

Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation

Valentina Ancillia Simbolon^{1*}, Vishnu Juwono²

¹² Faculty of Administrative Sciences, University of Indonesia, Depok, Indonesia

Email: valentina.a@ui.ac.id ; vjuwono@ui.ac.id

Abstract. Data leakage is one of the high potentials for criminal acts in cyberspace. The Indonesian government passed the Personal Data Protection Act (UU PDP) to ensure the security of every citizen's personal data. This study aims to compare the policies of the Personal Data Protection Act with the European Union General Data Protection Regulations (EU-GDPR). This study uses a qualitative descriptive analysis method with data from previous studies and official releases from the Indonesian government and the European Union. The results of this study illustrate that the PDP Law and the EU-GDPR have the same arrangements regarding the rights of personal data subjects. In the data processing aspect, the principle of processing personal data in the PDP Law is not mandatory. In contrast, in the EU-GDPR, the principle of processing personal data is mandatory. In the aspect of controlling and processing personal data, both rights and responsibilities are almost the same, both for the PDP Law and the EU-GDPR. In the aspect of imposing sanctions, EU-GDPR is more apparent in the mechanism of imposing sanctions in the form of fines. While in the PDP Law, sanctions consist of administrative sanctions, criminal sanctions, and criminal fines, the mechanism of imposing sanctions is not yet clear.

Keywords: Data; Protection; Regulation; Leakage

Received:14-11-2022 **Revised:**15-12-2022 **Accepted:**30-12-2022

INTRODUCTION

The increasingly high and massive use of the internet is the impact/effect of the penetration of digital technology, which is increasingly commonly used in the human environment. The use of the internet opens opportunities for people to connect without being limited by space and time. Ease of access is one of the crucial factors in increasing internet usage today. Digital 2022 April Global Statshot Report (Simon Kemp, 2022) reported that the number of internet users in the world reached 5 billion users or 63 percent of the world's population. This number has increased by nearly 200 million users from the previous year. Indonesia occupies the fourth position of all internet users worldwide, with 204.7 million users, after the People's Republic of China (PRC), India, and the United States (Statista.com, 2022).

Email Correspondence*:

valentina.a@ui.ac.id

The Association of Internet Service Providers in Indonesia (APJII) survey yielded data on the internet penetration rate in Indonesia in 2021 of 77.02 percent, meaning that 77.02 percent of the population are internet users. This figure increased by 3.32 percent from the previous year and spread across all provinces in Indonesia (Direktorat Jenderal Aplikasi Informatika, 2021). The condition of the Covid-19 pandemic has also affected the development of an increasingly high internet network because most community activities are carried out in online media that require an internet connection.

The high use of the internet raises the potential for data leakage. Data leaks arise from data theft, data loss, data storage discrepancies, and hacking actions. Todd mentions (Todd, 2019) that data collection has become essential to business processes, so data is a critical corporate asset. For this reason, electronic data is a valuable item that often becomes the object of theft. In addition, there is a tendency for data leakage to increase in terms of quantity and motive from 2005 to 2018. (Jung, 2021). Electronic data leaks have reached almost 27 million data since 2009 (the beginning of the calculation of data leaks in the internet world) until September 2013 (Wikina, n.d.). The data breach covers 674 entities and 153 health-related business associations. In mid-2018, SingHealth (Singapore Health Services), the largest healthcare institution in Singapore, experienced a major electronic data leak. It reported that as many as 1.5 million SingHealth patient data, including the personal data of the Prime Minister of Singapore, Lee Hsien Loong, were stolen and taken hostage (ransom) by hackers capable of exploiting SingHealth's electronic system, namely IHiS, Integrated Health Information Systems (Arif Rahman, 2019).

In Indonesia, data leaks often occur due to digital transformation, which the government echoes to improve public services. Based on the data leak report released by the National Cyber and Crypto Agency (BSSN) in 2020 (Rilis Resmi BSSN 2020), there are still many data leaks, especially personal data involving electronic system operators from both government and private elements. Based on the BSSN release, personal data leaks for BPJS Health participants totaled around 279 million participants consisting of National Identity Numbers (NIK), BPJS Participant Numbers, and as many as 20 million data containing pictures or photos of NIK owners. The same thing also happened to personal data belonging to around 2 million BRI Life insurance company customers who were allegedly leaked and sold on the internet. At the end of August 2021, there was a data leak of 1.3 million users of the Ministry of Health's eHAC application. In November 2021, hackers from Brazil claimed to have broken into the data of Polri personnel, and there were many other leaks of personal data.

In August 2022, Indonesia was shocked by unscrupulous hackers with callsigns Bjorka (Devira Prastiwi, 2022). The hacker leaked the personal data of Indonesian citizens and sold it on the Raid Forum. Data sold by Bjorka consist of Indihome customer data of 26 million customers (NIK, email, gender, keywords, and names), 1.3 billion SIM card user data, 105 million Indonesian citizen data leaked through the Commission's electronic system General Elections (KPU), list of letters from the State Intelligence Agency to the President of the Republic of Indonesia, and data on high-ranking state officials from the PeduliLindungi application. These various incidents of data leakage show the loss of citizens' privacy, which relates to the personal lives of data owners (Schauer, 1998).

The government has regulated the security of personal data in Government Regulation Number 71/2019 concerning the Implementation of Electronic Transaction Systems (PP PSTE 2019). The regulation states, "Personal Data is any data about a person, whether identified and/or identifiable separately or combined with other information, either directly or indirectly through electronic and/or non-electronic systems." Article 8 letter (a) PP PSTE also states, "Software used by Electronic System Operators must be guaranteed the security and reliability of operation as it should be." In its implementation, matters concerning personal data protection are regulated in the Regulation of the Minister of Communication and Informatics Number 20/2016 concerning Protection of Personal Data in Electronic Systems (Permenkominfo No.16/2016). This regulation is an implementing regulation on PP PSTE relating to guidelines for protecting personal data in electronic systems held in Indonesia. However, this regulation is ineffective because electronic systems administrators are not optimal in protecting personal data managed in their respective electronic systems.

The government enacted Law Number 27 of 2022 concerning Personal Data Protection to improve the security of Indonesian citizens' personal data (UU PDP, 2022). It is hoped that the presence of regulations can guarantee legal certainty for the Indonesian people, who are often victims of personal data leaks. The PDP Act is a benchmarking result from the European Union General Data Processing Regulations (EU-GDPR). The EU-GDPR is a regulation issued by the European Union that aims to protect the personal data and privacy of individuals living in the EU and European Economic Area (EEA) in the digital realm and promotes the more responsible use and processing of personal data. This regulation has been in effect since May 25, 2018, in EU member states and countries in the EEA. The EU-GDPR is also based on human rights principles and is considered an international benchmark for personal data protection (Sholikhah et al., 2021).

Previous research (Dio Ramadi Natha et al., n.d.) revealed that there are legal remedies that can be taken when personal data leaks occur, both by way of adjudication, which consists of litigation and arbitration, as well as through mediation and negotiation consensus processes. The facts show that law enforcement using Permenkominfo No.20/2016 cannot be used because the rule is a technical regulation. Next, Putri and Fahrozi (Destriani et al., 2020) said that the PDP Bill could be a solution to overcoming the uncontrolled leakage of personal data in Indonesia because government agencies already have solid legal standing in the law enforcement process. These studies further confirm that existing policies cannot address the problem of personal data leakage in Indonesia.

The previous research has focused on existing regulations such as the ITE Law, PP PSTE, and Permenkominfo No.20/2016, which discusses the protection of personal data that does not have clarity regarding the processes and mechanisms for protecting the rights of personal data subjects, the rights, and obligations of processors and controllers of personal data, as well as mechanisms for imposing sanctions. Meanwhile, the novelty of this research is to compare the PDP Law and the EU-GDPR to obtain an overview of the regulatory areas of the EU-GDPR and the PDP Law, especially in protecting personal data and law enforcement. The limitations in this paper are related to differences in state conditions such as the legal system, government bureaucracy, social, economic, and others.

METHODS

This research uses a qualitative descriptive analysis method to picture a situation objectively (Zha et al., 2018). The research data is sourced from literature studies, namely collecting relevant data and information, which is then studied, recorded, and processed to achieve objective research results. The data needed in this research is previous research taken from various journals that discuss data leakage, data protection policies in Indonesia, data protection policies in the European Union, as well as data that comes from official government releases.

This study uses secondary data. Article search process using the keywords "data leaks in Indonesia", "personal data protection policies in Indonesia", "comparative study data protection policy", and "the effectiveness of EU GDPR". The selected articles discuss personal data protection in Indonesia, the effectiveness of the EU GDPR policy, and the effects of personal data leakage. These articles became the primary reference data in this paper through analysis adjusted for research purposes.

RESULTS AND DISCUSSION

The enforcement of regulations regarding personal data in GDPR countries began with directives from the European Union commission on data protection issued in 1995. That aims to protect the data of all EU citizens, both electronic and non-electronic. The European Union Commission then officially enacted rules regarding the protection of personal data on May 25, 2018 (ben Welford, n.d.). Before it was formally enforced, the European Union Commission first allowed all stakeholders administering the electronic system to prepare instruments for compliance with GDPR for two years. The main things regulated in the GDPR policy are Personal Data Subjects, Personal Data Controllers, Personal Data Processors, and Sanctions (GDPR.EU, n.d.).

Implementing personal data protection in Indonesia is necessary because, after the Electronic Information and Transaction Law issuance, all electronic system operators must maintain the reliability of their electronic systems. Reliability is the probability that a product will work according to the desired function without failure under certain operating conditions and for a certain period (Sitania, 2010). The fact is that there are many failures in the operation of electronic systems in Indonesia, causing high data leaks, especially personal data leaks. At first, the Ministry of Communication and Informatics (Kemenkominfo) tried to create a policy catalyst for personal data protection by issuing Permenkominfo Number 20 of 2016 concerning personal data protection. Still, this regulation was not sufficiently binding on electronic system administrators who acted as controllers of personal data and processors of personal data. The presence of the PDP Law, which the government and the DPR passed on September 20, 2022 is a good milestone for Indonesia in ensuring the security of Indonesian citizens' personal data, both electronic and non-electronic (TN/AHA, 2022). This research divides into two areas of discussion, namely (1) a comparison of Data Protection Governance in the EU-GDPR and the PDP Law and (2) Challenges to the Implementation of the PDP Law in Indonesia.

Comparison of Data Protection Governance in the PDP Law with the EU-GDPR

The scope of discussion on the governance of the PDP Law and the EU-GDPR consists of the Rights of Personal Data Subjects, Processing of Personal Data, Controllers and Processors of Personal Data, and Imposition of Sanctions.

Personal Data Subject Rights

The analysis found that the rights of personal data subjects between the EU-GDPR and the PDP Law were more or less the same because the PDP Law was a benchmarking result from the EU-GDPR. The PDP Law and the EU GDPR both regulate the rights possessed by personal data

subjects, such as the right to be informed, the right to access data, the right to change data, the right to delete data, and the right to limit and refuse data processing.

The fundamental difference between the EU-GDPR and the PDP Law lies in the exclusion/limitation of the rights of personal data subjects. Within the EU- GDPR (GDPR.EU, n.d.), the implementation of the policy of limiting/exclusion of the rights of personal data subjects must contain several things, namely : (a) the purpose of processing or the category of the processing; (b) categories of personal data; (c) the scope of the restrictions introduced; (d) safeguards to prevent misuse or unlawful access or transfer; (e) controller specifications or controller categories; (f) the applicable storage and custody period taking into account the nature, scope, and purpose of processing or processing category; (g) risks to the rights and freedoms of data subjects; and (h) the right of the data subject to be notified of the restriction, unless doing so would be detrimental to the purpose of the restriction. This exclusion aims to maintain the consistency of protection for individuals so that the state or authorities do not act arbitrarily by smuggling regulatory terminology. While in the PDP Law, the implementation of the policy of limiting/exclusion of the rights of personal data subjects have not been regulated clearly and in detail.

Personal Data Processing

From the results of the analysis, it was found that the principle of processing personal data in the EU GDPR is mandatory. In contrast, in the PDP Law, the principle of processing personal data is not explained as something mandatory.

Within the EU-GDPR, personal data processing activities can be carried out by considering 6 (six) principles (GDPR.EU, n.d.), that is:

- a. Consent: Data processing can be carried out based on the consent given by the personal data subject to his personal data processing activities. The consent given by the personal data subject must be explicit, accessible, specific, and not cause ambiguity.
- b. Performance of Contract/Contractual Obligation: Data processing may be performed for the performance of a contract to which the data subject is a party or to take steps at the data subject's request before signing the contract.
- c. Legal Obligation: Data processing can be carried out to fulfill legal obligations, which are the responsibility of the personal data controller.
- d. Vital Interest: The processing of personal data may be carried out to protect the vital interests of the data subject or other person.

- e. Public Interest: The processing of personal data may be carried out for the performance of tasks performed in the public interest or the exercise of official powers conferred on controllers
- f. Legitimate Interest: Processing can be carried out for legitimate interests by personal data controllers and processors unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require personal data protection, especially if the data subject is a child.

Personal Data Controller and Personal Data Processor

The analysis found that the personal data controllers and personal data processors in the PDP Law and the EU-GDPR have the same rights and obligations. The fundamental difference is that every processing of personal data in the EU-GDPR must go through a Data Protection Impact Assessment (DPIA). At the same time, in the PDP Law, there is no mention of an assessment process from the personal data protection authority as stipulated in the PDP Law. Within the EU-GDPR, the personal data controller has a central role because it collects all personal data. A personal data controller is a legal entity, public authority, or other entity, alone or with others, that determines the purpose and means of personal data processing (GDPR.EU, n.d.). As personal data controllers, all legal entities/public authorities must be able to carry out their responsibilities in ensuring the security of personal data, the continuity of processing of personal data, and the rights of data subjects, so that the principles of personal data protection can be guaranteed. The principles referred to are based on law, fair, transparent, limiting objectives, minimizing data, data accuracy, limiting data storage, data confidentiality, data integrity, and data accountability can be guaranteed (GDPR.EU, n.d.).

In carrying out the duties and obligations of a personal data controller, the EU-GDPR requires that all processing of personal data carried out by the data controller must go through Data Protection Impact Assessment (DPIA). This assessment aims to determine personal data with a high risk (sensitive data), such as data on a person's political preferences, religion, ethnicity, race, sexual orientation, and health. Sensitive data initially complies with EU-Data Protection Directives are prohibited from being processed without the consent of the personal data subject. Thus, the entry into force of the EU-GDPR further strengthens that all sensitive data may not be processed arbitrarily by data controllers without going through the DPIA mechanism.

The DPIA mechanism assessment is based on measured risk from processing personal data using new technology and taking into account the characteristic, scope, context, and purpose of processing, which is likely to result in a high risk to the rights and freedoms of individuals.

Accordingly, the personal data controller must carry out an assessment of the impact of the planned processing on the protection of personal data before processing personal data.

The PDP Law describes the personal data controller as any person, public agency, or international organization, that acts individually or jointly in determining goals and exercising control over the processing of personal data. The Personal Data Controller is obliged to process personal data in a limited and specific manner, lawfully and transparently, and carry out the processing of personal data for the purpose of personal data processing. Under the PDP Law, the Personal Data Controller is not required to carry out an assessment to determine which personal data is high, medium, or low risk (UU PDP, 2022). All data is considered the same so that the treatment of personal data processing is done the same. The absence of a risk impact assessment carried out certainly has advantages and disadvantages. The advantage is that personal data will be processed with the same treatment so that the risk of sensitive personal data with ordinary personal data will be considered the same. When a data leak occurs, the treatment will also be the same. While the drawback is that when there is no risk-based assessment, priority-based risk mitigation cannot be carried out because personal data controllers carry out personal data processing regardless of the potential risk of personal data. The processor is a third party that processes personal data on behalf of the personal data controller. For example, in a social media company, the personal data controller is the social media company in question. In contrast, the personal data processor is a third party that uses the social media platform to monitor the behavior of social media users so that they can suggest certain advertisements to attract the attention of these social media users.

Sanctions

There are differences in sanctions between the EU-GDPR and the PDP Law. The EU-GDPR only provides administrative sanctions, while the PDP Law provides administrative and criminal sanctions (prison and fines). The calculation of administrative sanctions in the EU-GDPR is the same as the PDP Law; an ordinary violation will be subject to a fine of 2% of the violating company's annual global revenue. In comparison, serious violations will be subject to a fine of 4% of the violating company's annual global revenue. In the EU GDPR, a mechanism for administering administrative sanctions has been regulated. At the same time, in the PDP Law, there is no mechanism for imposing administrative or criminal sanctions that will be given to violators.

In imposing sanctions, the GDPR authorities consider the following aspects (GDPR.EU, n.d.):

- a. The nature of the severity and duration of the violation, taking into account the nature, scope, purpose of processing the data, and the number of data subjects affected, and the level of damage incurred;
- b. The character of the violation that occurred was caused intentionally or negligently;
- c. All measures taken by the personal data controller or processor to reduce the damage suffered by the personal data subject;
- d. The level of responsibility of controllers and processors of personal data taking into account the technical and organizational strategies implemented as stated in the EU-GDPR;
- e. Relevant previous violations that personal data controllers and processors have committed;
- f. The level of cooperation with the personal data supervisory authority to correct breaches and mitigate the adverse effects of said breaches;
- g. Categories of personal data affected by the breach;
- h. Notification of personal data security violations from personal data controllers and processors to supervisory authorities;
- i. Other aggravating or mitigating factors applicable to the circumstances of the case, such as the financial gain obtained or loss avoided, directly or indirectly, from the breach.

The level of EU-GDPR violations is divided into 2 (two) categories, namely ordinary violations and serious violations. The determination of ordinary and serious violations is based on the results of investigations carried out by the EU-GDPR enforcement authority. The following examples are companies that have been sanctioned as a result of being proven guilty of violating the EU-GDPR like Google. In 2019, Google was fined €50 million by the French state for the company's inability to make statements about the processing system of French citizens' personal data. Google is seen by the French state as failing to fulfill legal basis consent when Google uses customer data of French citizens for targeted purposes in advertising campaigns. Next British airways. In 2020, the British company Airways was fined € 20 million by the British government for failing to maintain the reliability of the ticket sales website. Hackers use the website to direct airline users to fraudulent sites, and hackers can access the personal data of airline users as many as 4,000 personal data to commit online fraud and the last Whatsapp . in 2020 (DW, 2021), Whatsapp was fined by the Irish state \$267 million for violating EU-GDPR policies. This company was accused and proven to have committed a personal data processing violation due to the transfer of data from the Whatsapp application server data to Facebook and Instagram.

Challenges of Implementation of Personal Data Protection Policy

Since it became effective in 2018, law enforcement through the process of imposing sanctions on companies that violate EU-GDPR provisions has been carried out. However, in practice, the EU-GDPR policy still faces formidable challenges, namely:

- a. Lack of readiness of business actors to meet and comply with EU-GDPR policies. In the first 11 months after implementation, the preparedness of business actors to comply with GDPR was only 8%, while 28% of business actors said they were not familiar with the EU-GDPR policy, and more than 51% of business actors said it was too complicated to comply with all the policies. Is in the EU-GDPR, especially for Micro, Small, and Medium Enterprises (MSMEs) (PRNewswire, 2017);
- b. There are additional costs for business actors to be able to pass the EU-GDPR policy compliance test certification. This will undoubtedly be difficult for MSME actors who have a business field in the personal data processing sector. Business actors must prepare staff who understand EU-GDPR policies and can carry out EU-GDPR compliance assessments so that when government authorities conduct an audit, the company is ready and obtains a certificate of compliance with EU-GDPR. A survey conducted in 2019 stated that MSMEs spend € 1000 to € 50,000 to get an EU-GDPR compliance certificate.

Just like the EU-GDPR, implementing the PDP Law in Indonesia certainly has the potential to face the same challenges because Indonesia's digital literacy is still not as mature as European Union countries. Potential obstacles to implementing the PDP Law are likely to come from various sectors, namely: The first challenge will, of course, come from MSME business actors. Based on a release issued by the Ministry of Cooperatives and Small and Medium Enterprises, there are 65 million MSME actors, and around 17.25 million (26.5%) are digital MSME actors. (Bank of Indonesia, 2021). Of course, some business actors in the digital MSME sector have businesses in the data processing sector, so they must strictly comply with all the provisions stipulated in the PDP Law to avoid administrative sanctions and criminal sanctions; The formation of the PDP Authority Institution must be manned by sufficient and competent personnel will pose challenges in Indonesia. The process of recruiting personnel who oversee the PDP authority agency must be made as influential as possible so that this person can be at the forefront of enforcing personal data protection in Indonesia and the PDP Law is a new legal regulation, so disseminating this policy rule also has its challenges. Policy outreach in Indonesia is often not on target, so many business actors are negatively affected. It is hoped that the

socialization of the PDP Law can be carried out correctly and on target so that all business actors, both individuals and corporations, have a high desire and awareness to comply with all the provisions contained in the PDP Law.

CONCLUSION

The research found several differences between the PDP Law and the EU-GDPR. Some of the differences are the exclusion of the rights of personal data subjects, the legal basis for processing personal data, the obligations of controlling personal data, and the imposition of sanctions. The principles of data processing, the process of imposing sanctions, and the authority of the personal data protection agency in the EU-GDPR are explained in more detail compared to the PDP Law. These three areas can be a reference so that the PDP Law can be more optimally implemented in Indonesia. The challenges of implementing the PDP Law in Indonesia can be overcome by conducting rapid, targeted, and effective dissemination so that business actors and public institutions understand the regulation. The government must also immediately form a personal data protection agency to oversee the PDP Law's implementation.

REFERENCE

- Arif Rahman. (2019, May 30). Tiga Penyebab Kebocoran Data di Kasus SingHealth. <https://cyberthreat.id/read/599/Tiga-Penyebab-Kebocoran-Data-di-Kasus-SingHealth>
- BBC. (2021, May 24). Three years of GDPR: the biggest fines so far. <https://www.bbc.com/news/technology-57011639>.
- Devira Prastiwi. (2022, September 12). 8 Fakta Terkait Kemunculan Hacker Bjorka yang Bocorkan Data Penting Indonesia. <https://www.liputan6.com/news/read/5067499/8-fakta-terkait-kemunculan-hacker-bjorka-yang-bocorkan-data-penting-indonesia>
- Direktorat Jenderal Aplikasi Informatika, dan tim. (2021). Dinamika Data Aplikasi Informasi Indonesia. In Jakarta Pusat (Issue 9).
- DW. (2021, February 9). Ireland fines WhatsApp €225 million for privacy breach. <https://www.dw.com/en/ireland-fines-whatsapp-225-million-for-eu-privacy-breach/a-59065206>.
- GDPR.EU. (n.d.). GDPR Subject-matter and objectives. <https://gdpr.eu/article-1-subject-matter-and-objectives-overview/>.

- Jung, K. (2021). Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk. *North American Actuarial Journal*, 25(4), 580–603. <https://doi.org/10.1080/10920277.2021.1919145>
- Natha, K. D. R., Budiarta, N. P., & Astiti, N. G. K. S. (2022). Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen pada Perdagangan Elektronik Lokapasar (Marketplace). *Jurnal Preferensi Hukum*, 3(1), 143-148.
- Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Berita Negara Republik Indonesia Tahun 2016 Nomor 1829 (2016).
- Peraturan Pemerintah Nomor 17 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara RI Tahun 2019 Nomor 185 (2019).
- Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.com). *Borneo Law Review*, 5(1), 46-68.
- Pusat Operasi Keamanan Siber Nasional. (2021). Laporan Monitoring Keamanan Siber Nasional.
- Todt, K. E. (2019). Data Privacy and Protection. *The Cyber Defense Review*, 4(2), 39-46. <https://doi.org/10.2307/26843891>
- Schauer, F. (1997). Internet privacy and the public-private distinction. *Jurimetrics*, 38, 555.
- Sholikhah, V. H., Sejati, N. R. F. F., & Shabitah, D. (2021). Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia. *Indonesian Scholars Scientific Summit Taiwan Proceeding*, 3, 54–63. <https://doi.org/10.52162/3.2021112>
- Simon Kemp. (2022). Digital 2022 April Global Statshot Report . <https://datareportal.com/reports/digital-2022-april-global-statshot>
- Sitania, F. D. (2010). Analisis Keandalan Produk Dengan Pola Penggunaan Intermittent. *Arika*, 4(2), 175-184.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara RI Tahun 2022 Nomor 196 (2022).
- Wikina, S. B. (n.d.). What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches.
- Zha, L. F., Nie, S. F., Chen, Q. W., Liao, Y. H., Zhang, H. S., Dong, J. T., Xie, T., Wang, F., Tang, T. T., Xia, N., Xu, C. Q., Zhou, Y. C., Zeng, Z. P., Jiao, J., Wang, P. Y., Wang, Q. K., Tu, X., & Cheng, X. (2018). IL-13 may be involved in the development of CAD via different

mechanisms under different conditions in a Chinese Han population. Scientific Reports, 8(1). <https://doi.org/10.1038/s41598-018-24592-9>