TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 36, 2022

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

TECHNIUM SOCIAL SCIENCES JOURNAL

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia

Kiki Rezki Ramadhan[1], Chandra Wijaya[2]

[1]Student in Magister Program, Faculty of Administrative Science, Universitas Indonesia, [2]Professor of Faculty of Administrative Science, Universitas Indonesia

kikirezkidewaamor@gmail.com

Abstract. Cases of leakage of personal data are a serious problem for countries that should be guaranteed safety as the identity and rights of individual citizens. In Indonesia, there are still many problems related to the security of cyberspace, one of which is becoming a trend of public issues, namely leakage of personal data. The rapid development of information and communication technology has provided changes to the character of community activities that are currently dominated by the use of the internet as a characteristic of modern society so the presence of the state to provide protection is important for the community. In this article, a case study of data leakage incidents in Indonesia and personal data protection policies carried out in the European Union, Singapore and Malaysia were chosen to be presented. The European Union is a supranational organization that has successfully implemented a policy of protecting personal data through the General Data Protection Regulation (GDPR). Meanwhile, Singapore has implemented a similar policy since 2012 through Personal Data Protection Act. Other learning can also be taken from Malaysia which already has a national regulation on data protection since 2010. Indonesia needs to take lessons by conducting policy comparative analysis and can contribute to the government in making derivative regulations from the newly ratified personal data protection law by the House of Representatives of the Republic of Indonesia to provide concrete protection for personal data in Indonesia.

Keywords. Protection of Personal Data, Personal Data Protection Policy, Cyber Security, Learning

I. Introduction

I.1. Cases of Leaks of Personal Data in Indonesia

In 2022 the Indonesian public was shocked by the leakage of cellular telephone registrant's data that were sold freely on the Breached Forums Hacking Forum Site (Kompas, 2022). A total of 87 GB of data is sold at IDR 743 million (around USD 50,000). This cyber security incident complements cases that had previously occurred such as leakage of PLN data, leakage of health applications owned by the Ministry of Health (E-HAC), BPJS Health data leakage, to the leak of banking data (BRI Life).

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

Protection of personal data is the protection of one of the individual rights carried out by the organizer of the electronic system and must be free from all kinds of disturbances including use without permission and illegal intervention (ITE Law, 2008).

Guarantee to Protection of Personal Data is an obligation that must be achieved by the state, this is by the mandate contained in the 1945 Constitution of the Republic of Indonesia. Protection of personal data is important by looking at the level of internet penetration in Indonesia in 2022 which reached 77.02 % (APJII, 2022). The percentage of internet penetration has increased from year to year, especially since the Pandemic Covid-19 which drastically has influenced and changed the character of community behavior in carrying out its daily activities through virtual or online methods. The application of restrictions on physical activity to break the chain of the spread of COVID-19 certainly has a great impact on the sectors of community activities such as the MSME sector and the education sector which were previously conventional face-to-face. Seeing the high activity of citizens in the virtual space, the state must be able to guarantee three principles of information security that include confidentiality, integrity, and availability of data from illegal access to irresponsible parties (ISO 27001). Some cases of data leakage that occurred in Indonesia have indicated the weak role of the government in realizing data protection. Regulations related to the activity of organizing information and electronic transactions have existed since 2008, namely through Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), but the Law has not been specifically intended to protect personal data until September 2022 Law Indonesia's personal data protection is passed.

The need for regulations specifically aimed at protecting personal data has become a separate policy challenge by remembering so many stakeholders. Issues related to sectoral ego, overlapping the authority of the authority body, until the case of recurring data leaks is also a serious problem that must be resolved. The last case leak case carried out by an actor threat calling himself Bjorka, has made the President of the Republic of Indonesia form a Special Data Security Team involving the Ministry of Communication and Information, the Cyber and Sandi State Agency, the State Intelligence Agency, and the Indonesian National Police (Setneg, 2022). In line with this, the need for an integrated and comprehensive coordination framework between institutions has been mapped by the Center for Digital Society of Gadjah Mada University in addition to the need for cyber security policies that also do not exist (CFDS UGM, 2019). Now through the presence of the Computer Security Incident Response Team (CSIRT) which is spread starting from the national level, ministries/institutions to the private sector can be the initial capital in terms of the organizational structure and its bodyguards. Furthermore, the legislative body only needs to take further steps to make a derivative of personal data protection policies at the managerial and operational technical levels that will complement the legal umbrella (Law on Personal Data Protection) that has just been ratified to maintain the identity of citizens in cyberspace.

I.2. Indonesian internet penetration

Based on a survey conducted by the Indonesian Internet Service Provider Association (APJII) in 2022, more than 77.02 % of Indonesian people use the internet. This means that there are 210,026,769 inhabitants of the total population of 272,682,600 Indonesians connected to the internet. Increased internet users have increased in the Covid-19 pandemic period due to the use of internet technology to replace face-to-face activities. This is also in line with the data released by the Organization for Economic Co-Operation and Development, where there is an

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

increase in internet access that continues to increase from year to year both by households and individuals throughout the world (OECD, 2021).

This is a reality that the development of technology and communication such as the evolution that occurs in cellular network technology has become the backbone that supports the activities of modern society, especially in the current era of the industrial revolution. Data released by Ookla also shows an increase in the need for average internet connection speed in Indonesia in 2022 which is 15.82 Mbps (increased 3.40 MBSP/+27.4%) for cellular networks and 20.13 Mbps (increased 4.04 Mbps/+25.1%) for fixed networks (Ookla, 2022).

In general, Indonesian people use the internet for the sake of social interaction through cyberspace. Furthermore, the internet is also used to support the daily activities of citizens such as access to public services, commerce, banking, education to entertainment. Based on research conducted on internet users in the age range of 16 to 64 years by Hootsuite, it is known that social media also has a role to support work. Indonesia itself is ranked 8th as a country in the world that uses social media to support work activities (Hootsuite, 2022).

I.3. Indonesian Personal Data Protection Index

Based on the assessment issued by the E-Governance Academy (EGA), the value protection value in Indonesia is 25%. This has an influence on the Indonesian National Siber Security Index which is ranked 83rd and is far below the Malaysian and Singapore cyber security index, which are ranked 19th and 29th (NCSI, 2020).

Table 1. National Cyber Security Index 2020

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
19	Malaysia	79.22	62.53	16.69
29	Singapore	71.43	80.26	-8.83
83	Indonesia	38.96	46.84	-7.88

Source: NCSI, 2020

The assessment organized by EGA is intended to see the state's readiness in preventing cyber threats through the implementation of cyber incident management. Assessment indicators are carried out by referring to cyber security governance which is generally intended to deal with current cyber threat trends such as personal data leaks. The assessment was carried out by measuring several aspects of cyber security taken by the state government including Legal Umbrella Regulation, Existing Authority Agency, Forms of Cooperation, and Policy Results. Based on the assessment in 2020, Indonesia's cyber security conditions can be described as consisting of several indicator categories as follows: Development of Cyber Security Policy 0%, Information and Analysis of Cyber Threats 20%, Professional Development and Education 44%, Contribution to Global Siber Safety 17%, Protection of Digital Services 20%, Protection of Critical Services 0%, Trust and Electronic Identification Services 89%, Protection of Personal Data 25%, Cyber incident response 67%, cyber crisis management 20%, cyber-criminal handling 78%, and cyber operations military 33%.

Furthermore, based on cyber security monitoring carried out by the Cyber Threat Intelligence Directorate of Siber BSSN Security Operations, data leakage is the most reported case. There are 99 Data Leakage Reports from a total of 179 reports throughout 2021. The leak was found on the Darknet which befell 78 agencies consisting of 60 cases in the government

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

sector, 5 cases in the field of law enforcement, 5 cases in the energy sector, 4 cases in the financial sector, 3 transportation cases, and 1 case in the telecommunications sector.

Table 2. Details of the data exposed from each field

Affected sector	Exposed data
Finance	27,738
Energy	23,881
Government	17,503
Telecommunication	13,626
Transportation	834
Law Enforcement	409

Source: BSSN, 2021

Of all cases of data leaks that occur, it is known that there are around 83,991 data exposed on the internet. Furthermore, a search conducted by Surfshark, a VPN service company based in the Netherlands said that Indonesia until the first quarter of 2022 entered into the category of 10 countries that experienced the most data leakage cases, with total data exposed as many as 429,860 data (Surfhark, 2022). This means that the leakage of data occurred more than the reports given by CTI BSSN in 2021.

Thus, seeing the facts above the problem of data leak cases can not only be resolved through the Authority Agency that has existed such as the Ministry of Communication and Information, BSSN, BIN, TNI, and Polri, but also the role of policy through regulations that will regulate authority, forms of cooperation, to the application Sanctions so that it can produce outcomes that can provide a real guarantee of protection for the personal data of citizens.

Indonesia needs to learn from neighboring countries such as Malaysia and Singapore which have already successfully implemented personal data protection policies. Even in a bad situation such as a data leak, Singapore takes a fast response, transparent, and solution mechanism. In 2021, the Singapore Personal Data Protection Commission (PDPC) imposed a $74,000 penalty on a local company for failing to protect 5.9 million RedDoorz Singapore and Southeast Asia customer data (PDPC, 2021). Furthermore, the application of sanctions that apply in the European Union through the General Data Protection Regulation is even more stringent, public and private sector organizations can be subject to a fine of up to 20 million euros if they do not comply with the rules that have been set (GDPR, 2018).

Based on the description above, the purpose of writing this article is to provide input to the Government in preparing derivative regulations from the Personal Data Protection Law which was recently passed by the DPR RI to overcome the problem of data leakage that is currently occurring through comparative studies of various regulations owned by the DPR RI. by the European Union countries, Singapore and Malaysia.

II. Method

This study uses qualitative methods through literature studies from various document sources. The researcher examined documents related to data protection policies in Indonesia and other countries, especially in the European Union through the General Data Protection Regulation, Malaysia through the Personal Data Protection Act 2010, and Singapore through the Personal Data Protection Act 2012. The researcher then compared the personal data

protection policies of these countries and supranational organizations as learning materials for the development of personal data protection policies in Indonesia.

The writing of this article is descriptive and explanatory to obtain facts and describe a comparative analysis of personal data protection policies from the three reference sources above. The author also presents relevant data related to the urgency and policy challenges currently being faced by Indonesia, especially to make regulations on the protection of personal data and its derivatives.

III.Literature Review

III. 1. Personal Data Protection Policy As Public Policy

The book 'Public Policy Making: An Introduction by James E Anderson (1979) defines public policy as a relationship between government units and their environment. Furthermore, according to William N Dunn (2003), public policy is a complex pattern based on collective choices that have ties of interdependence with one another. According to Chandler and Plano (1988), public policy is a strategic use of existing resources, where its implementation is carried out through interventions carried out on an ongoing basis by the government to protect the interests of disadvantaged groups in society.

III.2. Elements of a Personal Data Protection Policy

The challenges of personal data protection policies in Indonesia can be mapped through a literature review with comparative analysis and their suitability to existing conditions. According to Dunn, there are three elements of public policy, namely policy actors, the policy environment, and public policy itself. The three elements can be broken down into several specific attributes, including:

1) Policy actors can be in the form of the government, the private sector, academia to the community. Policy actors can also be interpreted as related to all forms of activity such as bureaucratic behavior, the role of interest groups, and shared problems that occur between political actors.

2) The policy environment can be interpreted as things that influence public policy such as technological developments, organizational needs, and values that develop in society to a developing public issue.

3) Public policy itself can be in the form of state law products that contain objectives that reflect the desired results and impacts, instruments or tools used to carry out policies, their authority, and governance.

Furthermore, based on the theory of policy levels proposed by Bromley in Widiana, et al. (2022), challenges related to data protection policies in Indonesia can also be mapped through three policy hierarchies as follows:

1) The general policy level is the making of regulations at the national level such as the preparation of strategies, laws, and government regulations to presidential regulations.

2) The managerial level is making regulations at the organizational level, institutions that run programs such as Ministerial Regulations.

3) The operational technical level is the making of regulations at the level of the implementing unit of activities or programs such as regulations for the head of the institution and the Instructions of the Directorate General.

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

IV.Results and Discussion

IV.1. European Union Personal Data Protection Policy

The European Union is one of the largest international organizations in the world as well as being an example of how countries with different interests can unite to achieve common goals. The organization works through a combination of supranational and intergovernmental systems, where decisions are made through deliberation among member states. This indicates that this organization has become a political and administrative unit that has spawned and increased the number of policies within the European Union, one of which is the General Data Protection Regulation. The important point of GDPR is that there is a risk-based approach that improves privacy and data protection, so the expected result is reputation and trust. GDPR is one proof that there is intervention and collective consensus of the European Union which makes this rule not only applicable internally but also outside the European Union about the processing of personal data belonging to its people. Another important note is contained in chapter 6 which mentions the existence of an independent supervisory authority. The value of protecting personal data that has been successfully carried out also affects the cybersecurity index for its member countries. The table below provides a comparison visualization that proves the success of the GDPR taken from the 3 European Union member countries with the top cybersecurity rankings.

Table 3. Cybersecurity Index Comparison With 3 EU Member States

	Greece	Lithuania	Belgium	Indonesia
Population	10.9 Million	2.9 Million	11.3 Million	258.7 Million
GPD per Capita	$29,100	$65,300	$30,500	$13,100
Cyber Security Policy	100%	100%	86%	0%
Personal Data Protection	100%	100%	100%	25%
Cyber Crisis Management	80%	100%	40%	20%
Cybersecurity Index	96.10%	93.51%	93.51%	38.96%
Cyber Security Rank	1	2	3	83

Source: NCSI, 2020

From the table, it can be seen that the value specifically aimed at protecting personal data in the three member states of the European Union reaches 100%. This is also supported by the existence of the implementation of cyber security regulations and supported by the existence of cyber crisis management that reflects the cooperation between stakeholders in addition to the existing GDPR policy.

IV.2. Singapore's Personal Data Protection Policy

As the most developed country in Southeast Asia, Singapore has implemented personal data protection since 2012 which was presented in the form of the Personal Data Protection Act 2012. Awareness of regulations specifically aimed at citizens privacy is important because Singapore has long been synonymous with digitization. The policies taken are also not only present as regulations but also clearly describe important things that confirm that policymakers in Singapore are serious about protecting the personal data of their citizens. Some important notes that can be seen from the data protection policy in Singapore include:

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

1)Article 7 states that there is an advisory board that provides advice to the government regarding the implementation of personal data protection policies. Through this article, it is known that there is a council with a strong role that can provide input to the implementation of policies.

2)Article 8 mentions the existence of an independent commissioner.

3)Article 10 states that there is a form of cooperation that aims to facilitate all stakeholders related to the data protection function. Furthermore, another important value in this article also aims to avoid duplication of activities between stakeholders in terms of data protection law enforcement.

Table 4. Cybersecurity Index Comparison With Singapore

	Singapore	Indonesia
Population	5.5 Million	258.7 Million
GPD per Capita	$98,000	$13,100
Cyber Security Policy	86%	0%
Personal Data Protection	100%	25%
Cyber Crisis Management	100%	20%
Cybersecurity Index	71.43%	38.96%
Cyber Security Rank	29	83

Source: NCSI, 2020

From the table, it can be seen that the score related to the personal data protection policy in Singapore reaches a score of 100%. Furthermore, the assessment on cyber crisis management also received a score of 100%, which means that Singapore is in a state of maximum readiness when faced with the worst situation such as a data leak case. Cyber management is considered as a working system within the organization that can also be interpreted as an instrument for implementing policies, where one of its manifestations is the existence of an advisory board and the existence of cooperation between institutions and all stakeholders as stated in Article 7 and Article 10 of the 2012 PDPA.

IV.3. Malaysia Personal Data Protection Policy

As one of Indonesia's neighbors in the Southeast Asia Region, Malaysia has also implemented a similar policy through the Laws of Malaysia Act 709 Personal Data Protection Act 2010. Several important notes in Malaysia's data protection policy include:

1) Part IV mentions the appointment, function, and authority of the commissioner.

2) In part VI, it is stated that there is an advisory board that is tasked with providing input to the government related to the administration and law enforcement by established policies. Article 72 states that an advisory board is appointed by the government consisting of a chairman, 3 members from the public sector, and at least 7 people but not more than 11 people from other sectors.

3) In the same section in article 79, it is stated by the council that advisors can invite anyone to attend in the context of solving a public problem related to data protection.

Technium Social Sciences Journal
Vol. 36, 18-28, October, 2022
ISSN: 2668-7798
www.techniumscience.com

Table 5. Cybersecurity Index Comparison With Malaysia

	Malaysia	Indonesia
Population	31.4 juta	258.7 Juta
GPD per Capita	$30,400	$13,100
Cyber Security Policy	86%	0%
Personal Data Protection	100%	25%
Cyber Crisis Management	40%	20%
Cybersecurity Index	79.22%	38.96%
Cyber Security Rank	19	83

Source: NCSI, 2020

Similar to the data protection policy implemented by Singapore, the regulations in force in Malaysia also have an advisory board to assist the government in implementing the policy. However, the form of coordination and cooperation has not been clearly stated in the regulations, resulting in the value of cyber crisis management at a score of 40%. Crisis management has an important role in consolidating all stakeholders in an integrated manner.

IV.4. Indonesia's Personal Data Protection Policy

The personal data protection policy in Indonesia is in the form of the Personal Data Protection Law which was ratified by the House of Representatives of the Republic of Indonesia at the 5th Plenary Session of the First Session of 2022 - 2023. In this regulation, there are 16 chapters and 76 articles that contain the owner's rights. personal data, obligations of controllers and processors of personal data, and institutions that administer regulations, prohibitions, and sanctions. An important note in this regulation is the position of the policy implementing agency under the President in the form of a Non-Ministerial Government Institution (LPNK). The legality of the institution is stated in article 58 paragraph (2), which is further related to the regulation submitted to the Presidential Regulation (UU PDP, 2022). The position of the institution under the President caused a reaction from the Non-Governmental Organizations who questioned the effectiveness of its supervision (Elsam, 2022). Regulations that are made to ensure data protection in both the public and private sectors should ensure more objective transparency if they are supervised by an independent authority.

IV.5. Lessons Learned

From the several personal data protection policies above, several things are important notes for Indonesia to learn. By looking at the assessment index issued by EGA through NCSI, it is realized that the form of personal data protection carried out by the Indonesian government is still very low. Furthermore, from the assessment of each aspect, a comparative analysis can be carried out based on the theory of policy and public administration. This is intended so that the role of the state in protecting the privacy of citizens is not only carried out through the development of technology and infrastructure but also needs to be developed from the aspect of policy making as a reference for the government to act.

Until now the policy of protecting personal data in Indonesia has not been effectively implemented, this is because there is a transition period of about 2 years since the regulation was enacted. Furthermore, several important things that need to be included in the regulation should not only be limited to general formalities that are specific to the topic, but it is necessary to look at several elements of public policy which will later become an ecosystem for the

implementation of public policy itself. Several factors need to be considered to address the challenges of data protection policies in Indonesia, including:

1) Cooperation governance is a concept involving all stakeholders related to the issue of personal data protection which is currently becoming a trend public issue due to the rise of data leakage cases in Indonesia. The behavior of accusing each other of authority indicates the weak coordination and management of cyber crises carried out by the state. So that the concept of cooperative governance is expected to be the answer to the sectoral ego issue, which so far the implementation of cyber security policies is still carried out sectorally. The launch of the CSIRT, which started in 2020, is only strengthened by articles related to the form of collaboration between stakeholders on personal data protection policies in Indonesia. This will also serve as a reference to avoid duplication of authority between authority bodies in carrying out the same function.

2) The need for an advisory board and an independent authority (commissioner) that can accommodate representatives from all stakeholders is one of the solutions that has been voiced by many people. Furthermore, this institution is expected to be able to provide input to the government and be free from subjective and political interests. This institution exists to accommodate public complaints related to data protection issues that have not been accommodated by state policy.

V. Conclusion

The invention of the internet which is the result of advances in technology and information is undeniable as a masterpiece in the history of human civilization that brings dynamic changes. In addition to the positive value of technological advances that continue to develop, there are also increasingly sophisticated cyber threats. Handling and responding to cases of personal data leaks that have occurred in Indonesia so far tend to be viewed from the point of view of technical aspects only, some of which mentioned the gap or gap in the number of IT experts with the rise of cyber threats. So that the strengthening taken by many organizations tends to be done on the technical aspect only.

The presence of the Personal Data Protection Law which has just been passed is a good first step from a policy aspect, thus placing Indonesia on par with several countries in the ASEAN region that have previously implemented data protection for their citizens. However, it is realized that this new policy still needs to be strengthened in its derivative regulations and will further regulate other specific matters that have not been accommodated.

By looking at the scope of supervision of the PDP Law which binds all sectors, both government and private, it is necessary to strengthen it through several suggestions and inputs that can be accommodated in its derivative regulations as follows:

1) The need and affirmations related to the governance of cooperation to synergize all stakeholders.

2) The need for an advisory board and independent institution (commissioner) whose membership consists of all stakeholders from the government sector, private sector, academia, community, and society so that the input provided will be objective and ensure transparency.

References

[1]Anderson, James E. (1979). *Public Policy Making : An Introduction*. https://medium.com/@indotesis/pengertian-bentuk-dan-tahapan-kebijakan-publik-b4edd8aaf462. Downloaded in September 2022.

[2]Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). *Profil Internet Indonesia 2022*. Page 10 - 17.
[3]Badan Siber dan Sandi Negara (BSSN). (2021). *Laporan Tahunan : Monitoring Keamanan Siber 2021*. Page 78 - 80.
[4]Center for Digital Society Universitas Gadjah Mada (CfDS UGM). (2019). *Strategi Keamanan Siber Indonesia : Rekomendasi Rencana Aksi dan Implementasi*. Page 16.
[5]Chandler, Ralph C dan Plano, Jack C. (1988). *The Public Administration Dictionary*. https://www.gramedia.com/literasi/pengertian-kebijakan-publik/. Downloaded in September 2022.
[6]Dunn, William N (2003). https://www.kajianpustaka.com/2017/03/pengertian-bentuk-dan-tahapan-kebijakan-publik.html. Downloaded in September 2022.
[7]General Data Protection Regulation (GDPR). (2018). https://en.wikipedia.org/wiki/General_Data_Protection_Regulation Downloaded in September 2022.
[8]Hootsuite - Social Media Management Platform. (2022). https://datareportal.com/reports/digital-2022-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2022&utm_term=Indonesia&utm_content=Global_Promo_Block. Downloaded in September 2022.
[9]Kementerian Sekretariat Negara Republik Indonesia. (2022). https://www.setneg.go.id/baca/index/presiden_jokowi_instruksikan_jajarannya_tindak_lanjuti_dugaan_kebocoran_data_pemerintah. Downloaded in September 2022.
[10]Kompas. (2022). *Kilas Balik : Lima Kasus Kebocoran Data Pribadi Di Indonesia*. https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-?page=all. Downloaded in September 2022.
[11]Laws of Malaysia Act 709. (2010). *Personal Data Protection Act 2010*. https://www.dataguidance.com/sites/default/files/personal_data_protection_act_2010.pdf. Downloaded in September 2022.
[12]Lembaga Studi dan Advokasi Masyarakat (ELSAM). (2022). https://www.cnnindonesia.com/teknologi/20220913112558-185-847090/ruu-pdp-final-lembaga-pdp-di-bawah-presiden-bisa-independen. Downloaded in September 2022.
[13]National Cyber Security Index (NCSI). (2020). https://ncsi.ega.ee/ncsi-index/. Downloaded in September 2022.
[14]Ookla - The Global Broadband Speed Test. (2022). https://datareportal.com/reports/digital-2022-indonesia. Downloaded in September 2022.
[15]Organization for Economic Co-operation and Development (OECD). (2021). https://data.oecd.org/ict/internet-access.htm. Downloaded in September 2022.
[16]Personal Data Protection Act 2012. (2012). https://sso.agc.gov.sg//Act/PDPA2012. Downloaded in September 2022.
[17]Personal Data Protection Committee (PDPC). (2021). https://seitimes.com/kronologi-kebocoran-data-pelanggan-reddoorz-singapura-dan-asia-tenggara/. Downloaded in September 2022.
[18]Sistem Manajemen Keamanan Informasi ISO 27001. https://www.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity. Downloaded in September 2022.

[19]Surfshark. (2022). *Data Breach Statistics By Country: First Quarter of 2022.* https://surfshark.com/blog/data-breach-statistics-by-country. Downloaded in September 2022.
[20]Undang-Undang Informasi dan Transaksi Elektronik. (2008).
[21]Undang-Undang Pelindungan Data Pribadi. (2022).
[22]Widiana, A., Wijaya, C., & Atmoko, A. W. (2022). The Challenges of Food Security Policy in Indonesia: Lesson Learned from Vietnam, India, and Japan. *Technium Social Sciences Journal*, *33*(1), 1-15. https://doi.org/10.47577/tssj.v33i1.6937. Downloaded in September 2022.