SRIWIJAYA CRIMEN AND LEGAL STUDIES
FACULTY OF LAW UNIVERSITAS SRIWIJAYA
Jalan Srijaya Negara, Palembang, 30139, Indonesia
Email: scls@fh.unsri.ac.id
http://journal.fh.unsri.ac.id/index.php/SCLS/index
E-ISSN: 2987-7350 P-ISSN: 2986-6367

SECURING THE FUTURE: INDONESIA PERSONAL DATA PROTECTION LAW AND IT' S IMPLICATION FOR INTERNET OF THINGS (IOT) DATA PRIVACY

Muhamad Alfat Fauzie

Faculty of Law, University of Melbourne, Australia, E-mail: fauzie.alfat94@gmail.com

Article

Keywords:

Indonesia, Personal Data Protection Law, IoT, data privacy, GDPR.

DOI:
10.28946/scls.v2i1.3743

Abstract

This paper examines Indonesia's Personal Data Protection Law (PDP Law) in the rapidly expanding Internet of Things (IoT) context. It explores the effectiveness of the PDP Law in safeguarding personal data amidst increasing IoT integration in various sectors, notably smart homes and wearable technology. Inspired by the EU's General Data Protection Regulation (GDPR), the PDP Law addresses data protection with specific regard to the unique challenges posed by IoT, such as extensive data collection and heightened vulnerability to breaches. Through a comparative analysis with GDPR, the paper highlights strengths and potential areas for improvement within the Indonesian framework, suggesting enhancements like incorporating privacy by design, establishing a robust data protection authority, and creating detailed guidelines for IoT data handling. The goal is to enhance the PDP Law's capability to manage privacy risks in an interconnected digital era, ensuring adequate data protection and compliance with global standards.

A. INTRODUCTION

In an era characterized by rapid technological advancement, the use of automation machines and artificial intelligence cannot be avoided. This advancement, without a doubt, brings convenience to humans in various sectors of activities.[1] One example is the Internet of Things (IoT), which embodies the interconnectedness of devices capable of autonomously gathering, exchanging, and processing large amounts of data.[2] This technology has found applications in various sectors globally, including the development of smart homes, where IoT devices can manage and automate household functions efficiently.

[1] Hussain Matar Mohamed Ghaith Alhosani, Amiruddin Ahhamat, and Norain Ismail, "Industrial Revolution 4.0 (IR 4.0) Competencies: A Literature Review of Manufacturing Industry," *Ethical and Regulatory*, no. 1 (2021): 3.
[2] Dejan Ilic, Branko Markovic, and Dragan Milosevic, "Strategic Business Transformation: An Industry 4.0 Perspective," *International Journal of Economics and Law 49*, 2017, 50.

In Indonesia, the adoption of IoT technology is particularly noteworthy, with an estimated 135 million IoT connections across diverse sectors. This technological integration revolutionizes Indonesians' daily lives by incorporating IoT in smart homes and wearable technology, reflecting a significant shift towards a more interconnected and efficient lifestyle. This growth trajectory aligns with the Indonesian government's strategic vision, which positions IoT as a key driver in the nation's transition towards future technology development. Complemented by the ongoing expansion of 5G networks, these developments signify a commitment to technological advancement and forecast a future of continued innovation and increased IoT adoption in Indonesia.[3]

The rapid adoption of Internet of Things (IoT) technology, while offering numerous benefits, raises significant concerns regarding privacy and security. The implementation of IoT in smart homes, for instance, involves extensive communication and data transfer among various devices, utilizing different protocols and technologies.[4] This protocol diversity, each with varying security levels, can create vulnerabilities. The potential for a 'weak link' in any device could allow hackers to compromise the entire network, posing a substantial risk to consumer privacy and safety.[5]

This security issue was highlighted in a 2017 research project funded by the Australian Communications Consumer Action Network (ACCAN), which investigated security vulnerabilities in consumer IoT devices. It tested 20 consumer IoT devices, including cameras, motion sensors, smoke alarms, sleep and weighing scales, air quality monitors, light bulbs, power switches, talking dolls, photo frames, printers, controllers, voice assistants, smart TVs, and smart speakers. The findings were concerning. Every single device tested exhibited some form of security flaw, with many presenting potentially serious security issues. This research underscores the need for security measures in IoT devices, especially given their increasing integration into daily life and the consequent risk to consumer privacy and safety.[6]

In response to these challenges, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), effective October 17, 2022, with mandatory enforcement beginning in 2024.[7] Inspired by the European Union's General Data Protection Regulation (GDPR)[8], the PDP Law shares many similarities with GDPR but presents distinct differences and implementation challenges. The effectiveness of the PDP Law hinges on several factors, including the awareness and compliance levels among data controllers and processors, the capacity and authority of the Personal Data Protection Authority (PDPA), and the interplay of political and economic interests within the Indonesian context. These elements suggest that the PDP Law's impact in safeguarding personal data might differ from that of the GDPR, especially concerning their respective extraterritorial effects. The success of the PDP Law in Indonesia thus hinges on addressing these specific challenges and adapting its enforcement mechanisms to the local context.

This paper aims to critically examine the capabilities of the PDP Law in mitigating privacy risks, with a particular focus on the Internet of Things (IoT). The paper will conduct a

[3] Statista Research Department, "Topic: Internet of Things (IoT) in Indonesia," Statista, n.d.
[4] Thanaphol Pattanasri, "Mandatory Data Breach Notification and Hacking the Smart Home: A Legal Response to Cybersecurity," *QUT Law Review* 18, no. 2 (2018): 7.
[5] "The Internet of Things - An Introduction to Privacy Issues with a Focus on the Retail and Home Environments," Office of the Privacy Commissioner of Canada, n.d.
[6] Vijay Sivaraman, Hassan Habibi Gharakheili, and Clinton Vernandes, "Inside Job: Security and Privacy Threats for Smart-Home IoT Devices," *Australian Communications Consumer Action Network, 2017*, 2017, 7–10.
[7] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection]" (n.d.).
[8] "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 Da" (n.d.).

comparative analysis with the European Union's General Data Protection Regulation (GDPR) to achieve this. This comparative approach will facilitate the extraction of insights and the formulation of recommendations based on effective practices observed in GDPR's application. By doing so, the paper aspires to contribute meaningfully to the ongoing discourse on data protection and privacy, with a specific emphasis on IoT and a broader perspective on data protection.

B. RESEARCH METHODS

This research is normative legal research using a statutory and case approach. Primary data from this research comes from statutory regulations, and secondary data comes from other sources with the same research theme, such as books, journals, official websites, etc. This research was analyzed using qualitative descriptive analysis.

C. ANALYSIS AND DISCUSSION

1. IOT and the Risk It Carries

The Internet of Things (IoT) represents a significant shift in the digital landscape, moving from the realm of intangible digital data to the tangible physical world.[9] This concept encapsulates a network of interconnected devices, often called 'Things,' that communicate and operate autonomously, often with little human intervention.[10] There is no single commonly accepted definition of the IoT. Still, most scholars would agree that the IoT is a concept that refers to a network of interconnected physical objects equipped with sensors and internet connectivity, capable of autonomously storing, processing, and exchanging data without human intervention. This definition is derived from the characteristics of IoT, which have physical objects in the physical world capable of connecting to the internet and communicating with other devices over a network.

IoT can store data received either by input from humans in the initial installment or by using sensors built into the devices. Many devices in IoT contain microelectromechanical systems sensors, which translate physical phenomena, like movement, heat, pressure, or location, into digital information.[11] These sensors are incorporated into consumer devices and together, the collective interaction of these consumer devices creates the digital phenomenon known as the IoT. Examples of IoT devices include innovative technology like smart speakers, intelligent door locks, fitness and health wearables, bright lighting, networked thermostats, smart TVs, robot vacuums, indoor security systems, smart locks and most of the devices with sensor and networking functions attached to it can be considered to be IoT.[12]

The most known implementation of IoT would be the smart home application, which introduced the convenience for users to enjoy everyday facilities in their homes automatically by simply specifying what tasks the user wants the device to perform.[13] In this implementation, all smart household devices are connected to the internet, which allows them to send and receive data over a network. For example, we can change the brightness of a smart lightbulb to suit our eyes or turn off the light at midnight to save electricity automatically by commanding them over the phone firsthand. In this case, the user's phone device is connected to a smart

[9] Guido Noto La Diega, "Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies," *Milton, UNITED KINGDOM: Taylor & Francis Group*, 2022, 2.
[10] Noto La Diega, "No," n.d., 21.
[11] Scott R Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consen," *SSRN Scholarly Paper*, n.d., 98.
[12] cltc2015, "New CLTC Report Highlights Privacy Risks in the 'Internet of Things' - CLTC UC Berkeley Center for Long-Term Cybersecurity," CLTC (blog), n.d.
[13] Pattanasri, *Mandatory Data Breach Notification and Hacking the Smart Home*, n.d.

lightbulb over the internet, which means even when the user is outside the house, the user can still command the smart lightbulb as long as the user can connect—giving the ultimate sensation of complete control over the house.

As far as the benefit it gets, IoT comes with its inherent risk, especially regarding privacy data. Different smart devices will need different kinds of information take for example, a smart lightbulb will require customer preferences on when the light should be turned off, or the smart door lock will need each family member's fingerprints to open the locked door. The information IoT needs will vary depending on the task it requires, and this data can range from trivial data such as temperature, motion, and time to personal data such as locations and fingerprints. This information is then stored in the device provider's servers, sometimes outside the country.[14] Each of these varying pieces of information that IoT is collecting increases an individual's digital trail and goes 'much closer to knowing and understanding the unique complexities and individual features of 'a human being' than may be expected.[15]

It is known that there are three particular threats to cybersecurity regarding the application of IoT in smart homes. These are data and identity theft, device hijacking, and ransomware.[16] In the context of the smart home, the infrastructure of the devices comprising the home environment may expose the network to shared vulnerabilities.[17] These particular threats use the characteristics of IoT, which have interconnected networks with other devices and target the device with the least amount of security. This may arise from poor cybersecurity protocols in a particular device or from outdated software nearing the end of its product life-cycle.[18] Nevertheless, hackers may target these vulnerabilities and infiltrate a smart home network through physical proximity to the home or remote activation and access of the sensors in the smart devices.[19]

IoT in smart homes presents a more susceptible and attractive target for hackers due to their complex, interconnected nature.[20] This is because the sheer volume of data stored in even a few connected smart home devices provides more opportunities and incentives for hackers to extract personal information. Multiple devices connected on a single, smart home network can increase the vulnerability to hacking due to the larger device they can target. Access to only one device may provide a hacker with a gateway into all of the smart home devices connected to that network and the data they stored.[21] The most common data and identity theft method in the smart home is credential-harvesting malware, where hackers bypass security protocols through social engineering and credential phishing. The mass of data collected from multiple devices can form a unique user's digital profile. The digital profile can even detail the user's behavior and habits through smart television and energy consumption on a smart meter, thus providing pieces of information that may seem trivial at first. Still, it may become troublesome if it is known for people to stalk somebody.

Moreover, the hacker who has already breached one of the IoT devices in the network may have control over the device or device hijacking. This presents another threat as a hacker infiltrating the IoT device can compromise the device or take control of the devices. For example,

---

[14] Ibid.
[15] Kaman Tsoi and Mandy Milner, "'What Can I Help You with?': Privacy and the Digital Assistant," *Privacy Law Bulletin* 13, no. 9 (n.d.): 191.
[16] Pattanasri, "Mandatory Data Breach Notification and Hacking the Smart Home," 272.
[17] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev, "A Review of Internet of Things for Smart Home: Challenges and Solutions," *Journal of Cleaner Production*, n.d., 140.
[18] Sivaraman, Gharakheili, and Fernandes, "Inside Job: Security and Privacy Threats for Smart-Home IoT Devices," n.d., 23–24.
[19] European Union Agency for Cybersecurity (EU body or agency) et al, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media," LU: Publications Office of the European Union, 2014.
[20] Pattanasri, *Mandatory Data Breach Notification and Hacking the Smart Home*.
[21] Ibid.

a hacker who hacks smart thermostats may use them to increase heating system temperature and cause pipes to burst by altering user inputs, or surveillance cameras may be remotely turned on to view the activities of inhabitants inside the house. Hackers can also use this threat to extort funds from the victims by using the information they get or blocking access to the devices.[22]

IoT devices, often designed for specific, less complex tasks such as controlling lighting or managing door locks, typically do not incorporate the robust, multi-core processors in more sophisticated devices like smartphones, laptops, or tablets. This hardware limitation is a fundamental reason for the IoT's susceptibility to cyber-attacks. Another weakness in IoT security is the lack of strong authentication and authorization protocols. Many IoT devices are configured with default usernames and passwords, which are easily exploitable by hackers. This basic security oversight offers a low barrier of entry for malicious actors seeking to gain unauthorized access to networks. Additionally, the absence of encryption in data transmission is a significant concern. Without encryption, data sent to and from IoT devices can be intercepted and manipulated by unauthorized individuals, compromising the integrity and confidentiality of the information.[23]

Furthermore, IoT devices often have vulnerabilities in their firmware. Since these devices are typically designed for simplicity and cost-effectiveness, their firmware may not be rigorously tested or secured against hacking attempts. This oversight can leave devices open to exploits, allowing attackers to take control of the device or use it as a gateway to infiltrate broader network systems. Unlike computers or smartphones, which regularly receive and prompt users to install security updates, many IoT devices cannot be easily updated. This situation is aggravated by the fact that some devices may not have a user interface or are not connected to a network that facilitates updates. As a result, many IoT devices operate with outdated software that is full of unpatched security vulnerabilities. Alarmingly, there have been instances where IoT devices are found to be pre-installed with malware. This malware can become active once the device connects, leading to a compromised network environment.[24]

In 2022, the number of IoT connections in Indonesia reached more than 134 million, an increase from around 108.5 million in the previous year. According to Statista Digital Market Insight, the estimated number of IoT connections will continue to increase and reach about 404 million by 2028.[25] This means IoT in various sectors in Indonesia has become a booming trend, ranging from the automotive, consumer, healthcare, industrial, smart cities, smart homes, and smart finance applications. In particular, the growing trend in smart homes has started to gain attraction among Indonesian consumers. Among various sectors, smart homes gained the highest number of users and generated the most revenue in 2022. This indicates the growing interest in convenient homes for Indonesian households.[26]

While the growing number of users in IoT can be perceived as having a positive impact on Indonesia's economy, this is not necessarily true because of the risk it carries. There are already a lot of instances where data breaches in Indonesia happen, such as data breach in the marketplace Tokopedia, COVID tracing information on electronic health alert card (eHAC), banking detail of a state-owned insurance department from Bank Rakyat Indonesia, data user from state-owned utility company Perusahaan Listrik Negara (PLN) and a telecom company Indihome.[27] While it is still unknown if the data breaches come from IoT devices or any other

[22] Ibid.
[23] "What Is IoT Security? Definition and Challenges of IoT Security," Fortinet, n.d.
[24] Ibid.
[25] Statista Research Department, "Indonesia: IoT Connections 2018-2028," Web page, Statista, September 22, 2023, https://www.statista.com/forecasts/1410767/indonesia-iot-connections.
[26] Statista Research Department, "Indonesia: IoT Connections 2018-2028," Statista, n.d.
[27] "Top 10 Cybersecurity Breaches in Indonesia," cyberlands.io, n.d.

means, it is still a major concern for Indonesia with its data breach history and the inherent weakness of IoT.

Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law) on October 17, 2022, to answer the challenge of data breaches. But, according to the National Cyber Security Index (NCSI) version 28 April 2023, Indonesia scored 20% in the protection of digital services, including the sub-indicator of protection of IoT Devices. This means that Indonesia has not fully implemented the necessary measures to ensure the security of IoT Devices, such as establishing a national IoT security framework, setting minimum security requirements, and conducting regular audits and tests.[28] This is perhaps because PDP Law is still transitional and will become mandatory in 2024. Accordingly, the PDP Law will be accompanied by the follow-up regulation to regulate the implementation of the PDP Law.

2. Indonesia Response: The Personal Data Protection Law (PDP Law)

Indonesia has been addressing the challenge of personal data protection through legislative efforts and ongoing developments. One of them is the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which aims to ensure citizens' rights to personal protection, raise public awareness, and ensure recognition and respect for the importance of personal data protection. This regulation provides a new framework for personal data protection in Indonesia and regulates how data controllers, processors, and relevant parties process personal data. Although it was enacted in 2022, there is still a 2 years transition before it began to be mandatory, until October 17, 2024. Once the transition period elapses, all parties must comply with all the provisions of the PDP Law, and any incompliance thereto may be enforced.[29]

Before the enactment of the PDP Law, the regulation regarding personal data protection contained in several laws and regulations that spread out in several laws, such as Law No. 11 of 2008 on Electronic Information and Transaction (EIT Law)[30] as amended by Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transaction (EIT Law Amendment)[31], Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transaction (Reg. 71)[32], and its implementing regulation such as the Minister of Communications & Informatics Regulation No. 5 of 2020 on the Private Sector Electronic System Operator, as lastly amended by Minister of Communications & Informatics Regulation No. 10 of 2021 (MOCI Reg 5/2020)[33], and Minister of Communications & Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System (MOCI Reg. 20/2016)[34]. The PDP Law in Indonesia presents a comprehensive framework for protecting and processing personal data, which is particularly relevant in the context of IoT. This technology, characterized by its network of interconnected devices collecting and exchanging data, raises specific

[28] "National Cyber Security: Indonesia," NCSI, n.d.
[29] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection].
[30] ""Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Law No. 11 of 2008 on Electronic Information and Transaction]" (n.d.).
[31] "Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transaction]" (n.d.).
[32] "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik [Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transaction]" (n.d.).
[33] "Peraturan Menteri Komunikasi Dan Informatika Nomor 10 Tahun 2021 Tentang Perubahan Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat [Minister of Communications & Informatics Regula" (n.d.).
[34] "Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik [Minister of Communications & Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System]" (n.d.).

challenges for personal data protection due to the vast amounts and types of data generated. PDP Law broadly defines personal data as data regarding individuals who are identified or can be identified separately or in combination with other information, either directly or indirectly, through an electronic or non-electronic system.[35] The broad definition of personal data under the PDP Law is significant for IoT applications. This includes less obvious identifiers like IP addresses or device IDs, which can indirectly lead to individual identification when combined with location or behavioral data.

The PDP Law provides a far-reaching scope for its applicability, including individuals, corporations, public institutions, and international institutions that control and/or process personal data. In this regard, the PDP Law confirms its extra-territorial scope as it would also cover any personal data of Indonesian subjects outside of Indonesia, whether processed in Indonesia or outside of Indonesia, provided that such processing has a legal impact in Indonesia.[36] However, the PDP Law does not apply to individuals who process personal data for personal or household use.[37]

In distinguishing between general and specific personal data, the PDP Law addresses the nuanced nature of information collected in the IoT ecosystem. IoT devices often gather sensitive information (specific personal data), including health metrics from wearables or biometric data from smart home systems.[38] The Law mandates stricter protection and consent for processing this sensitive data, acknowledging its potential for a more significant impact on individuals, including risks of discrimination or significant personal loss.[39] This distinction ensures a heightened level of security and privacy for sensitive data, which is often at the core of IoT functionalities. There is howe however, no clear differentiation between the requirements for processing general and specific data, except that (a) a data controller may be obligated to carry out data protection impact assessment when processing personal data with high potential risk to data subject, which includes, among others, such an event where it would process specific personal data;[40] (b) a personal data controller and processor may be obliged to appoint a data protection officer (DPO), in the event that the main activity of the personal data controller consists of processing personal data in a large scale that involves specific personal data and//or that relates to criminal acts.[41]

Regarding processing personal data, the PDP Law outlines various stages, including collection, analysis, storage, correction, display, and deletion.[42] Each stage is critically important in the IoT framework, where the risk of data misuse or breach is amplified due to the volume and variety of data handled. The PDP Law mandates stringent requirements such as explicit consent, compliance with legal obligations, and ensuring data processing serves the public interest or legitimate purposes.[43] These provisions aim to safeguard personal data throughout its lifecycle in the IoT ecosystem, providing ethical and lawful handling at every step.

---

[35] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection].
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] "'Penjelasan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Elucidation of the Law No. 27 of 2022 on Personal Data Protection],' Indonesia § (n.d.), Art 4." (n.d.).
[40] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art 34." (n.d.).
[41] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 53." (n.d.).
[42] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 16." (n.d.).
[43] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 20." (n.d.).

The PDP Law also addresses the complexities of cross-border data transfers, common in the global IoT network. It stipulates that such transfers must only occur under adequate data protection or by establishing appropriate safeguards.[44] This aspect is crucial not only for safeguarding data in IoT but also represents a strategic move to position Indonesia as a compliant and attractive partner in the global market, especially in technology sectors heavily reliant on data exchange. This harmonization boosts confidence among international partners and investors and ensures that Indonesian businesses are equipped to compete and collaborate in markets where stringent data protection is a prerequisite.[45] For technology sectors, where cross-border data flows are integral to operations and innovation, this alignment means Indonesian companies can engage more seamlessly in international projects, data sharing, and technology development with countries that already implement personal data regulation similar to GDPR. Moreover, by adhering to internationally recognized standards, Indonesia will likely attract more foreign investment and technological collaborations, fostering an environment conducive to digital innovation and growth. This strategic alignment with global data protection norms thus plays a pivotal role in Indonesia's integration into the global digital economy.[46]

The PDP Law in Indonesia addresses data breaches with an approach that is particularly relevant in the Internet of Things (IoT) context. Given the interconnected nature of IoT devices and networks, the Law's broad definition of data breaches is crucial, as it encompasses a range of increasingly common scenarios in this domain. These scenarios include traditional data leaks or unauthorised access incidents and the more complex breaches that can occur in IoT networks, such as unauthorized inter-device communications or the exploitation of vulnerabilities in one device, leading to a cascade of security issues across the network.[47] The Law mandates a stringent 3x24-hour notification period for reporting such breaches, underscoring the criticality of rapid response in the IoT environment.[48] This requirement is particularly pertinent in IoT, where the extensive and often sensitive nature of data handled, combined with the network's complexity, means that delays in addressing breaches can exacerbate the scope of data misuse and increase the risk of severe consequences for individuals' privacy and security.

In Indonesia, the Personal Data Protection (PDP) Law outlines specific sanctions for data privacy breaches, primarily encompassing fines and, in cases of intentional infringement, the possibility of imprisonment.[49] The law grants the Personal Data Protection Authority (PDPA) the power to enforce various administrative sanctions. These sanctions include issuing written warnings, temporarily suspending personal data processing activities, mandating the deletion or destruction of personal data, and imposing administrative fines. Importantly, the PDP Law sets a ceiling for these fines, capping them at a maximum of 2% of the annual income or revenue of the party found in violation.[50] These measures, targeting prohibited conduct in relation to

[44] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 56(1)." (n.d.).
[45] Yusuf, "Transfer Data Antarnegara Bisa Dilakukan Jika Memiliki Aturan Setara UU PDP," Ditjen Aptika (blog), n.d.
[46] Rini Kustiasih, "Kelayakan Regulasi Perlindungan Data Pribadi Syarat Kerja Sama Internasional," Web page kompas.id, n.d.
[47] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 16(2)." (n.d.).
[48] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 46(1)."
[49] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 67-71." (n.d.).
[50] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 57." (n.d.).

personal data, have been in effect and enforceable since the PDP Law was enacted, demonstrating Indonesia's commitment to ensuring data privacy and protection.

3. Comparative Analysis of PDP Law and GDPR

The General Data Protection Regulation (GDPR) applies a comprehensive scope of data processing activities in both the private and public sectors.[51] The GDPR emphasizes the protection of data belonging to citizens and residents of the European Union, regardless of whether the data processor is an organization based within the EU. It also considers where and how the data processing occurs. This action has an extraterritorial effect on these provisions by providing comprehensive cross-border protection for EU data subjects.

Similarly, PDP Law also applies to both private and public sectors. It also has an extraterritorial reach, addressing actions outside Indonesia that have legal consequences within the country or adversely affect its national interests.[52] However, the absence of an independent data protection authority raises questions about how enforcement of this law, particularly in the public sector, will be monitored. Article 58 of the PDP Law states that to realize personal data protection, there will be an agency established by the President that will be regulated in a regulation of the President, but so far, it still has not appeared.[53] Further details are needed quickly to define the role and powers of the said agency in law enforcement and to establish mechanisms for imposing sanctions on other ministries, government institutions, and the private sector.

The scope of the definition of personal data relates to how personal data is described in legal provisions.[54] The GDPR defines personal data based on identifiable characteristics as 'any information relating to an identified or identifiable person (data subject)'.[55] However, the PDP Law does not explicitly refer to individual persons. Instead, it defines a person as an individual or part of a corporation/institution. This definition necessitates more explicit criteria and a clear description to distinguish between individuals and institutions. moreover, a more explicit definition and criteria for the individual categories are needed to differentiate data processing activities for household purposes from those of a commercial nature.

GDPR establishes exemptions for small and medium-sized enterprises (SMEs). This provision allows adaptability in meeting additional obligations by considering the nature and volume of the data processing, the nature, scope, and purpose of the data processing, and the size of the processing entity. Under GDPR, organizations or companies with fewer than 250 employees are exempt from the data controller's obligation to maintain records of processing activities unless there is a risk to the rights and freedoms of data subjects, if the processing is not occasional, or if it involves special categories of data or data relating to criminal convictions and offenses.[56] In contrast, Indonesia's PDP Law does not consider SMEs to be a distinct

[51] "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*, 2016.
[52] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 2(1)." (n.d.).
[53] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 58." (n.d.).
[54] G.W. Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford, United Kingdom ; New York: NY: Oxford University Press, 2014).
[55] "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," 2016.
[56] "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* OJ L 119/1, no. Art. 30(5). (2016).

category. Article 2 of the PDP Law states that as long as a business is registered as a legal entity, it is subject to the law.[57] Such a generic approach overlooks the varying capacity levels of diverse business scales and the differing maturity levels of related industries in implementing legal compliance. This lack of distinction in the Indonesian PDP Law suggests that all legal entities, regardless of their size or the nature and volume of data they process, are uniformly subject to the same data protection obligations. This could present challenges for smaller businesses in Indonesia, which might lack the resources and infrastructure to comply with the same standards as larger corporations, potentially impacting their operational efficiencies. Data controllers and processors should demonstrate accountability by showing compliance with the regulations to enhance compliance. This includes actions ensuring personal data protection through principles like privacy by design and privacy by default. Privacy by design under GDPR means that data processors shall consider privacy at the initial stages when designing and developing a product as well as services that involve processing personal data.[58] Thus, it encourages companies to implement technical and organizational measures at the earliest stages of the design of processing operations in a way that safeguards privacy and data protection principles right from the start. [59] Privacy by default under GDPR means that the controller, by default, uses only the necessary data for each specific purpose of the processing being processed.[60] This means the data controller must consider both the volume of personal data and the types, categories, and levels of detail of personal data. If personal data is not needed after the first processing, it shall be deleted or anonymised by default.[61] The GDPR has tightened rules for data controllers and processors, emphasising these principles.

Several major issues arise concerning data controller and processor obligations in Indonesia. First, the PDP Law contains significant gaps compared to the GDPR. It does not mandate principles of privacy by design and privacy by default, which are crucial for ensuring privacy and data protection are central to data collection and use, including in digital innovation or technology. The PDP Law also does not regulate joint controllers in data processing or when processors engage sub-processors. Most importantly, there is no explicit provision on data processor obligations to notify controllers immediately in case of a data breach. Second, the PDP Law lacks specific regulations. Currently, the PDP does not account for the varying capacities of controllers to provide complete information about data breaches to subjects and the Ministry of Communication and Informatics within the specified timeframe (3x24 hours).[62] As a result, it does not allow for phased disclosure of data breach information without undue delay.

The enforcement of PDP Law in the international arena is anticipated to be facilitated through international agreements. However, as of now, there haven't been significant developments in establishing specific international agreements for enforcing the PDP Law, which might be attributed to its recent introduction and ongoing developmental phase. Despite lacking targeted bilateral agreements concerning specific data protections, Indonesia has a strong foundation of international relations, as evidenced by its existing bilateral agreements with 162 countries. Furthermore, Indonesia's active participation in multilateral agreements

[57] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 2." (n.d.).
[58] "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* OJ L 119/1 (2016): Art. 25(1).
[59] Daniela Jezoya, "Principle of Privacy by Design and Privacy by Default," *Regional Law Review 2020*, 2020, 129.
[60] "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* OJ L 119/1, no. Art. 25(2). (2016).
[61] Jezova, "Principle of Privacy by Design and Privacy by Default," n.d., 133.
[62] "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [Law No. 27 of 2022 on Personal Data Protection], Art. 46." (n.d.).

with major international organizations such as the International Monetary Fund (IMF), World Trade Organization (WTO), International Labour Organization (ILO), Food and Agricultural Organization (FAO), ASEAN Free Trade Area (AFTA), and the Economic and Social Council (ECOSOC) underscores its global engagement and commitment. This international relationship can pave the way for smoother and more efficient future negotiations and collaborations in enforcing its PDP Law. Such a robust international presence can foster cooperative frameworks and dialogues necessary for the effective cross-border application of data protection standards, which is increasingly important in the interconnected digital landscape.[63]

Based on the previous analysis, several recommendations can be proposed to enhance the effectiveness of Indonesia's Personal Data Protection (PDP) Law:

1. Clarify the data protection rules and the roles and responsibilities of the data protection authority. In line with this, the government needs to identify subsidiary policies necessary to supplement the current PDP Law and strengthen its enforcement in the future. This should include international cooperation related to personal data protection, ensuring the PDP Law aligns with global data protection standards and practices.
2. Incorporate fundamental data protection principles such as privacy by design, privacy impact assessments, and privacy by default. These principles are essential for ensuring that data protection is an integral part of the planning and operation of data processing activities. Additionally, the government should expedite the creation of bilateral or multilateral agreements to enforce the PDP Law internationally, prioritizing collaboration with international organizations. This would ensure a comprehensive and globally aligned approach to data protection.
3. Consider the diversity in size and capacity of entities subject to the PDP regulations, enabling adaptable compliance with the PDP Law. The law must accommodate the different capabilities of entities, allowing them to comply without breaching the regulations. Moreover, the PDP Law should recognize that the role of the data protection authority extends beyond law enforcement. It should also involve educating various stakeholders about the importance of personal data protection for the sustainability of their businesses and empowering them to build compliance with existing laws. This approach ensures adherence to the law and fosters a culture of data protection awareness and responsibility.

In light of the previous analysis, it is clear that while Indonesia's Personal Data Protection (PDP) Law is a significant step in the right direction, there is an urgent need to strengthen and clarify its provisions to ensure robust data protection, especially in the context of international collaboration and the burgeoning realm of IoT. In its current form, the law already lays a foundational framework for protecting personal data. Still, rapid reinforcement is required to keep pace with the evolving demands of data security and privacy, particularly in the international arena, where IoT data flows across borders. Overall, while commendable in its current state, the PDP Law needs rapid and decisive enhancements to effectively secure data protection, particularly in safeguarding IoT privacy data protections on an international level.

D. CONCLUSION

The exploration of Indonesia's Personal Data Protection (PDP) Law, particularly concerning the burgeoning Internet of Things (IoT) sector, reveals both its strengths and areas for improvement. While the PDP Law marks a critical step towards aligning Indonesia with global data protection standards, primarily influenced by the European Union's General Data Protection Regulation (GDPR), it faces distinct challenges in its application and enforcement. The law's broad definition of personal data and its extraterritorial scope are commendable, yet

[63] "Kerjasama Luar Negeri," Web page, Direktorat Jenderal Perhubungan Laut, n.d.

they necessitate further clarity and detailed guidelines, especially considering the unique complexities of IoT ecosystems. The PDP Law's current framework, although robust in its intentions, needs refinement to address specific IoT-related vulnerabilities and data protection nuances. This includes incorporating principles such as privacy by design and by default, which are essential for preemptively safeguarding data in an IoT-dominated landscape. Additionally, the law must consider the diversity of entities it governs, particularly regarding small and medium-sized enterprises (SMEs), and provide adaptable compliance mechanisms that recognize varying capacities and resources.

The law's enforcement mechanisms, including establishing a data protection authority and formulating international agreements for cross-border data protection, are critical areas needing immediate attention. These mechanisms are essential for the law's effectiveness, especially in a digital age where data flows transcend national boundaries. To enhance the PDP Law's impact on IoT data privacy, it is imperative to strengthen its provisions, clarify roles and responsibilities, and foster international cooperation. By doing so, Indonesia can protect its citizens' data privacy more effectively and position itself as a compliant and forward-thinking participant in the global digital economy. In its enhanced form, the PDP Law has the potential to set a precedent in IoT data protection, balancing technological innovation with the fundamental right to privacy and data security.

REFERENCES

"Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law No. 11 of 2008 on Electronic Information and Transaction] (n.d.).

Alhosani, Hussain Matar Mohamed Ghaith, Amiruddin Ahhamat, and Norain Ismail. "Industrial Revolution 4.0 (IR 4.0) Competencies: A Literature Review of Manufacturing Industry." *Ethical and Regulatory*, no. 1 (2021): 3.

cltc2015. "New CLTC Report Highlights Privacy Risks in the 'Internet of Things' - CLTC UC Berkeley Center for Long-Term Cybersecurity." CLTC (blog), n.d.

Department, Statista Research. "Indonesia: IoT Connections 2018-2028." Statista, n.d.

Diega, Guido Noto La. "Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies." *Milton, UNITED KINGDOM: Taylor & Francis Group*, 2022, 2.

Diega, Noto La. "No," n.d., 21.

European Union Agency for Cybersecurity (EU body or agency) et al. "Threat Landscape and Good Practice Guide for Smart Home and Converged Media." LU: Publications Office of the European Union, 2014.

Greenleaf, G.W. *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford, United Kingdom ; New York: NY: Oxford University Press, 2014.

Ilic, Dejan, Branko Markovic, and Dragan Milosevic. "Strategic Business Transformation: An Industry 4.0 Perspective." *International Journal of Economics and Law 49*, 2017, 50.

Jezova. "Principle of Privacy by Design and Privacy by Default," n.d., 133.

Jezoya, Daniela. "Principle of Privacy by Design and Privacy by Default." *Regional Law Review 2020*, 2020, 129.

Web page, Direktorat Jenderal Perhubungan Laut. "Kerjasama Luar Negeri," n.d.

Kustiasih, Rini. "Kelayakan Regulasi Perlindungan Data Pribadi Syarat Kerja Sama Internasional." Web page kompas.id, n.d.

NCSI. "National Cyber Security: Indonesia," n.d.

Pattanasri. *Mandatory Data Breach Notification and Hacking the Smart Home*, n.d.

Pattanasri, Thanaphol. "Mandatory Data Breach Notification and Hacking the Smart Home: A Legal Response to Cybersecurity." *QUT Law Review* 18, no. 2 (2018): 7.

"Penjelasan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Elucidation of the Law No. 27 of 2022 on Personal Data Protection]," Indonesia § (n.d.),

Art 4. (n.d.).
Peppet, Scott R. "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consen." *SSRN Scholarly Paper*, n.d., 98.
Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat [Minister of Communications & Informatics Regula (n.d.).
Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik [Minister of Communications & Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System] (n.d.).
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transaction] (n.d.).
"Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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*, 2016.
"Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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," 2016.
"Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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* OJ L 119/1, no. Art. 30(5). (2016).
"Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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* OJ L 119/1 (2016): Art. 25(1).
"Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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* OJ L 119/1, no. Art. 25(2). (2016).
Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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 Da (n.d.).
Sivaraman, Gharakheili, and Fernandes. "Inside Job: Security and Privacy Threats for Smart-Home IoT Devices," n.d., 23–24.
Sivaraman, Vijay, Hassan Habibi Gharakheili, and Clinton Vernandes. "Inside Job: Security and Privacy Threats for Smart-Home IoT Devices." *Australian Communications Consumer Action Network, 2017*, 2017, 7–10.
Statista Research Department. "Topic: Internet of Things (IoT) in Indonesia." Statista, n.d.
Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A Review of Internet of Things for Smart Home: Challenges and Solutions." *Journal of Cleaner Production*, n.d., 140.
Office of the Privacy Commissioner of Canada. "The Internet of Things - An Introduction to Privacy Issues with a Focus on the Retail and Home Environments," n.d.
cyberlands.io. "Top 10 Cybersecurity Breaches in Indonesia," n.d.
Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transaction] (n.d.).
Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law No. 27 of 2022

on Personal Data Protection].
Fortinet. "What Is IoT Security? Definition and Challenges of IoT Security," n.d.
Yusuf. "Transfer Data Antarnegara Bisa Dilakukan Jika Memiliki Aturan Setara UU PDP." Ditjen Aptika (blog), n.d.