.

to receiving, examining, and following up on reports related to alleged maladministration in the provision of public services, including those related to personal data. They do not have the specialized expertise in data protection to handle the increasing complexity of data privacy violations in the digital age.

#### 4. *Otoritas Jasa Keuangan*

In relation to personal data in the financial services matter, Indonesia also has a Financial Services Authority or *Otoritas Jasa Keuangan (OJK)*. *OJK* plays a crucial role in protecting customer personal data within Indonesia's financial sector by overseeing, regulating, and educating financial institutions.<sup>58</sup> Its mandate includes ensuring that financial institutions adhere to the security and privacy standards when handling personal data. In the case of the 2023 data breach at Bank Syariah Indonesia, the *OJK* was directly involved in addressing the situation. Following the breach, where approximately 1.5 TB of sensitive data, including customer information, financial documents, legal papers, confidentiality agreements, and internal access passwords, was stolen by the Lockbit 3.0 hacker group<sup>59</sup>, the *OJK* took immediate steps to investigate and enforce compliance measures. The authority worked to assess the extent of the damage and ensure that the bank's response aligned with national data protection protocols.<sup>60</sup> This incident highlights the pressing need for a dedicated Personal Data Protection Agency (PDPA) in Indonesia. While the *OJK* plays a key role in regulating the financial sector, the breach underscored the limitations of existing structures in managing personal data protection across all sectors.

#### 5. Jurisdictional Overlaps

The overlapping roles and unclear responsibilities of these institutions create confusion and inefficiency in enforcing data protection regulations. For instance, in the context of the recent data breaches, both *Komdigi* and *BSSN* were involved. Adding to the confusion, controversial statements from *Komdigi* officials appeared to shift the responsibility for cybersecurity to *BSSN*, highlighting the lack of clear coordination and roles in handling cyber threats.

<sup>58</sup> Otoritas Jasa Keuangan, "Tugas Dan Fungsi," Tentang OJK, accessed April 8, 2025, <https://ojk.go.id/id/tentang-ojk/pages/tugas-dan-fungsi.aspx>.

<sup>59</sup> Prima, Erwin. "LockBit Klaim Bobol 1,5 TB Data Pribadi, Pengamat Minta BSI Siapkan Mitigasi," *TEMPO*, May 2023, <https://www.tempo.co/digital/lockbit-klaim-bobol-1-5-tb-data-pribadi-pengamat-minta-bsi-siapkan-mitigasi-188407>.

<sup>60</sup> Sinaga, Guna Gerhat, et al. "Analisis Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia)." *Jurnal Pendidikan Tambusai* 7, no. 3 (2023): 28374-28383.

Without clear authority over enforcement, their efforts can become disjointed, delaying necessary actions. The Ombudsman may intervene in public sector cases but lacks the authority to address violations by private entities, leading to gaps in enforcement. This lack of a centralized enforcement body undermines the law's effectiveness.

Additionally, the absence of a dedicated data protection authority means that there is no clear institution to oversee the entirety of Indonesia's data protection framework. This lack of coordination between agencies reduces the capacity to hold companies accountable for data protection failures, leaving many breaches unaddressed.

In comparison to other ASEAN countries, Indonesia's data protection framework also lacks integration with the ASEAN Framework on Personal Data Protection. While countries like Singapore and Malaysia have established dedicated regulatory bodies (such as the Personal Data Protection Commission in Singapore) with clear authority to enforce data protection laws, investigate breaches, and issue sanctions, Indonesia's fragmented approach makes cross-border data protection coordination more challenging. The ASEAN Framework emphasizes regional cooperation and alignment of data protection standards<sup>61</sup>, but Indonesia's lack of a central agency undermines its ability to collaborate effectively on issues like cross-border data transfer and regional data privacy enforcement. Establishing a centralized data protection agency would help Indonesia align more closely with regional standards and improve its international cooperation efforts.

### **C. Challenges in Establishing Indonesia's Personal Data Protection Agency**

The establishment of an independent Personal Data Protection agency (PDPA) in Indonesia, as mandated by the Personal Data Protection Law (UU PDP No. 27 of 2022), is facing significant challenges. Despite the law's progressive aims to protect citizens' personal data, the lack of an established and operational PDPA has led to inefficiencies and weak enforcement of data protection regulations. Below are some of the key challenges identified from the existing mechanisms and the comparative analysis of other countries' enforcement structures.

---

<sup>61</sup> ASEAN Member States, "Framework on Personal Data Protection," Asean Telecommunications and Information Technology Ministers Meeting (TELMIN) (Bandar Seri Begawan: ASEAN, November 25, 2016), <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>.

### 1. Absence of a Clear Timeline for PDPA Formation

One of the primary challenges in the operationalization of Indonesia's PDPA is the absence of a specific timeline for its establishment. The UU PDP mandates that this law shall come into effect two years after it is enacted<sup>62</sup>, however it does not stipulate a specific deadline for the creation of the agency, which has resulted in significant delays. This lack of urgency has caused legal uncertainty, with violations of the law not being addressed, and administrative penalties not being enforced. The comparative analysis of countries like Ireland, Australia, and Singapore underscores the importance of having a dedicated authority to ensure the effective enforcement of data protection laws.

### 2. Staffing and Technical Expertise Shortages

The creation and operation of a data protection authority require highly specialized personnel with expertise in data protection law, cybersecurity, and technology management. Indonesia faces a shortage of qualified personnel capable of handling the complexities of data privacy enforcement.<sup>63</sup> According to experts, staffing issues remain one of the biggest barriers to operationalizing the Indonesian PDPA.<sup>64</sup> To address this, the PDPA must recruit skilled experts and invest in continuous training programs to stay ahead of evolving digital threats.

### 3. Budgetary Constraints

The PDPA's effectiveness is closely tied to sufficient funding. Indonesia's budget allocation for the agency has been a concern, as the government has yet to provide adequate financial support to create the infrastructure necessary for its independent operations.<sup>65</sup> Without financial autonomy, the PDPA may be subject to political interference, undermining its independence and capacity to take action against violations.<sup>66</sup> This

---

<sup>62</sup> UU PDP 22/2022, art. 75.

<sup>63</sup> Ahmad, Rumadi. "Lembaga Perlindungan Data Pribadi," *kompas.id*, July 21, 2024, <https://www.kompas.id/baca/opini/2024/07/19/lembaga-perlindungan-data-pribadi>.

<sup>64</sup> Yamin, Ahmad Fachri, et al. "Perlindungan data pribadi dalam era digital: Tantangan dan solusi." *Meraja Journal* 7, no. 2 (2024): 138-155.

<sup>65</sup> Doly, Denico. "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)." *Negara Hukum: Membangun Hukum untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223-244.

<sup>66</sup> Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *Justisi* 10, no. 1 (2024): 20-35.

challenge highlights the need for a sustainable funding model that ensures the agency's ability to carry out its mandate effectively.

#### 4. Political Will and Bureaucratic Hurdles

Another significant barrier is bureaucratic inefficiency and political resistance to the creation of an independent data protection agency. There is a lack of political will to push forward the formation of the PDPA, and inter-agency collaboration has been inadequate.<sup>67</sup> For example, the law assigns multiple agencies with overlapping duties, but clear guidelines for cooperation between these agencies are not in place. This fragmentation of authority leads to inconsistent enforcement and missed opportunities for protecting personal data. Establishing an independent agency would resolve these issues by consolidating responsibilities and ensuring a coordinated response.

#### 5. Urgency for Presidential Action

Given the current enforcement challenges and the lack of clear timelines for establishing the PDPA, the Indonesian government must take immediate action. Presidential Regulation should be issued to formalize the creation of the agency and provide it with the necessary authority and resources to enforce the PDP Law effectively.<sup>68</sup> Without this independent body, Indonesia's data protection framework will continue to be ineffective, leaving personal data rights vulnerable to violations.

## Socio-Political Context Affecting Administrative Sanctions Enforcement

The socio-political landscape plays a crucial role in shaping the enforcement of administrative sanctions related to the Personal Data Protection Law (PDP Law) in Indonesia. A key factor in ensuring the effectiveness of law enforcement is the independence of state institutions responsible for overseeing these regulations. According to Sri Soemantri, state institutions can be divided into two categories: primary state institutions and auxiliary state organs.<sup>69</sup> While primary institutions hold the central responsibilities of governance, auxiliary organs are established to support specific goals that cannot be achieved by

<sup>67</sup> Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)."

<sup>68</sup> See UU PDP 22/2022, art. 58(3)-(4).

<sup>69</sup> Basarah, Ahmad. "Kajian Teoritis Terhadap Auxiliary States Organ dalam Struktur Ketatanegaraan Indonesia." *Masalah-Masalah Hukum* 43, no. 1 (2014): 1-8.

primary institutions alone. Independent state institutions, which serve this auxiliary function, must operate autonomously, free from personal or institutional influence.<sup>70</sup> This autonomy is essential for ensuring impartial enforcement of laws and maintaining public trust in the regulatory process.

In the context of data protection, the creation of an independent Personal Data Protection Agency (PDPA) would serve as an auxiliary institution, providing the necessary oversight and enforcement mechanisms that go beyond the capabilities of existing governmental bodies.<sup>71</sup> These independent agencies should be separate from the executive, legislative, and judicial branches, ensuring that their decisions are not subject to political influence. Independence, in this sense, means operating with freedom, autonomy, and self-governance<sup>72</sup>, which are the critical qualities for an institution tasked with protecting citizens' personal data from misuse or breach.

The lack of such an independent institution in Indonesia has contributed to the inefficiencies in enforcing the PDP Law. The socio-political challenges, such as political interference and institutional fragmentation, hinder the establishment of a truly independent body. Thus, for Indonesia to address these challenges, it must prioritize the creation of an autonomous and independent PDPA that can effectively oversee data protection efforts, ensuring that they are carried out in accordance with both national and international standards. This is crucial for understanding the limitations and opportunities for effective enforcement of administrative sanctions under the Personal Data Protection Law (PDP Law).

## A. Socio-Political and Cultural Factors

The rapid growth of digital technologies in Indonesia brings with it both opportunities and challenges in ensuring data protection. Socio-political factors, such as government coordination, political will, and cultural perspectives on privacy, play an essential role in shaping how data protection laws are enforced. One notable concern is the lack of public awareness and understanding of data

---

<sup>70</sup> Mangar, Irma, and Muhammad Rosyid Ridho. "Lembaga Independen Negara dalam Ketatanegaraan Indonesia." *Definisi: Jurnal Agama Dan Sosial Humaniora* 1, no. 2 (2022): 75-84.

<sup>71</sup> Lembaga Studi dan Advokasi Masyarakat (eLSAM). *Skenario Pembuatan Otoritas Pelindungan Data Pribadi Di Indonesia: Opsi dan Implikasi: Seri HAM dan Internet*. Jakarta: ELSAM, 2022. <https://www.elsam.or.id/policy-paper/skenario-pembentukan-otoritas-pelindungan-data-pribadi-di-indonesia--opsi-dan-implikasi>.

<sup>72</sup> Matheus, and Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU."

protection rights<sup>73</sup>, which can delay compliance and the effectiveness of administrative sanctions.

Moreover, political and institutional factors present significant barriers to effective enforcement. The fragmentation of regulatory authority across multiple institutions, such as the Ministry of Communication and Digital (*Komdigi*) and the National Cyber and Crypto Agency (*BSSN*), often results in overlapping jurisdictions and unclear responsibilities. This lack of coordination undermines the unified enforcement of data protection laws, leading to gaps in the response to data breaches, as seen in high-profile incidents involving data leaks like the Bjorka hacking cases.

As emphasized in recent discussions, the establishment of the Personal Data Protection Agency (PDPA) is critical. The agency must operate independently from political and institutional influence to perform its duties effectively, especially when dealing with violations of data protection laws by both public and private sectors. The independence of the PDPA will not only ensure that enforcement is impartial but also reinforce the public's trust in the regulatory process. However, creating an independent agency requires clear legal frameworks and adequate political support to prevent external interference.

## **B. Balancing Data Protection with Economic and Digital Transformation Goals**

Indonesia's ongoing digital transformation presents a delicate balancing act between ensuring robust data protection and fostering economic growth. As Indonesia positions itself as a leader in the digital economy, the enforcement of data protection regulations must be aligned with the broader goals of economic and technological advancement.<sup>74</sup> However, overly stringent regulations could stifle innovation and discourage investment in the rapidly expanding tech sector.

The Indonesian government must address these tensions by ensuring that the operationalization of the PDP Law does not hinder the growth of digital industries. Effective regulation should not only protect personal data but also

---

<sup>73</sup> See Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)."

<sup>74</sup> Rosadi, Sinta Dewi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78-90.

promote a competitive digital economy.<sup>75</sup> This requires the establishment of a regulatory framework that can evolve with technological advancements while maintaining robust safeguards against data misuse.

As discussed in recent analyses, the PDPA must adopt a flexible regulatory approach that integrates digital literacy programs, infrastructure development, and international cooperation.<sup>76</sup> To ensure that the PDP Law fosters both data protection and economic growth, the regulatory body must support industries in adopting best practices without imposing excessive burdens on innovation. Ensuring that digital and data privacy regulations align with international standards, as seen in comparative models from countries like the EU, is key to maintaining global competitiveness while protecting the rights of individuals.<sup>77</sup>

## **Comparative Analysis: Administrative Sanctions Enforcement in Ireland, Australia, And Singapore**

This comparative study aims to evaluate the efficiency of data protection enforcement mechanisms in Ireland, Australia, and Singapore, with the goal of identifying best practices that could be adapted to enhance Indonesia's data protection framework. These three countries were selected for comparison due to their well-established and robust data protection agencies, which have been recognized internationally for their effectiveness in enforcing data protection laws.

Ireland was included in this study because it hosts the Data Protection Commission (DPC), the key authority overseeing the enforcement of the European Union's General Data Protection Regulation (EU GDPR). As one of the most thorough and stringent data protection frameworks globally, the EU GDPR makes Ireland's approach highly relevant for understanding top-tier standards in data protection enforcement.

Australia presents a distinct legal and regulatory framework, with the Office of the Australian Information Commissioner (OAIC) responsible for enforcing the Privacy Act 1988. Australia's data protection strategy emphasizes transparency and accountability, aiming to balance privacy rights with economic factors.<sup>78</sup> This makes Australia a compelling case for comparison,

---

<sup>75</sup> Wibowo, Ari, Widya Alawiyah, and Azriadi. "The importance of personal data protection in Indonesia's economic development." *Cogent Social Sciences* 10, no. 1 (2024): 2306751.

<sup>76</sup> Wibowo, Alawiyah, and Azriadi.

<sup>77</sup> Rosadi, "Data Privacy Law in the Application of Smart City in Indonesia."

<sup>78</sup> Mishova, Ana. "Data Protection Laws Around the World: A Global Perspective," *GDPR Local*, August 16, 2024, <https://gdprlocal.com/data-protection-laws-around-the-world-a->

especially for Indonesia, which faces a similar challenge of balancing economic development with adherence to stringent data protection regulations.

Singapore was chosen for its rapid emergence as a digital hub in Southeast Asia and its robust data protection framework, which is enforced by the Personal Data Protection Commission (PDPC). Singapore's approach is particularly relevant to Indonesia due to the similarities in economic and technological landscapes as two of them are members of Association of Southeast Asian Nation (ASEAN) regional cooperation. The PDPC is known for its pragmatic and business-friendly approach<sup>79</sup>, which could provide valuable insights for Indonesia as it seeks to create a data protection agency that is both effective and conducive to economic growth.

This comparative study is relevant to Indonesia's context as it faces the challenge of implementing and enforcing its recently enacted Personal Data Protection Law (PDP Law). By analyzing the structures, enforcement mechanisms, and best practices of Ireland, Australia, and Singapore, Indonesia can derive valuable lessons on how to effectively enforce its data protection laws, protect persona data, and uphold the rights of data subject.

## A. Key Factors in Administrative Sanctions Enforcement

The effective of administrative sanctions enforcement in data protection laws is shaped by several key factors, including jurisdictional scope, sanctioning powers, and enforcement efficiency. While some jurisdictions, such as the European Union under the General Data Protection Regulation (GDPR), have broad extraterritorial reach, others, like Australia and Singapore, focus primarily on domestic enforcement. Similarly, the severity and type of sanctions vary from high financial penalties in the EU to compliance-driven in Singapore. However, enforcement effectiveness is not solely determined by the legal authority to impose fines; it is also depending on investigate capacity, regulatory consistency, and enforcement speed. This section outlines the common enforcement

---

global-perspective/; Office of the Australian Information Commissioner (OAIC), "Australian Privacy Principles Guidelines: Privacy Act 1988" (Sydney: Office of the Australian Information Commissioner (OAIC), December 2022), <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>.

<sup>79</sup> Tan, Steve and Victoria Tan, "Understanding How the PDPA Permits Organisations to Leverage on Personal Data in Achieving Innovation," in *Personal Data Protection Digest*, ed. Yeong Zee Kin. Singapore: Academy Publishing, 2023.

principles and key trends across jurisdictions, providing a comparative foundation for the country-specific case studies in the following sections.

### 1. Jurisdictional Scope

Jurisdictional scope determines whether a data protection authority (DPA) can enforce sanctions against entities beyond its national borders. In some jurisdictions, data protection laws apply extraterritorially, ensuring that companies processing domestic users' data remain subject to enforcement, even if they operate abroad. For example, global frameworks such as GDPR apply to any organization handling EU citizens' personal data, regardless of location.<sup>80</sup> In contrast, some legal regimes, such as those in Australia and Singapore, focus on enforcing compliance only within their national borders, limiting their ability to regulate foreign-based data controllers and processors.

Another key consideration is how DPAs coordinate with other jurisdictions in handling cross-border violations. Some regulators, such as the Irish Data Protection Commission (DPC), work within a regional enforcement framework, where EU member states cooperate under GDPR's One-Stop-Shop Mechanism to ensure harmonized enforcement.<sup>81</sup> However, other countries rely on bilateral or regional agreements to strengthen enforcement against foreign entities.

In the comparative analysis, each country's regulatory agency's authority to handle data breaches and enforce penalties across domestic and international jurisdictions will be assessed. Indonesia can learn from these models in terms of how it might handle cross-border data flows, particularly given its growing role in global digital trade and ASEAN's increasing importance in regional data protection frameworks.

### 2. Types of Sanctions and Enforcement Powers

The nature and severity of administrative sanctions differ significantly across jurisdictions. Common enforcement mechanisms include financial penalties, compliance orders, processing bans, and corrective measures. Some regulators, such as the Irish DPC under GDPR, impose high fines as a

---

<sup>80</sup> European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 679 (2016), art. 3, <https://data.europa.eu/eli/reg/2016/679/oj>.

<sup>81</sup> Data Protection Commission, "One Stop Shop (OSS)," International Transfers, accessed March 20, 2025, <https://www.dataprotection.ie/organisations/international-transfers/one-stop-shop-oss>.

deterrent<sup>82</sup>, while others, such as Singapore's PDPC, emphasize compliance-based corrective actions.<sup>83</sup>

In general, enforcement agencies tend to categorize violations based on severity, with penalties increasing for more serious breaches. For example, several jurisdictions apply tiered sanctions, where minor infractions may result in warnings or corrective orders, while serious violations may lead to multi-million-dollar fines or restrictions on data processing activities.<sup>84</sup> Another key factor is whether the enforcement system prioritizes punitive measures (such as large corporate fines) or compliance-based outcomes (such as requiring organizations to strengthen security measures without imposing heavy financial penalties).

### 3. Effectiveness of Enforcement

Even with strong legal frameworks, the success of administrative sanctions depends on how effectively a regulator can investigate, prosecute, and enforce penalties. Assessing the effectiveness of enforcement requires analyzing how well these sanctions contribute to compliance and data protection goals. Some jurisdictions, such as Ireland under GDPR, have faced criticism for slow enforcement timelines, particularly in handling major tech companies that challenge regulatory decisions.<sup>85</sup> Other regulators, such as Singapore's PDPC, focus on swift and preventive enforcement, resolving cases faster by prioritizing compliance over prolonged litigation.<sup>86</sup> While in Australia, their enforcement mechanism highlights the need for higher penalties and clearer breach notification procedures.<sup>87</sup> The comparative study section will analyze whether

---

<sup>82</sup> European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 83.

<sup>83</sup> Singapore, Personal Data Protection Act (2012), art. 29(2)(a)-(d) & sec 50, <https://sso.agc.gov.sg/Act/PDPA2012>.

<sup>84</sup> Wolff, and Atallah. "Early GDPR penalties: Analysis of implementation and fines through May 2020," pp. 66-69.

<sup>85</sup> Burgess, Matt. "How GDPR Is Failing," *Wired*, accessed March 20, 2025, <https://www.wired.com/story/gdpr-2022/>.

<sup>86</sup> Singapore, Personal Data Protection Commission Singapore, "Enforcement of the Act," PDPC Singapore, March 22, 2025, <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/enforcement-of-the-act>.

<sup>87</sup> Macpherson, John, Tim Brookes, Amanda Ludlow, Geoff McGrath, and Andrew Hilton. "Australia's Massive New Privacy Penalties Become Law but Will Be Clarified," *Ashurst Business Insight*, December 2, 2022, <https://www.ashurst.com/en/insights/australias-massive-new-privacy-penalties-become-law-but-will-be-clarified/>.

these sanctions truly deter data violations and whether the enforcement authorities' decisions lead to long-term improvements in data security.

## B. Data Protection Commission of Ireland

The Data Protection Commission (DPC) is tasked with safeguarding individuals' fundamental rights to personal data within the European Union (EU). It oversees adherence to the General Data Protection Regulation (GDPR) and is also in charge of enforcing other key regulatory frameworks, such as the Irish e-Privacy Regulations (2011) and the EU's Law Enforcement Directive.<sup>88</sup> The DPC, established under the authority of the GDPR that became effective on May 25, 2018, is responsible for regulating the processing of personal data within the European Union. The GDPR defines the obligations of data controllers and processors, with the primary goal of enhancing individuals' rights over their personal data. In accordance with Article 51(1) of the GDPR, the regulation mandates the appointment of one or more independent public bodies to oversee its enforcement.<sup>89</sup> Additionally, Recital 117 of the GDPR specifies that data protection supervisory authorities in EU member states are endowed with full independence to perform their functions and enforce the regulation effectively.<sup>90</sup> This independence is essential for effectively safeguarding individuals' personal data.

The GDPR outlines the roles and duties of data protection agency in its member states. These include helping individuals protect their personal data rights, providing guidance and support to legislative bodies for regulatory implementation, and primarily ensuring the enforcement of data protection laws.<sup>91</sup> Data protection authorities are also responsible for handling any issues related to data breaches or violations reported by individuals or organizations. They impose sanctions, mediate data subject access requests, and provide guidelines to help interpret the provisions within the GDPR.<sup>92</sup> Additionally, the Data Protection Authority (DPA) also functions to raise awareness and ensure compliance regarding the risks, rules, and rights of

---

<sup>88</sup> Data Protection Commission Ireland, The Data Protection Commission, <https://www.dataprotection.ie/en>.

<sup>89</sup> See General Data Protection Regulation, recitals 117.

<sup>90</sup> See General Data Protection Regulation.

<sup>91</sup> Schwartz, Paul M. "Global Data Privacy: The EU Way." *New York University Law Review* 94, no. 4 (2019): 771-818.

<sup>92</sup> Daigle, Brian, and Mahnaz Khan. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce and Economics* (June 2020): 1-38.

personal data protection during its processing among organizations and the public.<sup>93</sup> DPAs (Data Protection Authorities) across member states also collaborate with other supervisory authorities in the European Union on issues related to complaints and suspected violations involving cross-border data processing.<sup>94</sup>

The jurisdictional scope of the DPC is extensive, as the GDPR applies not only to EU-based entities but also foreign organizations that handle personal data of EU citizens.<sup>95</sup> This extraterritorial reach gives the DPC significant power to regulate the actions of global tech companies, regardless of where they are based. For example, the DPC has imposed sanctions on companies like Facebook (Meta), which process data of EU residents even though they are headquartered outside the EU. This broad jurisdiction ensures that Ireland can hold international companies accountable for data breaches and non-compliance with EU privacy laws.

When violations are identified, the DPC has the authority to issue formal reprimands and can mandate that data controllers or processors rectify their practices to comply with the regulation, typically within a designated period.<sup>96</sup> The DPC's enforcement authority extends to imposing administrative sanctions<sup>97</sup>, which include temporary or definitive limitations on data processing, or in more serious cases, banning data processing altogether.<sup>98</sup> Moreover, the DPC is authorized to enforce the correction, deletion, or limitation of personal data. It is also responsible for informing individuals or

---

<sup>93</sup> Data Protection Commission, The Data Protection Commission, <https://www.dataprotection.ie/en>.

<sup>94</sup> Haniver, Rob. "Ireland - Data Protection Overview: Guidance Note". *DataGuidance*, (2024), <https://www.dataguidance.com/notes/ireland-data-protection-overview>.

<sup>95</sup> European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 3

<sup>96</sup> European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 83.

<sup>97</sup> Data Protection Commission, "Data Protection Commission Announces Conclusion of Inquiry into WhatsApp," *News & Media*, January 19, 2023, <https://www.dataprotection.ie/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp>.

<sup>98</sup> Aktopis, Michael S., and Ron B. Katwan. "Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU)." *International Legal Materials* 60, no. 1 (2021): 53-98.

recipients who have been impacted by data breaches when required.<sup>99</sup> Another potential sanction the DPC can impose involves suspending data transfers to third countries or international organizations when these transfers are deemed non-compliant.<sup>100</sup>

The sanctioning powers of the DPC are equally robust. Under the GDPR, the DPC can impose hefty financial penalties, including fines of up to €20 million or 4% of global annual turnover (whichever is higher).<sup>101</sup> These fines are intended to act as a deterrent to large corporations that may otherwise consider data breaches as a cost of doing business. In 2022, for instance, the DPC fined WhatsApp €225 million for failing to comply with GDPR's transparency rules.<sup>102</sup> Additionally, the DPC has the power to issue other sanctions, such as restrictions on data processing activities or even banning them in severe cases.

When it comes to enforcement efficiency, the DPC has had notable success in imposing penalties and making high-profile companies comply with the GDPR. A significant case managed by the DPC of Ireland was the Facebook vs. DPC Ireland case, which focused on Facebook's adherence to the General Data Protection Regulation (GDPR) and its management of cross-border data transfers. This case attracted considerable attention due to issues concerning Facebook's methods for transferring data of European users to the United States under the Privacy Shield framework, which has since been invalidated.<sup>103</sup> The DPC initiated an investigation into whether Facebook's data processing activities adhered to GDPR requirements, particularly focusing on the company's cross-border data flow mechanisms.

Following its investigation, the DPC levied a €265 million fine on Meta, the parent company of Facebook, for non-compliance with GDPR regulations

---

<sup>99</sup> Data Protection Commission, "Data Protection Commission Announces Decision in Facebook 'Data Scraping' Inquiry," News & Media, November 28, 2022, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry>.

<sup>100</sup> *Data Protection Commission*.

<sup>101</sup> European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 83.

<sup>102</sup> Data Protection Commission, "Data Protection Commission Announces Conclusion of Inquiry into WhatsApp."

<sup>103</sup> Aktipis, and Katwan. "Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU)."

concerning user consent and cross-border data transfers.<sup>104</sup> Additionally, the DPC ordered Facebook to amend its data processing operations to ensure compliance with GDPR.<sup>105</sup> The DPC's enforcement action was notable not only for the substantial size of the fine but also for its wider impact on cross-border data transfers between the EU and the U.S., which played a role in the dissolution of the Privacy Shield agreement.

The effectiveness of the DPC's response in this case was a landmark in GDPR enforcement. However, there was criticism regarding the length of time it took to conclude the investigation, leading to questions about the efficiency of handling such complex cross-border cases.<sup>106</sup> Despite the protracted timeline, the case set an important precedent and sent a clear signal to large multinational corporations regarding the seriousness of GDPR compliance, especially in the area of international data transfers. The outcome demonstrated the DPC's commitment to ensuring that companies are held accountable for data processing violations, reinforcing the GDPR's role as a robust regulatory framework in protecting personal data.

The GDPR's one-stop-shop mechanism is designed to streamline enforcement across EU member states, but it can lead to delays, especially in cases involving multinational corporations. Despite these challenges, the DPC remains a powerful entity that has successfully held companies accountable for breaches, setting an example for other countries in the EU and beyond.

## C. Office of the Australian Information Commissioner (OAIC)

The Office of the Australian Information Commissioner (OAIC), an independent statutory agency, oversees the Privacy Act 1988, ensuring that individual privacy rights are upheld and that Australia's privacy laws are properly enforced.<sup>107</sup> Established in 2010,<sup>108</sup> the OAIC operates

<sup>104</sup> Data Protection Commission, "Data Protection Commission Announces Decision in Facebook 'Data Scraping' Inquiry," *News & Media*, November 28, 2022, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry>.

<sup>105</sup> *Data Protection Commission*.

<sup>106</sup> Aktipis, and Katwan. "Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU)."

<sup>107</sup> Office of the Australian Information Commissioner (OAIC), "What We Do," OAIC, February 20, 2025, <https://www.oaic.gov.au/about-the-OAIC/what-we-do>.

<sup>108</sup> Office of the Australian Information Commissioner (OAIC), "Australian Privacy Principles Guidelines," OAIC, March 10, 2023,

as a regulatory body with a comprehensive mandate that includes overseeing privacy, freedom of information, and the management of government data.<sup>109</sup>

The main responsibility of the OAIC is to ensure adherence to the Australian Privacy Principles (APPs), which dictate the proper management of personal information by organizations and government bodies, including its collection, storage, use, and disclosure. Beyond enforcing privacy regulations, the OAIC also works to raise public awareness about privacy rights and offers guidance to organizations to help them comply with these standards.<sup>110</sup> The OAIC carries out several crucial regulatory functions, such as investigating privacy-related concerns—whether initiated by complaints or at the commissioner’s own initiative—and monitoring compliance with privacy laws across the entities it oversees.<sup>111</sup> It also has the authority to direct government agencies to conduct privacy impact assessments and enforce compliance by bringing legal action if needed. Furthermore, the OAIC can impose administrative penalties for severe or recurring breaches of privacy, as well as award compensation for damages resulting from privacy violations.<sup>112</sup>

In addition to enforcing the Privacy Act 1988 (Cth), the OAIC oversees the Freedom of Information Act 1982 (FOI Act) and administers the Australian Information Commissioner Act 2010 (AIC Act).<sup>113</sup> The OAIC’s responsibilities encompass personal data protection, access to government information, and the transparency of data usage across public and private sectors through these legislative frameworks. This oversight covers a range of industries, including healthcare, telecommunications, and financial services, positioning the OAIC

---

<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>.

<sup>109</sup> Office of the Australian Information Commissioner (OAIC), “OAIC Corporate Plan 2024–25,” OAIC Corporate Plan (Sydney: Office of the Australian Information Commissioner (OAIC), August 29, 2024), 5, <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25>.

<sup>110</sup> Office of the Australian Information Commissioner (OAIC), “What We Do.”

<sup>111</sup> Office of the Australian Information Commissioner (OAIC), “Privacy Regulatory Action Policy,” OAIC, February 17, 2025, <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy>.

<sup>112</sup> McMillan, John. “Privacy-a regulator’s perspective.” *ALAL Forum*, no. 83 (2016): 78-82.

<sup>113</sup> Office of the Australian Information Commissioner (OAIC), “Part 1: Introduction to the Freedom of Information Act 1982,” OAIC, March 10, 2023, <https://www.oaic.gov.au/freedom-of-information/freedom-of-information-guidance-for-government-agencies/foi-guidelines/part-1-introduction-to-the-freedom-of-information-act-1982>.

as a crucial authority in ensuring the protection of personal data across various sectors.<sup>114</sup>

The OAIC also shows a critical role in managing data transfer issues, ensuring the security and protection of personal data both within Australia and across international borders. The jurisdictional scope of the OAIC covers domestic entities and foreign organizations that collect or process personal data from Australian residents. Similar to the GDPR's extraterritoriality, the OAIC has the authority to hold foreign companies accountable, ensuring that even multinational corporations respect Australian privacy laws when interacting with Australian citizens. For instance, the OAIC can investigate and take enforcement actions against global companies like Google and Facebook if they violate Australian privacy principles, even if their headquarters are overseas.

The OAIC has the authority to enforce compliance with the Privacy Act 1988 (Cth) through a variety of measures. These include investigating data breaches and issuing administrative penalties, such as fines or directives to halt illegal data processing practices. The specific enforcement actions available to the OAIC encompass:

- a. Enforceable undertakings, which require an organization to take specific actions to address and prevent further breaches<sup>115</sup>
- b. Compliance notices, which direct organizations to stop specific practices or align their data processing activities with legal requirements.<sup>116</sup>
- c. Civil penalties for severe or repeated breaches of the Privacy Act, which may involve significant financial fines.<sup>117</sup>
- d. Public declarations, where the OAIC may publicly announce a breach, aiming to increase transparency and accountability.

In addition, OAIC can also seek an injunction as part of its enforcement actions. Although the OAIC does not directly issue injunctions, it has the authority to seek such orders from the Federal Court or Federal Circuit Court.

In terms of sanctioning powers, the OAIC has several tools at its disposal, including the ability to impose fines for breaches of the APPs. While the maximum penalties under the Privacy Act are somewhat lower than those in

---

<sup>114</sup> Office of the Australian Information Commissioner (OAIC), "Guide to Securing Personal Information," OAIC, March 10, 2023, <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>

<sup>115</sup> Australia, "Privacy Act 1988 (Cth)" (2024), sec. 80, <https://www.legislation.gov.au/C2004A03712/latest/text>

<sup>116</sup> See Privacy Act 1988 (Cth)" (2024), sec. 80W.

<sup>117</sup> See Privacy Act 1988 (Cth), sec. 26.

the EU reaching up to AUD 2.1 million, the OAIC can also require organizations to take enforceable undertakings, which compel companies to change their practices and improve data protection measures. The OAIC has utilized these powers effectively in cases like the Uber data breach and the Optus data breach. In these instances, the OAIC not only imposed fines but also required the companies involved to take corrective measures, enhancing their data security practices preventing future breaches.

The enforcement efficiency of the OAIC has been proven in several cases, such as the investigation into Uber's mishandling of a data breach involving 1.2 million Australian costumers and drivers. The breach involved sensitive information such as names, email addresses, phone numbers, and driver's license details.<sup>118</sup> Rather than immediately informing the impacted individuals and regulatory bodies, Uber attempted to conceal the breach by paying the hackers to erase the compromised data.<sup>119</sup>

The OAIC's investigation determined that Uber violated the Privacy Act 1988, specifically APP 1.2 and APP 11.1, by failing to reasonably notify individuals about the breach and by not adequately protecting the data.<sup>120</sup> In December 2019, the OAIC approved an enforceable undertaking from Uber. This legally binding agreement required Uber to take specific actions to improve its data protection practices, such as implement a comprehensive data security program, engage in independent audits of data security practices, and improve its processes for responding and notification procedures to data breaches.

In addition to the enforceable undertaking accepted by the OAIC in 2019, Uber was also fined \$7.5 million AUD as part of a broader settlement related to the Uber data breach.<sup>121</sup> The 7.5 million fine was part of a joint settlement agreement involving several U.S. states and global regulatory bodies, including actions taken by the Australian regulators.<sup>122</sup> This financial penalty imposed by the OAIC was one of the largest penalties in Australia data

---

<sup>118</sup> Office of the Australian Information Commissioner (OAIC), "Uber Found to Have Interfered with Privacy," OAIC, March 10, 2023, <https://www.oaic.gov.au/news/media-centre/uber-found-to-have-interfered-with-privacy>.

<sup>119</sup> Office of the Australian Information Commissioner (OAIC).

<sup>120</sup> Hunt, Jon, Robert Neely, and Melissa Tan, "Uber Decision a Stark Reminder of the Extraterritorial Reach of the Privacy Act 1988 (Cth)," *Lander & Rogers*, August 2021, <https://www.landerson.com.au/legal-insights-news/uber-decision-reminder-of-extraterritorial-reach-of-privacy-act>.

<sup>121</sup> Hunt, Neely, and Tan.

<sup>122</sup> Hunt, Neely, and Tan.

protection history and sent a clear message that companies must comply with their obligations to report data breaches and protect personal information.

This case exemplified the OAIC's strong enforcement mechanism, demonstrating that severe penalties would be imposed in cases of deliberate negligence and data mismanagement. The OAIC's response included issuing fines and mandating improvements in Uber's data protection systems has enhanced its enforcement efficiency. Despite some challenges, the OAIC remains a key player in protecting privacy in Australia and has demonstrated that consistent and proportionate enforcement can improve data protection compliance.

## D. Singapore Personal Data Protection Commission (PDPC)

The Personal Data Protection Commission (PDPC) is Singapore's principal regulatory authority tasked with overseeing and enforcing the Personal Data Protection Act 2012 (PDP Act). Established in 2013, the PDPC plays a crucial role in ensuring that organizations managing personal data in Singapore comply with the nation's data protection laws.<sup>123</sup> The PDPC's objective is to protect individuals' personal data while supporting Singapore's economic growth by fostering trust in data usage and encouraging the development of digital services.<sup>124</sup>

The PDPC's mandate extends beyond merely enforcing the PDP Act; it also works to foster a culture of compliance and responsible data use. The PDPC enhances awareness of personal data protection by educating both organizations and the public about their responsibilities and rights under the law. Additionally, the PDPC helps businesses implement data protection frameworks that allow them to innovate while respecting individuals' privacy.<sup>125</sup>

---

<sup>123</sup> Singapore Government Agency, "Personal Data Protection: Encouraging Data-Driven Innovation While Protecting Personal Data Use," *Infocomm Media Development Authority*, October 10, 2024, <https://www.imda.gov.sg/about-imda/data-protection/personal-data-protection>.

<sup>124</sup> Singapore Government Agency, "Personal Data Protection: Encouraging Data-Driven Innovation While Protecting Personal Data Use." *See also* Chik, Warren B. "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform." *Computer Law & Security Review* 29, no. 5 (2013): 554-575' Wong YongQuan, Benjamin. "Data Privacy Law in Singapore: the Personal Data Protection Act 2012." *International Data Privacy Law* 7, no. 4 (2017): 287-302.

<sup>125</sup> *See* Singapore Government Agency, "Personal Data Protection: Encouraging Data-Driven Innovation While Protecting Personal Data Use."

The PDPC also oversees the regulation of data usage in evolving technologies, such as artificial intelligence (AI) and big data analytics.<sup>126</sup> It promotes data innovation by encouraging organizations to adopt practices that unlock the value of data while ensuring that data protection standards are met.

The jurisdictional scope of the PDPC extends to organizations both within Singapore and those that process data of Singaporean residents, even if they are located outside the country. This extraterritorial jurisdiction is crucial in a globalized digital economy where data flows freely across borders. By applying its authority to foreign entities that handle Singaporeans' data, the PDPC ensures that international companies also comply with Singapore's data protection laws, creating a high standard for privacy across regions.

In terms of sanctioning powers, the PDPC has comprehensive set of tools, including financial penalties (up to SGD 1 million or 10% of annual turnover for larger organizations), compliance warnings and directions, compliance audits and assessments, until the ability to suspend or cease data processing operations.<sup>127</sup> The PDPC's enforcement actions are primarily guided by the PDP Act, with key enforcement actions such as:

- a. Warnings and directions, as a preventive measure which allows the organization to correct its practices before more severe actions are taken. Directions may include instructions to cease particular data processing activities, rectify data breaches, or implement improved data protection measures.<sup>128</sup>
- b. Financial fines, for serious or repeated violations of the PDP Act where the violations have caused significant harm to individuals or where the organization has shown negligence in handling personal data. For grave violations, the PDPC can levy fines of up to SGD \$1 million (approximately USD \$750,000) or 10% of the organization's annual turnover for companies with over SGD \$10 million in turnover.<sup>129</sup>
- c. Compliance notices and cease processing orders, obliging an organization to take particular actions to remedy a breach within stipulated period and in more serious cases, the PDPC may effectively prohibiting the

---

<sup>126</sup> Singapore Info-communications Media Development Authority (IMDA) and Personal Data Protection Commission. *Model Artificial Intelligence Governance Framework*, Second Edition. Singapore: Personal Data Protection Commission, 2020.

<sup>127</sup> See Singapore Personal Data Protection Act 2012, sec. 29(2)(a)-(d) & 50.

<sup>128</sup> See Singapore Personal Data Protection Act 2012, sec. 29(2)(a).

<sup>129</sup> See Personal Data Protection Act 2012, sec. 29(2)(d).

organization from continuing to process personal data until the breach is remedied.<sup>130</sup>

- d. Compliance audits and assessments, to assess whether organizations are adhering to requirements of the PDP Act. This power allows the PDPC to proactively investigate organizations that may pose a high risk of non-compliance, particularly those that handle sensitive data or engage in high-volume data processing.<sup>131</sup>

The PDPC uses a range of penalties to ensure compliance with the PDPA. One notable example is the SingHealth data breach of 2018, which compromised 1.5 million patient records. The PDPC imposed a fine of SGD 1 million on SingHealth and SGD 750,000 on its IT vendor. In addition to the fines, the PDPC required the organizations involved to implement more robust data protection measures, including stronger cybersecurity protocols and regular system audits. Another case happened on December 28, 2023, the PDPC found Carousell in violation of its Protection Obligation under Singapore's Personal Data Protection Act (PDP Act). The company was penalized \$58,000 for failing to implement sufficient security measures to protect user personal data.<sup>132</sup>

With amendments made to the PDP Act in 2020, the PDPC now has greater flexibility and more stringent penalties at its disposal, enabling the Commission to respond more effectively to serious breaches. With fines reaching up to 10% of annual turnover for large companies, the penalties are designed to ensure that organizations treat personal data protection as a critical business priority.<sup>133</sup> Additionally, the enforcement efficiency of the PDPC is evident in its swift response to major data breaches, such as the SingHealth and Carousell incident. The PDPC's approach combines financial penalties with

<sup>130</sup> See Singapore Personal Data Protection Act 2012, sec. 29(2)(c).

<sup>131</sup> See Singapore Personal Data Protection Act 2012. For further context, *also see* Putra, Tegar Islami, et al. "Risks of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites." *Journal of Private and Commercial Law* 8, no. 2 (2024): 110-128; Fernando, Zico Junius, Anis Widyawati, and Kasmento Rinaldi. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1-39.

<sup>132</sup> See Singapore Personal Data Protection Commission, Case No. DP-2209-C0166; DP-2210-C0312 In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Carousell Pte. Ltd. (December 28, 2023)

<sup>133</sup> Allen, Margaret Hope, Ming Yuet Tham, and Faraaz Amzar, "Singapore," in *The Privacy, Data Protection and Cybersecurity Law Review*, ed. Alan Charles Raul, 9th ed. London: Law Business Research Ltd, 2022., pp. 204-218.

corrective measures, ensuring that organizations not only face fines but also take action to prevent future violations. Furthermore, the PDPC’s proactive role in enforcing the PDPA and its ability to issue mandatory breach notifications help ensure that violations are addressed promptly and effectively. This combination of deterrent sanctions and preventative measures makes the PDPCs enforcement mechanisms highly efficient.

E. Lessons from Comparative Models for Indonesia’s PDPA

The development of Indonesia’s Personal Data Protection Act (PDPA) can greatly benefit from examining and learning from the data protection frameworks of other countries.<sup>134</sup> Ireland, Australia, and Singapore have each established comprehensive regulations that address privacy concerns while accommodating the needs of businesses in a rapidly evolving digital landscape. By studying these international models, Indonesia can identify key practices and strategies that may be relevant and effective in its own legal context. The following comparative analysis outlines the regulatory frameworks of these countries, focusing on factors such as enforcement, compliance, data subject rights, and international cooperation, and draws lessons that could help Indonesia build a more robust and adaptive data protection law.

TABLE 1. Comparative Analysis for Indonesia’s PDPA

| Key Factor           | Ireland (DPC)                                                                   | Australia (OAIC)                                                                                      | Singapore (PDPC)                                                                           | Lessons for Indonesia                                                                             |
|----------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Jurisdictional Scope | Extraterritorial reach via GDPR, applies to non-EU companies processing EU data | Applies to Australian and foreign entities processing Australian data. Focus on national coverage but | Applies to both domestic and foreign entities processing Singaporean data. Strong focus on | Indonesia should ensure its PDPA has extraterritorial jurisdiction, applying to foreign companies |

<sup>134</sup> See Marischa, Diva, and Reni Budi Setianingrum. "Transfer of Personal Data by E-Commerce Companies: A Study from the Perspective of Indonesian Personal Data Protection Laws." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 4, no. 1 (2024): 48-64; Rahman, Yogi Muhammad, Aflah Haora, and Elsa Nurfitriani Sutansi. "Personal Data Protection in the Era of Globalization (Indonesia Perspective)." *Tirtayasa Journal of International Law* 2, no. 1 (2023): 15-30; Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding privacy in the digital age: A comparative analysis of data protection strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (2024): 233-251.

| Key Factor             | Ireland (DPC)                                                                                                                           | Australia (OAIC)                                                                                                                                                         | Singapore (PDPC)                                                                                                                                  | Lessons for Indonesia                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        |                                                                                                                                         | also applies to international data transfers.                                                                                                                            | international applicability.                                                                                                                      | handling Indonesian data, similar to GDPR.                                                                                                                                                |
| Sanctioning Powers     | Fines up to €20 million or 4% of global turnover, corrective actions like data processing restrictions and bans.                        | Fines up to AUD 2.1 million, enforceable undertakings requiring corrective actions, and compliance notices.                                                              | Fines up to SGD 1 million or 10% of annual turnover, compliance directions, cease processing orders, and audits.                                  | Indonesia's PDPA should adopt a mix of fines, corrective actions, and compliance orders. Penalties should be proportional and include preventative measures.                              |
| Enforcement Efficiency | Effective enforcement, high-profile cases like Facebook and WhatsApp, but sometimes delayed due to complex cross-border investigations. | Proactive enforcement, especially in large-scale breaches like Optus, but relies on cooperation with other regulators and often faces challenges in international cases. | Efficient enforcement with swift responses to breaches like SingHealth. Proactive audits and breach notifications enhance enforcement efficiency. | Indonesia's PDPA should be independent and adequately resourced for proactive enforcement, similar to PDPC and OAIC. It should include mandatory breach notifications and routine audits. |

Sources: Authors, 2025

The experiences of Ireland, Australia, and Singapore offer valuable lessons for Indonesia as it develops its independent Personal Data Protection Agency (PDPA) under the Personal Data Protection Law (UU PDP). One critical lesson is the importance of establishing a jurisdictional scope that allows Indonesia to regulate both domestic and international entities that handle Indonesian citizens' data. Indonesia's PDPA should adopt an extraterritorial jurisdiction similar to that of the GDPR, ensuring that foreign companies must comply with Indonesian data protection laws when processing Indonesian personal data. This would prevent Indonesia from being left behind in the increasingly globalized digital economy, where cross-border data flows are the norm.

In terms of sanctioning powers, Indonesia can benefit from adopting a mix of penalties similar to those in Ireland, Australia, and Singapore. The DPC has the power to impose fines up to 4% of global turnover for severe violations, sending a strong deterrent message to organizations that mishandle personal data. Similarly, the OAIC in Australia and the PDPC in Singapore utilize a mix of fines, compliance orders, and corrective actions to address non-compliance. Financial penalties, along with compliance orders and corrective actions, should form the backbone of Indonesia's enforcement strategy. However, the PDPA should ensure that penalties are proportional to the severity of the violation and include both preventive and punitive elements. This balance will help deter non-compliance while also enabling businesses to improve their data protection practices without stifling innovation.<sup>135</sup>

Therefore, the enforcement efficiency of Indonesia's PDPA can be enhanced by ensuring that the PDPA is independent and equipped with the necessary resources to handle complex investigations and breaches. Drawing inspiration from the PDPC and OAIC, Indonesia should adopt a proactive approach that includes mandatory data breach notifications and routine audits of companies' data protection practices. Furthermore, collaboration with regional bodies like ASEAN and alignment with global frameworks such as the GDPR will ensure that Indonesia's PDPA is not only effective within its borders but also respected internationally.

Singapore's leadership within ASEAN offers a significant example of how countries can cooperate regionally to enhance data protection standards. While Indonesia should maintain focus on national priorities, it is also crucial to align its PDPA with regional frameworks such as the ASEAN Framework on Personal Data Protection. Singapore has been at the forefront of setting regional standards for data protection, and its PDPC plays a leading role in shaping the region's data protection agenda. Indonesia can benefit from this leadership by aligning its PDPA with ASEAN standards, which will foster regional cooperation and facilitate cross-border data flow. By learning from these models, Indonesia can develop a comprehensive data protection regime that is both rigorous and adaptive to the challenges of the digital age.

---

<sup>135</sup> Martin, Nicholas, et al. "How data protection regulation affects startup innovation." *Information Systems Frontiers* 21, no. 6 (2019): 1307-1324.

## Recommendations for Indonesia's PDPA Design and Implementation

As Indonesia establishes its Personal Data Protection Agency under the Personal Data Protection Law (UU PDP), it is essential to implement effective strategies that ensure the agency's ability to enforce data protection regulations and uphold the privacy rights of individuals. Drawing on lessons from global examples like Ireland, Australia, and Singapore, this section outlines key recommendations for ensuring the PDPA's success in Indonesia.

### A. Ensuring Independence and for Indonesia's PDPA Design and Implementation

For the PDPA to be effective in safeguarding personal data, it must operate with complete independence from political influence. This ensures that enforcement actions are based solely on legal principles and data protection concerns, rather than political pressures. The PDPA must be structured as an autonomous entity, directly reporting to the President or another high-level governmental body, ensuring that its decisions are not swayed by day-to-day political changes.<sup>136</sup>

Moreover, the leadership of the PDPA should be selected through a transparent and merit-based process, focusing on candidates with extensive expertise in data protection, law, and technology. Ensuring a politically neutral recruitment process for key officials will further strengthen the PDPA's credibility and public trust. It is also crucial that the agency's budget remains stable and secure, with adequate resources allocated to carry out its duties effectively. Independence in budgeting will prevent potential political interference and ensure the PDPA's financial autonomy, thus allowing it to operate efficiently.<sup>137</sup>

### B. Enhancing Regulatory Capacity and Expertise

---

<sup>136</sup> Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431-455.

<sup>137</sup> Djafar, Wahyudi, and M. Jodi Santoso. *Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Indonesia: Seri HAM dan Internet*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (eLSAM) & Australian Government- Department of Foreign Affairs and Trade (DFAT), 2019.

The regulatory capacity of the PDPA will determine its success in enforcing the law and ensuring compliance across various sectors. For the PDPA to be effective, it must be equipped with highly skilled personnel and specialized knowledge in areas such as data security, digital forensics, and cyber law. Building the PDPA's expertise through continuous training is crucial for staying ahead of emerging threats in the fast-evolving digital environment.<sup>138</sup>

Additionally, Indonesia should foster international cooperation with data protection authorities in countries like Ireland, Australia, and Singapore to facilitate knowledge-sharing, improve technical capabilities, and align with global standards. This collaboration can include joint training programs, conferences, and workshops to exchange insights on tackling complex data breaches and other privacy issues. Furthermore, the PDPA must also adopt modern technological tools for data breach detection, case management, and reporting, ensuring that enforcement is timely and efficient.

## C. Strengthening Public Awareness and Compliance Culture

A crucial element for the success of Indonesia's PDPA is creating a strong compliance culture among both organizations and the public. The PDPA should lead the way by implementing nationwide awareness campaigns to educate both businesses and individuals about their rights and responsibilities under the new data protection law. These campaigns should emphasize the importance of data security and the consequences of non-compliance, providing practical steps for organizations to safeguard personal data.<sup>139</sup>

Furthermore, businesses should be encouraged to integrate data protection by design and data protection by default into their operations. This will ensure that privacy measures are embedded into the processes of companies from the outset. The PDPA should also collaborate with educational institutions to include data protection literacy in school curricula, equipping the next generation with the knowledge to understand and respect privacy rights. Additionally, promoting public understanding of their privacy rights—such as the right to access and correct their data—will encourage greater participation in the data protection ecosystem.

---

<sup>138</sup> Djafar, and Santoso, p. 25.

<sup>139</sup> Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)."

## D. Legal and Institutional Reforms to Improve Enforcement

In order to strengthen the effectiveness of enforcement, Indonesia must implement legal and institutional reforms that address the challenges of the current data protection framework. The PDPA must be granted clear authority and responsibility for handling all matters related to personal data protection, which will help avoid jurisdictional overlaps with other existing regulatory bodies like Kominfo or BSSN. This clarity in roles and responsibilities is vital for ensuring smooth enforcement operations and avoiding confusion among businesses and the public.<sup>140</sup>

Moreover, the sanctions available under the PDPA should be proportionate to the severity of the violations. Drawing inspiration from the GDPR, Indonesia's data protection law should include financial penalties, compliance orders, and the authority to suspend or ban data processing activities when necessary. However, sanctions should not only be punitive; they must also have a preventive effect, encouraging businesses to adopt proactive measures to comply with data protection laws. Establishing clear guidelines for the application of sanctions will ensure consistency in enforcement, providing transparency for businesses and individuals alike.

Additionally, the PDPA should ensure that its enforcement mechanisms are flexible and adaptable to emerging technologies and new types of data processing. With the rapid growth of fields like artificial intelligence (AI) and big data, the PDPA will need the flexibility to regulate and enforce rules related to these technologies, which often raise unique data privacy concerns. To this end, the PDPA should regularly review its enforcement strategies to keep up with the evolving digital landscape, ensuring that enforcement remains robust and effective.

## Conclusion

Based on the research findings, it is clear that Indonesia's Personal Data Protection (PDP) Law is a critical step forward in safeguarding the privacy of its citizens. However, its enforcement mechanisms are hindered by the lack of a dedicated agency responsible for administrative sanctions. This study highlights the importance of establishing an independent Personal Data

---

<sup>140</sup> Mahardika, Ahmad Mahardika. "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi dalam Sistem Ketatanegaraan Indonesia." *Jurnal Hukum* 37, no. 2 (2021): 101-118.

Protection Agency (PDPA) to ensure that data protection laws are effectively implemented. Comparative analysis with enforcement practices in Ireland, Australia, and Singapore reveals that these countries have achieved significant success through independent, empowered agencies. By adopting similar structures and practices, Indonesia can improve its legal framework, address jurisdictional overlaps, and effectively handle data breaches.

The immediate creation of the PDPA, supported by adequate resources, political will, and institutional independence, is essential for enhancing data protection in Indonesia. Furthermore, the PDPA should be equipped with sufficient legal authority to impose sanctions, conduct audits, and ensure compliance, thereby fostering a culture of data protection among businesses and individuals. International cooperation and alignment with regional frameworks, such as the ASEAN Personal Data Protection Framework, will also be crucial for improving cross-border data governance. In conclusion, establishing a robust and independent PDPA is the cornerstone for ensuring that Indonesia's data protection laws fulfill their intended purpose, protect individual privacy, and support Indonesia's digital economy.

## References

- Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." *Lex Scientia Law Review* 7, no. 2 (2023): 995-1048.
- Ahmad, Rumadi. "Lembaga Perlindungan Data Pribadi," *kompas.id*, July 21, 2024, <https://www.kompas.id/baca/opini/2024/07/19/lembaga-perlindungan-data-pribadi>.
- Aktipis, Michael S., and Ron B. Katwan. "Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (CJEU)." *International Legal Materials* 60, no. 1 (2021): 53-98.
- Ali, Salim Ibrahim, Zuryati Mohamed Yusoff, and Zainal Amin Ayub. "Legal research of doctrinal and non-doctrinal." *International Journal of Trend in Research and Development* 4, no. 1 (2017): 493-495.
- Allen, Margaret Hope, Ming Yuet Tham, and Faraaz Amzar, "Singapore," in *The Privacy, Data Protection and Cybersecurity Law Review*, ed. Alan Charles Raul, 9th ed. London: Law Business Research Ltd, 2022., pp. 204-218.

- Arifin, Ridwan, et al. "Improving Law Student Ability on Legal Writing through Critical and Logical Thinking by IRAC Method." *Indonesian Journal of Advocacy and Legal Services* 1, no. 1 (2019): 107-128.
- ASEAN Member States, "Framework on Personal Data Protection," Asean Telecommunications and Information Technology Ministers Meeting (TELMIN) (Bandar Seri Begawan: ASEAN, November 25, 2016), <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>.
- Australia, "Privacy Act 1988 (Cth)" (2024), <https://www.legislation.gov.au/C2004A03712/latest/text>
- Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431-455.
- Badan Siber dan Sandi Negara, "Tentang Kami - Badan Siber dan Sandi Negara," Badan Siber dan Sandi Negara, accessed April 7, 2025, <https://bssn.acaraseru.id/bssn.acaraseru.id>.
- Bagiarto, Widodo. "Pakar Kritik Menkominfo Anggap Tak Penting Pengamanan Siber," Rmol.id, accessed April 7, 2025, <https://rmol.id/politik/read/2023/12/03/599796/pakar-kritik-menkominfo-anggap-tak-penting-pengamanan-siber>.
- Banisar, David, and Simon G. Davies. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *John Marshall Journal of Computer & Information Law* 18, no. 1 (1999): 1-15.
- Basarah, Ahmad. "Kajian Teoritis Terhadap Auxiliary States Organ dalam Struktur Ketatanegaraan Indonesia." *Masalah-Masalah Hukum* 43, no. 1 (2014): 1-8.
- Budiman, Ahmad. "Otoritas Pengawas Pelindungan Data Pribadi," *Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis* XIII, no. 5 (February 2021): 26, [https://berkas.dpr.go.id/pusaka/files/info\\_singkat/Info%20Singkat-XIII-5-I-P3DI-Maret-2021-181.pdf](https://berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XIII-5-I-P3DI-Maret-2021-181.pdf).
- Burgess, Matt. "How GDPR Is Failing," *Wired*, accessed March 20, 2025, <https://www.wired.com/story/gdpr-2022/>.
- Changshan, Ma. "The Fourth Generation of Human Rights' Under the Background of Smart Society and Its Protection." *China Legal Science* 5, no. 1 (2019): 5-24.

- Chik, Warren B. "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform." *Computer Law & Security Review* 29, no. 5 (2013): 554-575.
- CNN Indonesia, "Ribuan Data Pemerintah Diduga Bocor, Termasuk Prakerja Hingga CPNS," *CNN Indonesia*, April 9, 2022, <https://www.cnnindonesia.com/teknologi/20220408160348-192-782309/ribuan-data-pemerintah-diduga-bocor-termasuk-prakerja-hingga-cpns>.
- Daigle, Brian, and Mahnaz Khan. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce and Economics* (June 2020): 1-38.
- Data Protection Commission Ireland, The Data Protection Commission, <https://www.dataprotection.ie/en>.
- Data Protection Commission, "Data Protection Commission Announces Conclusion of Inquiry into WhatsApp," *News & Media*, January 19, 2023, <https://www.dataprotection.ie/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp>.
- Data Protection Commission, "Data Protection Commission Announces Decision in Facebook 'Data Scraping' Inquiry," *News & Media*, November 28, 2022, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry>.
- Data Protection Commission, "One Stop Shop (OSS)," International Transfers, accessed March 20, 2025, <https://www.dataprotection.ie/organisations/international-transfers/one-stop-shop-oss>.
- Dirgantara, Adhyasta, and Dani Prabowo, "Data PeduliLindungi Bocor, Pemerintah Diminta Tak Saling Lempar Tanggung Jawab," *KOMPAS*, November 18, 2022, <https://nasional.kompas.com/read/2022/11/18/05230361/data-pedulilindungi-bocor-pemerintah-diminta-tak-saling-lempar-tanggung?page=all>
- Djafar, Wahyudi, and M. Jodi Santoso. *Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Indonesia: Seri HAM dan Internet*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (eLSAM) & Australian Government-Department of Foreign Affairs and Trade (DFAT), 2019.
- Doly, Denico. "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of

- a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)." *Negara Hukum: Membangun Hukum untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223-244.
- European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 679 (2016). <https://data.europa.eu/eli/reg/2016/679/oj>.
- Fernando, Zico Junius, Anis Widyawati, and Kasmanto Rinaldi. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1-39.
- Finck, Michèle, and Frank Pallas. "They who must not be identified—distinguishing personal from non-personal data under the GDPR." *International Data Privacy Law* 10, no. 1 (2020): 11-36.
- Flaherty, David H. *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*. North Carolina: UNC Press Books, 2014.
- Greenleaf, Graham. "Independence of data privacy authorities (Part I): International standards." *Computer Law & Security Review* 28, no. 1 (2012): 3-13.
- Haniver, Rob. "Ireland - Data Protection Overview: Guidance Note". *DataGuidance*, (2024), <https://www.dataguidance.com/notes/ireland-data-protection-overview>.
- Howie, Emily. "Protecting the human right to freedom of expression in international law." *International Journal of Speech-Language Pathology* 20, no. 1 (2018): 12-15.
- Hunt, Jon, Robert Neely, and Melissa Tan, "Uber Decision a Stark Reminder of the Extraterritorial Reach of the Privacy Act 1988 (Cth)," *Lander & Rogers*, August 2021, <https://www.landersonline.com.au/legal-insights-news/uber-decision-reminder-of-extraterritorial-reach-of-privacy-act>.
- Imaduddin, Achmad Hanif. "Dari Jaga NIK Hingga Ganti Password, Berikut Deretan Pernyataan Kontroversial Menkominfo," *tempo.co*, September 8, 2022, <https://www.tempo.co/politik/dari-jaga-nik-hingga-ganti-password-berikut-deretan-pernyataan-kontroversial-menkominfo-293535>.
- Karina, Dina. "44 Juta Data MyPertamina Diduga Bocor, Pertamina dan Telkom Bakal Investigasi," *Kompas TV*, November 11, 2022,

- [https://www.kompas.tv/bisnis/347339/44-juta-data-mypertamina-diduga-bocor-pertamina-dan-telkom-bakal-investigasi#google\\_vignette](https://www.kompas.tv/bisnis/347339/44-juta-data-mypertamina-diduga-bocor-pertamina-dan-telkom-bakal-investigasi#google_vignette)  
Kementerian Komunikasi dan Digital, "Ruang Lingkup, Tugas, Dan Fungsi," Komdigi, accessed April 7, 2025, <https://www.komdigi.go.id/profil/tugas-fungsi>.
- Lamdayoung, Cindy Thia. "Loss Due to Data Leaks: How is the Legal Protection for Account Owners on Marketplace?." *Journal of Creativity Student* 5, no. 1 (2020): 25-42.
- Lembaga Studi dan Advokasi Masyarakat (eLSAM). *Skenario Pembuatan Otoritas Pelindungan Data Pribadi Di Indonesia: Opsi dan Implikasi: Seri HAM dan Internet*. Jakarta: ELSAM, 2022. <https://www.elsam.or.id/policy-paper/skenario-pembentukan-otoritas-pelindungan-data-pribadi-di-indonesia--opsi-dan-implikasi>.
- Macpherson, John, Tim Brookes, Amanda Ludlow, Geoff McGrath, and Andrew Hilton. "Australia's Massive New Privacy Penalties Become Law but Will Be Clarified," *Ashurst Business Insight*, December 2, 2022, <https://www.ashurst.com/en/insights/australias-massive-new-privacy-penalties-become-law-but-will-be-clarified/>.
- Mahardika, Ahmad Mahardika. "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi dalam Sistem Ketatanegaraan Indonesia." *Jurnal Hukum* 37, no. 2 (2021): 101-118.
- Mangar, Irma, and Muhammad Rosyid Ridho. "Lembaga Independen Negara dalam Ketatanegaraan Indonesia." *Definisi: Jurnal Agama Dan Sosial Humaniora* 1, no. 2 (2022): 75-84.
- Marischa, Diva, and Reni Budi Setianingrum. "Transfer of Personal Data by E-Commerce Companies: A Study from the Perspective of Indonesian Personal Data Protection Laws." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 4, no. 1 (2024): 48-64.
- Martin, Nicholas, et al. "How data protection regulation affects startup innovation." *Information Systems Frontiers* 21, no. 6 (2019): 1307-1324.
- Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *Justisi* 10, no. 1 (2024): 20-35.
- McMillan, John. "Privacy-a regulator's perspective." *AIAL Forum*, no. 83 (2016): 78-82.
- Mertokusumo, Sudikno. *Penemuan Hukum: Sebuah Pengantar*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2010.

- Mishova, Ana. "Data Protection Laws Around the World: A Global Perspective," *GDPR Local*, August 16, 2024, <https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/>.
- Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding privacy in the digital age: A comparative analysis of data protection strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (2024): 233-251.
- Office of the Australian Information Commissioner (OAIC), "Australian Privacy Principles Guidelines: Privacy Act 1988" (Sydney: Office of the Australian Information Commissioner (OAIC), December 2022), <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>.
- Office of the Australian Information Commissioner (OAIC), "Australian Privacy Principles Guidelines," OAIC, March 10, 2023, <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>.
- Office of the Australian Information Commissioner (OAIC), "Guide to Securing Personal Information," OAIC, March 10, 2023, <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>
- Office of the Australian Information Commissioner (OAIC), "OAIC Corporate Plan 2024–25," OAIC Corporate Plan (Sydney: Office of the Australian Information Commissioner (OAIC), August 29, 2024), 5, <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25>.
- Office of the Australian Information Commissioner (OAIC), "Part 1: Introduction to the Freedom of Information Act 1982," OAIC, March 10, 2023, <https://www.oaic.gov.au/freedom-of-information/freedom-of-information-guidance-for-government-agencies/foi-guidelines/part-1-introduction-to-the-freedom-of-information-act-1982>.
- Office of the Australian Information Commissioner (OAIC), "Privacy Regulatory Action Policy," OAIC, February 17, 2025, <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy>.
- Office of the Australian Information Commissioner (OAIC), "Uber Found to Have Interfered with Privacy," OAIC, March 10, 2023, <https://www.oaic.gov.au/news/media-centre/uber-found-to-have-interfered-with-privacy>.

- Office of the Australian Information Commissioner (OAIC), "What We Do," OAIC, February 20, 2025, <https://www.oaic.gov.au/about-the-OAIC/what-we-do>.
- Ombudsman Republik Indonesia, "Tugas Dan Fungsi," Profil Tugas dan Fungsi, accessed April 8, 2025, <https://ombudsman.go.id/profiles/index/pfft>.
- Otoritas Jasa Keuangan, "Tugas Dan Fungsi," Tentang OJK, accessed April 8, 2025, <https://ojk.go.id/id/tentang-ojk/pages/tugas-dan-fungsi.aspx>.
- Palupy, Heppy Endah. "Privacy and data protection: Indonesia legal framework." *Thesis of Master Program in Law and Technology*, Tilburg: Tilburg University, 2011.
- Prima, Erwin. "LockBit Klaim Bobol 1,5 TB Data Pribadi, Pengamat Minta BSI Siapkan Mitigasi," *TEMPO*, May 2023, <https://www.tempo.co/digital/lockbit-klaim-bobol-1-5-tb-data-pribadi-pengamat-minta-bsi-siapkan-mitigasi-188407>.
- Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, and Moh Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (2020): 182-200.
- Putra, Tegar Islami, et al. "Critically Reveal the Dimensions of Damage from Unauthorized Use of Personal Data (Study of Decision Number 78/Pid. Sus/2024/PN Tng)." *The Digest: Journal of Jurisprudence and Legisprudence* 5, no. 2 (2024): 231-262.
- Putra, Tegar Islami, et al. "Risks of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites." *Journal of Private and Commercial Law* 8, no. 2 (2024): 110-128.
- Putra, Tegar Islami, Nurul Fibrianti, and Adinda Zeranica Putri Fakhis. "Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection." *The Indonesian Journal of International Clinical Legal Education* 7, no. 2 (2025): 203-234.
- Putri, Riani Sanusi. "Saling Lempar Tanggung Jawab Atasi Kebocoran Data Pribadi," *TEMPO*, accessed March 29, 2025, <https://www.tempo.co/arsip/saling-lempar-tanggung-jawab-atasi-kebocoran-data-pribadi-290025>.
- Rahim, Erman I., et al. "Personal Data Protection in Political Party Information Systems in the Organization of General Elections: Concept and Law Reform Recommendations." *Journal of Law and Legal Reform* 6, no. 3 (2025): 1305-1348.
- Rahman, Yogi Muhammad, Aflah Haora, and Elsa Nurfitriani Sutansi. "Personal Data Protection in the Era of Globalization (Indonesia

- Perspective)." *Tirtayasa Journal of International Law* 2, no. 1 (2023): 15-30.
- Republic of Indonesia, "Law of the Republic of Indonesia No. 39 Year 1999 Concerning Human Rights," Pub. L. No. 39, § preamble (1999).
- Republic of Indonesia, Law of the Republic of Indonesia No. 27 Year 2022 on Personal Data Protection (UU PDP)," Pub. L. No. 27 (2022). [https://jdih.setkab.go.id/PUUdoc/176837/Salinan\\_UU\\_Nomor\\_27\\_Tahun\\_2022.pdf](https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf).
- Rettob, Krisna. "Perlindungan HAM Di Era Digital Dalam Perspektif Pelayanan Publik," *Online Article*, Ombudsman RI, December 2024, <https://ombudsman.go.id:443/artikel/r/artikel--perlindungan-ham-di-era-digital-dalam-perspektif-pelayanan-publik>.
- Rizkinaswara, Leski. *Data pelanggan PLN bocor, kominfo: Sudah dipanggil dan terus dipantau*, Ditjen Aptika Kominfo (Aug. 22, 2022), <https://aptika.kominfo.go.id/2022/08/data-pelanggan-pln-bocor-kominfo-sudah-dipanggil-dan-terus-dipantau/>
- Rosadi, Sinta Dewi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78-90.
- Rosadi, Sinta Dewi. "Data Privacy Law in the Application of Smart City in Indonesia." *Journal of Legal, Ethical and Regulatory Issues* 24, no. 4S (2021): 1-9.
- Salwa, Nikita Dewi Kurnia. "Tantangan & Hambatan Besar Yang Dihadapi CSIRT-BSSN Indonesia," *Computer Security Incident Respond Team Indonesia*, November 18, 2024, <https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn>.
- Saraswati, Retno, Zainal Arifin Hoesein, and Susi Dian Rahayu. "Implementation of Administrative Sanctions in Abuse Law Enforcement Utilization of Green Open Space in Bekasi City." *IOP Conference Series: Earth and Environmental Science*. Vol. 1270. No. 1. IOP Publishing, 2023.
- Schwartz, Paul M. "Global Data Privacy: The EU Way." *New York University Law Review* 94, no. 4 (2019): 771-818.
- Sinaga, Guna Gerhat, et al. "Analisis Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia)." *Jurnal Pendidikan Tambusai* 7, no. 3 (2023): 28374-28383.
- Singapore Government Agency, "Personal Data Protection: Encouraging Data-Driven Innovation While Protecting Personal Data Use," *Infocomm Media Development Authority*, October 10, 2024,

<https://www.imda.gov.sg/about-imda/data-protection/personal-data-protection>.

Singapore Info-communications Media Development Authority (IMDA) and Personal Data Protection Commission. *Model Artificial Intelligence Governance Framework*, Second Edition. Singapore: Personal Data Protection Commission, 2020.

Singapore Personal Data Protection Commission, Case No. DP-2209-C0166; DP-2210-C0312 In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Carousell Pte. Ltd. (December 28, 2023)

Singapore, Personal Data Protection Act (2012), <https://sso.agc.gov.sg/Act/PDPA2012>.

Singapore, Personal Data Protection Commission Singapore, "Enforcement of the Act," PDPC Singapore, March 22, 2025, <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/enforcement-of-the-act>.

Surfshark, "Data Breach Statistics Globally," Global data breach statistics, Surfshark, January 28, 2025, <https://surfshark.com/research/data-breach-monitoring>.

Suwondo, Denny. "The Legal Protection of Personal Data in the Perspective of Human Rights." *Law Development Journal* 5, no. 4 (2021): 419-429.

Tan, Steve and Victoria Tan, "Understanding How the PDPA Permits Organisations to Leverage on Personal Data in Achieving Innovation," in *Personal Data Protection Digest*, ed. Yeong Zee Kin. Singapore: Academy Publishing, 2023.

Voss, W. Gregory. "Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems II." *Colorado Technology Law Journal* 19, no. 2 (2021): 377-427.

Voss, W. Gregory. "The CCPA and the GDPR are not the same: why you should understand both." *CPI Antitrust Chronicle* 1, no. 1 (2021): 7-12.

Wibowo, Ari, Widya Alawiyah, and Azriadi. "The importance of personal data protection in Indonesia's economic development." *Cogent Social Sciences* 10, no. 1 (2024): 2306751.

Widiatedja, I. Gusti Ngurah Parikesit, and Neha Mishra. "Establishing an independent data protection authority in Indonesia: a future-forward perspective." *International Review of Law, Computers & Technology* 37, no. 3 (2023): 252-273.

- Wolff, Josephine, and Nicole Atallah. "Early GDPR penalties: Analysis of implementation and fines through May 2020." *Journal of Information Policy* 11 (2021): 63-103.
- Wong YongQuan, Benjamin. "Data Privacy Law in Singapore: the Personal Data Protection Act 2012." *International Data Privacy Law* 7, no. 4 (2017): 287-302.
- Yamin, Ahmad Fachri, et al. "Perlindungan data pribadi dalam era digital: Tantangan dan solusi." *Meraja Journal* 7, no. 2 (2024): 138-155.
- Yolanda, Erlyns, and Rugun Romaida Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif." *Journal of Syntax Literate* 8, no. 6 (2023): 4166-4182.
- Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?." *Pandecta Research Law Journal* 19, no. 2 (2024): 173-202.
- Zhang, Yueming. "Processing of personal data by public authorities in China: assessing equivalence for cross-border transfers from the EU to China." *European Journal of Law and Technology* 14, no. 1 (2023).

\*\*\*

### **Acknowledgment**

This study was conducted by Firsta Rahadatul 'Aisy and A.M. Adzkiya' Amiruddin as the scholarship awardees provided by the Indonesian Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan RI, LPDP) to pursue a master's degree in law at The University of Melbourne and Universitas Indonesia. The authors would like to express their sincere gratitude to Muhammad Azil Maskur from Universitas Negeri Semarang for his valuable input and assistance during the revision process. Appreciation is also extended to the anonymous reviewer for their insightful feedback, and to the editorial team of the *Journal of Indonesian Legal Studies* for their support and guidance throughout the publication process.

### **Funding Information**

The research was supported and funded by the Indonesian Endowment Fund for Education Agency (*Lembaga Pengelola Dana Pendidikan RI, LPDP*).

### **Conflicting Interest Statement**

The authors state that there is no conflict of interest in the publication of this article.

### **Generative AI Statement**

None

### ***Notification***

Starting from the 2024 issue, our journal has transitioned to a new platform for an enhanced reading experience. All new articles and content will now be available on this updated site. However, we would like to assure you that archived issues from 2016 to 2023 are still accessible via the previous site. You can view these editions by visiting the following link: <https://journal.unnes.ac.id/sju/jils/issue/archive>.