ISSN No:-2456-2165

Personal Data Protection Framework Ranking with Analytical Hierarchy Process (AHP)

Aqil Athalla Reksoprodjo[1], Muhammad Dachyar[2], Novandra Rhezza Pratama[3]
Department of Industrial Engineering, Faculty of Engineering, Universitas Indonesia, Depok, 16424, Indonesia

Abstract:- There are many options for personal data protection framework. However, there are no rank of the available frameworks. The ranking of the framework gives a perspective on the merit and drawbacks of the frameworks, and it will provide a point for consideration in adopting and implementing the framework. This study aims to rank potential framework options for protecting personal data. Experts are involved for the evaluation and scoring of the criteria. The Analytical Hierarchy Process (AHP) technique is used to weigh the selection criteria and rank the alternatives, respectively based on the expert's judgement. The findings demonstrate that for businesses ISO 27701 is the top framework of choice for personal data security.

Keywords:- *Framework Ranking; Personal Data Protection**;** AHP.*

I. INTRODUCTION

The rapid transmission of information via internet platforms has created chances for data hacking and unauthorized disclosure of data.

Approximately 73.7%, or approximately 202.6 million Indonesians, are active internet consumers, out of a total population of 274.9 million. While active social media users in Indonesia reached 170 million, or 61.8% of the country's total population [1]

In Indonesia, there are a total of 1,637,937,022 instances of anomalous cyber traffic, of which approximately 55 percent are aimed at data breaches [2]

As a result of this data hacking, both the owners of personal data and the organizations that administer such data have suffered significant losses. As one piece of personal identification information may be worth up to USD 180 [3] One of the reasons for this is that information, primarily personal data, is viewed as a commodity and has significant value for parties that can make use of it [4],[5]

Consequently, the security of information, particularly personal data and within cyberspace, is essential for businesses to have today and is of utmost importance [6]

This research is aimed to rank the available choices of framework for empowering personal data protection for Indonesian organization.

II. LITERATURE REVIEW

A. Personal Data Protection

Companies and organizations that collect, use, and process personal data are exhorted to be able to abide by all applicable laws and regulations, particularly those pertaining to personal data protection [7].

Companies that effectively implement personal data protection have a positive effect on company growth. [8]

With special attention to personal data protection, it has been demonstrated that businesses based on personal data protection can enhance their business and offer a competitive advantage to businesses or companies that implement it [9].

Complying with personal data protection practices is essential for businesses and organizations not only due to the regulations and benefits they provide, but also due to the necessity of doing so.

This is supported by the strong influence of digitalization on businesses in the present day. Digitalization has been extremely beneficial to human life, particularly in terms of integrating human life with technology [10]. Nevertheless, the digitalization process will typically increase security risks that digitalization actors typically overlook or give less attention to [10].

In addition to having a positive impact on the company and ensuring compliance with personal data protection regulations, there will be side effects in the form of increased company expenses induced by company compliance with personal data protection regulations.

Regional standards or regulations for the preservation of personal data exist, so each nation has its own set of regulations. The General Data Protection Regulation of the European Union is one of them. The GDPR is currently used as a guideline for data protection practices.

Not only the owner, collector, and user of data, but also third parties who process data are typically governed by regulations pertaining to the preservation of personal data [11],[12].

Given the importance of implementing personal data protection for companies or organizations, despite the fact that its application has negative side effects, but due to market demands in which personal data security is now a factor for consumers when selecting products or services, companies or

organizations must implement personal data protection practices.

The company must protect personal data utilized in its operations, such as consumer data, as well as the personal data of its employees, as both fall under the umbrella of personal data.

B. Personal Data Protection Framework

The development of technology, particularly in the communication and information sector, which is now integrated into daily life [13] is accompanied by a rise in contemporary difficulties. The development of new technologies has also spurred the issuance of new regulations, particularly concerning the protection of personal data. Regulations pertaining to the preservation of personal data govern the collection, handling, and use of personal data by organizations and businesses [13].

Compliance with personal data protection regulations presents a challenge for businesses and organizations. This is due to the complexity of business operations, particularly with the constant flow of information [13].

Due to the complexity of meeting the standards governed by personal data protection regulations, organizations and businesses require measures or frameworks to make it easier for them to comply.

The data framework is crucial to improving personal data protection systems and complying with regulations. There have been numerous frameworks for personal data protection, but selecting the correct one for an organization and complying with the regulation is challenging.

C. ENISA Guideline for Personal Data Protection

The European Union Agency for Network and Information Security, also known as ENISA, was established in 2004. Its mission is to increase the awareness and culture of information security and cybersecurity in the European Union's society [14].

ENISA has issued guidelines for personal data protection to aid in GDPR compliance and reduce the risk of noncompliance with the regulation. The guideline includes Data Protection by Design and Default, Data Protection Impact Assessment, Data Protection Engineering, Privacy Enhancing Technologies, and Data Breach Notification [15]-[18].

EU's GDPR also requires organizations to have a data breach notification system to ensure that if a data breach occurs within the organization, the organization will be notified and will attempt to mitigate the effects. The data incident notification guideline has been published by ENISA. It discusses how to manage an incident, as well as coordination with other parties, the content of notification information, and the timeline.

The ENISA is primarily viewed as beneficial for assisting organizations in complying with the GDPR.

D. ISO 27701:2019

The International Organization for Standardization (ISO) has issued ISO 27701 as a standard. Prior to the publication of ISO 27701, this standard was referred to as ISO 27752 during the formulation process; it was renamed ISO 27701 in 2019 [19] when it was ratified.

The ISO 27701 standard is an extension of the ISO 27001 standard that emphasizes the preservation of personal data in greater depth. ISO 27001 is a standard for information security in general; ISO 27701 is an extension or development that is more specific to information security for personal data [20], [21].

ISO 27701 was developed in response to global challenges in the protection of personal data. With the adoption of the EU General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) by the United Kingdom, all activities in the European Union and the United Kingdom that involve personal data must comply with these regulations. However, neither the GDPR nor the DPA specify how to achieve compliance with these regulations; this is the impetus behind the development of the ISO 27701 extension from its progenitor ISO 27001.

The Privacy Information Management System (PIMS) is thoroughly discussed in ISO 27701. This ISO 27701[22] standard addresses system design, system implementation, and system supervision.

ISO 27701 contains specific guidelines for PIMS design and implementation. Information security policy; information security organization; human resource security; asset management; access control management; cryptography; physical and environmental safety; security operations; communication security; acquisition, development, and maintenance of systems; management of supplier relationships; information security incident management; information security aspects on business continuity; Compliance [20], [21].

In addition to the design and implementation considerations of PIMS, ISO 27701 also provides specific guidelines for personal data managers and processors. Moreover, ISO 27701 is said to be compatible with and integrate well with existing standards and regulations [19].

E. ASEAN Personal Data Protection Framework

The ASEAN Organization is a collection of Southeast Asian countries. One of the objectives is to increase cooperation among its members in addressing diverse contexts of problems, including political, economic, social, cultural, and many others. Several member nations, including Singapore, Malaysia, Thailand, the Philippines, and now Indonesia, have legal regulations regarding personal data protection [23].

ISSN No:-2456-2165

Brunei Darussalam issued the ASEAN Framework on Personal Data Protection in 2016 through the ASEAN Telecommunications Ministers meeting in Bandar Seri Begawan [23], [24].

The ASEAN Framework on Personal Data Protection does not essentially require ASEAN member states to adopt this framework; this is to demonstrate the commitment of ASEAN member states to prioritize personal data protection [23]-[25].

This ASEAN framework contains seven main principles to strengthen the protection of personal data: (i) consent, notification, and purpose, (ii) accuracy of personal data, (iii) security, (iv) access and correction, (v) transfer between countries or territories, (vi) storage, and (vii) accountability [23].

III. RESEARCH METHODOLOGY

In Regarding data collection and processing, this study involves three main steps. These stages include determining the selection criteria, applying the Analytical Hierarchy Process (AHP) to weight the selection criteria, and ranking the alternatives.

For determining the selection criteria, the council of experts will evaluate which criteria can be considered in this study for the selection of a personal data protection framework based on a review of the relevant literature. In addition, the specialists suggested the inclusion of certain criteria in the selection procedure. The involved specialists have diverse backgrounds, with a focus on information security, cyber security, and risk management.

After the selection criteria have been determined, the AHP is used to calculate the relative importance of each criterion. The purpose of balancing the criteria is to determine which criteria should be given the most weight and consideration. [26],[27].
Expert Choice software is used to perform the AHP calculation.

IV. RESULTS AND DISCUSSION

This study aims to aid in the selection and ranking of three data framework alternatives for the preservation of personal data, considering the four most important criteria for selecting the data framework to be used by Indonesian businesses.

The framework alternatives are chosen according to how closely they adhere to Indonesia's characteristics. Due to the fact that every expert involved is Indonesian and conversant with the Indonesian environment. If the European Union General Data Protection (GDPR) is regarded as the most sophisticated rule for personal data protection, then the ENISA Personal Data Protection framework is involved, as it is widely used for complying with EU's GDPR. Other options include ISO 27701 and ASEAN Personal Data Protection Framework. ISO 27701 is a standard published by the International Organization for Standardization, and it was intended to be extensively implemented without regard to regional or regulatory restrictions. As a result of Indonesia's membership in ASEAN and 2016 ratification of the framework, the ASEAN PDP Framework is selected.

The criteria are derived from a review and analysis of literature review to data protection in general. There are a total of four criteria that could be considered for this study. In addition to criteria for literature analysis, the expert's opinion also includes additional criteria. The criteria consist of business & economy, legal, technical, and security.

The weight assigned to each ranking criterion is depicted in fig. 1 results.

Legal criteria are ranked as the highest priority criterion with a score of 0.61, followed by Business & Economy with 0.19, Security with 0.15, and Technical with 0.05.

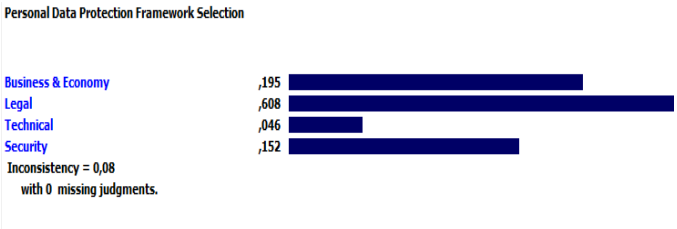

Fig 1. Criteria Weights

This indicates that compliance with the rules and regulations plays a significant role in determining which framework will be chosen. As a result of the fact that administrative sanctions, penalties, and criminal sanctions will be implemented if a company fails to comply with Indonesian law, noncompliance may result in company dissolution.

Based on the results, business & economy is more important than security. Complying with the requirements of the regulation may necessitate that businesses also plan their financial expenditures for adoption, operation, and technology, while the security will improve automatically. Therefore, the security factor is still regarded as significant, but it can be covered by legal factors. This is demonstrated by the comparatively low sum of the business & economy weight score of 0.19 and the security weight score of 0.15.

Technical is deemed less essential than the other three criteria, given that the objective is to comply with the rules and regulations by enhancing personal data protection. The company will have to adapt to the technical challenges that it may encounter. As a result, the objective is to comply with regulations and strengthen the system for protecting personal information.

After calculating the relative importance of each criterion, the next stage is to select the best alternative for the framework for protecting personal data. Fig 2 results represent the ranking of the framework alternatives considered in this study.

In comparison to ENISA and ASEAN, the score indicates that ISO 27701 is the best option. Since ISO 27701 is a part of the ISO standard series and an extension of ISO 27001, it is considered to be the most compatible with the environment of Indonesian organization and the easiest to integrate with existing systems. As a result, the framework will be easier to implement for many organizations in Indonesia that are already familiar with it. While the ENISA is believed to be more difficult to implement due to its emphasis on Privacy by Design, which must be incorporated into every system, it is simpler to implement in a new system. While ASEAN lacks specific details on how to implement the guidelines and the guidelines themselves, the ASEAN has adopted the guidelines.

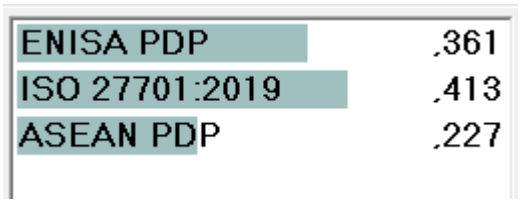

Fig 2. Framework Ranking

V. CONCLUSION

Based on the findings, it can be concluded that ISO 27001 is the highest-ranking personal data protection framework that Indonesian organizations can use to strengthen their personal data protection.

Legal criteria were the most essential criterion, so compliance with the rules and regulations is considered to be of the utmost importance. Followed by the business & economy criterion, which was the adoption and operation costs of the framework. The security criteria are adhered to, and if the regulations are met, the security will automatically follow and strengthen itself. Due to the need for compliance, which necessitates that businesses adapt to the technical difficulties encountered, the technical criteria were deemed to be of less important.

REFERENCES

[1]. Kementerian Komunikasi dan Informatika (Kominfo), "Laporan Kinerja Kementerian Komunikasi dan Informatika 2021,
[2]. D. O. K. S. Badan Sandi dan Siber Negara, "Laporan Tahunan 2021 Monitoring Keamanan Siber," Badan Sandi dan Siber Negara Republik Indonesia, 2022.
[3]. IBM Security, "Cost of a Data Breach Report," 2021.
[4]. N. N. Neto, S. Madnick, A. M. G. D. Paula, and N. M. Borges, "Developing a Global Data Breach Database and the Challenges Encountered," *Journal of Data and Information Quality*, vol. 13, no. 1, pp. 1–33, 2021, doi: 10.1145/3439873.
[5]. P. Petrov, I. Kuyumdzhiev, R. Malkawi, G. Dimitrov, and J. Jordanov, "Digitalization of Educational Services with Regard to Policy for Information Security," vol. 11, no. 3, pp. 1093–1102, 2022, doi: 10.18421/TEM113
[6]. A. A. Loishyn, S. Hohoniants, M. Y. Tkach, M. H. Tyshchenko, N. M. Tarasenko, and V. S. Kyvliuk, "Development of the Concept of Cybersecurity of the Organization," vol. 10, no. 3, pp. 1447–1453, 2021, doi: 10.18421/TEM103.Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7]. O. Olukoya, "Assessing frameworks for eliciting privacy & security requirements from laws and regulations," *Comput Secur*, vol. 117, p. 102697, 2022, doi: 10.1016/j.cose.2022.102697.
[8]. O. Y. Guseva, I. O. Kazarova, I. Y. Dumanska, M. A. Gorodetskyy, L. V Melnichuk, and V. H. Saienko, "Personal Data Protection Policy Impact on the Company Development," *WSEAS Transactions on Environment and Development*, vol. 18, pp. 232–246, 2022, doi: 10.37394/232015.2022.18.25.
[9]. A. Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 78–82, 2020, doi: 10.1109/MCE.2019.2953739.
[10]. A. Shahim, "Security of the digital transformation," *Comput Secur*, vol. 108, p. 102345, 2021, doi: 10.1016/j.cose.2021.102345.
[11]. N. K. S. Dharmawan, D. P. D. Kasih, and D. Stiawan, "Personal data protection and liability of internet service provider: A comparative approach," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 4, pp. 3175–3184, 2019, doi: 10.11591/ijece.v9i4.pp3175-3184.
[12]. Z. S. Li, C. Werner, N. Ernst, and D. Damian, "Towards privacy compliance: A design science study in a small organization," *Inf Softw Technol*, vol. 146, no. April 2021, p. 106868, 2022, doi: 10.1016/j.infsof.2022.106868.
[13]. V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO / IEC27001 : 2013 and ISO / IEC27002 : 2013 to GDPR compliance controls," *Information & Computer Security*, 2020, doi: 10.1108/ICS-01-2020-0004.
[14]. D. Markopoulou, V. Papakonstantinou, and P. de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation," *Computer Law and Security Review*, vol. 35, no. 6, p. 105336, 2019, doi: 10.1016/j.clsr.2019.06.007.
[15]. European Network and Information Security Agency, *Privacy and Data Protection by Design – from policy to engineering*, no. December. 2014. doi: 10.2824/38623.
[16]. European Network and Information Security Agency, "ONLINE PLATFORM FOR SECURITY OF PERSONAL," 2019. doi: 10.2824/3000.
[17]. European Network and Information Security Agency, *DATA PROTECTION ENGINEERING*, no. January. 2022.
[18]. European Network and Information Security Agency, "A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment," no. December, 2017.

[19]. International Standard Organization, *INTERNATIONAL STANDARD ISO / IEC Security techniques — Extension to*, vol. 2019. 2019.
[20]. O. M. Fal', "Documentation in the ISO/IEC 27701 Standard," *Cybern Syst Anal*, vol. 57, no. 5, pp. 796–802, 2021, doi: 10.1007/s10559-021-00404-3
[21]. M. I. Fadhil, "Control Design of Information Security Related to Privacy in The Smart SIM Business Process," pp. 66–72, 2021.
[22]. S. A. Grishaeva, "Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701 : 2019," pp. 2021–2023, 2021.
[23]. T. Tampubolon and R. Ramadhan, "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara," *Padjadjaran Journal of International Relations*, vol. 1, no. 3, p. 270, 2020, doi: 10.24198/padjir.v1i3.26197.
[24]. ASEAN, "Framework on Personal Data Protection," pp. 1–6, 2016.
[25]. S. S. Surtiwa, C. J. Gultom, F. Law, U. Indonesia, and J. Barat, "Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer to Peer Lending ASEAN for Data Protection :," vol. 558, no. Aprish 2019, pp. 720–726, 2021.
[26]. G. Giovanni, R. Gita, M. Dachyar, and N. R. Pratama, "Ideal Location Selection for Global Excavator Manufacturing Facilities in North America," no. July 2021, pp. 310–319, 2022.
[27]. M. Dachyar, M. Salman, and R. Nurcahyo, "Strategies to Improve the Education and Research Scholarship Program at the Universities," vol. 12, no. 1, pp. 389–395, 2023, doi: 10.18421/TEM121.