ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 2, pp. 156-171
DOI:10.33168/JSMS.2024.0210

A Decision-Making Model for Selecting Personal Data Protection Frameworks for Companies in Indonesia

Aqil Athalla Reksoprodjo, Muhammad Dachyar, Novandra Rhezza Pratama

Department of Industrial Engineering University of Indonesia, Depok, West Java, Indonesia 16424
a.a.reksoprodjo@gmail.com

Abstract. In the modern business landscape, companies frequently utilize personal data for various purposes. However, a lack of attention to data security can create vulnerabilities that may lead to data breaches and misuse of personal information. To bolster personal data protection efforts, the implementation of a robust data security system is imperative. Selecting an appropriate framework plays a crucial role in enhancing personal data protection measures. For companies operating in Indonesia, the absence of a dedicated personal data protection framework tailored to Indonesia's Personal Data Protection Act adds complexity to the selection process. This research aims to address this challenge by identifying the optimal framework alternative for personal data protection. To achieve this objective, an Analytical Hierarchy Process (AHP) approach is employed to ascertain the relative importance of selection criteria. Subsequently, the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is used to rank the available alternatives. The findings of this study reveal that ISO 27701 emerges as the top choice for the personal data protection framework for companies in Indonesia. By adopting ISO 27701, businesses can enhance their data security measures, comply with relevant regulations, and safeguard personal data more effectively. This research provides valuable insights to assist companies in Indonesia in making informed decisions to protect sensitive personal information.

Keywords: Framework Selection, Personal Data Protection, Information Security, Decision Making

1. Introduction

The high rate of information exchange through internet media enables opportunities for crime in the form of data hacking and the misuse of personal data.

Indonesia has a total population of 274.9 million, of which 73.7%, or around 202.6 million Indonesians, are active internet users. While active social media users reached 170 million people, or equivalent to 61.8% of the total population of Indonesia. (Kementerian Komunikasi dan Informatika (Kominfo), 2021)

There is a total of 1.637.937.022 anomalous cyber traffic in Indonesia with approximately 55% being aimed at data breaching (Badan Sandi dan Siber Negara, 2022).

The losses experienced by both personal data owners and companies that manage personal data are quite significant due to this data hacking. As one personal identification information may be worth up to 180 USD (IBM Security, 2021). One of the reasons is that information, mostly personal data, is considered a commodity and has a significant value for parties that can make good use of it (Neto et al., 2021; Petrov et al., 2022).

Meanwhile, on the other hand, the government of the Republic of Indonesia has passed the Indonesian Republic Act number 27/2022 concerning Personal Data Protection (PDP Act) to protect especially the owners of personal data. The collection, management, processors, and users of personal data need to refer to the PDP Act or will be subject to sanctions as stipulated in the provisions of the PDP Act.

Therefore, the security of information, especially personal data and within cyberspace is very important nowadays and companies need to have it (Loishyn et al., 2021; Altarawneh & Tarawneh, 2023).

Thus, companies in Indonesia need to have a data protection system, especially for personal data protection, to thwart hacking efforts, prevent the misuse of personal data, and conform to the standards imposed by the PDP Act. Although there are now various alternative frameworks, none have been specifically designed for companies in Indonesia or based on the Indonesian PDP Act.

The personal data protection frameworks are in place to assure that everyone’s private information is respected and protected from any unauthorized access, misuse, and abuse.

In conclusion, a personal data protection framework intends to establish a legal and regulatory environment that helps protect individuals' personal data and encourages organizations to use responsible data-handling practices to preserve public trust in the digital age and protect individuals' privacy.

The vital function of the framework adds up to the urgency of companies in Indonesia to select the currently available frameworks to strengthen their personal data protection system.

The lack of research considering the importance of personal data protection in Indonesia triggered this research. Several publications discuss personal data protection in Indonesia, but it merely discusses the importance of the legal side (Sudarwanto & Kharisma, 2021). However, none of them discusses the technical of the implementation and what the affected organization should do to comply with the Indonesian PDP Act.

Malindzakova & Puskas (2018) build a decision-making model for ERP selection with data protection consideration. This remains the closest model to be considered. However, the criteria are already preset and predetermined and do not go through a validation process with the panel of experts. Other than that, it only uses the AHP method for both criteria weighting and alternatives ranking thus making it less robust than using a different method for each criteria weighting and alternatives ranking.

The available frameworks are yet to be chosen by companies and organizations. The lack of a decision-making model reference for choosing the right and relevant framework adds to the challenges for companies to select the framework.

Until now several questions remain not yet clearly answered. What are the criteria for selecting the frameworks? Do the criteria weights affect the framework selection? The answer to the questions will

be a strong point and guidance for selecting the best framework to be implemented.

This research's main objective is to obtain the first choice of framework for empowering personal data protection for Indonesian-based companies and to further comply with the Indonesian PDP Act.

2. Literature Review

2.1. Personal Data Protection

Organizations and companies that collect, utilize, and process personal data are urged to be able to abide by all applicable laws and regulations especially those that are related to personal data protection (Olukoya, 2022).

Companies that successfully implement personal data protection have a positive impact on company development (Guseva et al., 2022; Madyatmadja et al., 2023).

With special attention to personal data protection, it has been shown that businesses based on personal data protection can improve their business and provide a competitive advantage for businesses or companies that implement it (Cavoukian, 2020; Cui & Lim, 2022).

Not only because of the regulations and positive impacts provided but complying with personal data protection practices is also a necessity for companies or organizations.

This is supported by the strong influence of digitalization on companies today. Digitalization has helped human life a lot, especially in integrating human life with technology (Shahim, 2021). However, the digitization process will generally increase security risks that usually digitalization actors neglect or pay less attention to (Shahim, 2021).

In addition to having a positive impact on the company, and to comply with personal data protection regulations, there will be side effects in the form of increased company expenses caused by company compliance with personal data protection regulations (Tsohou et al., 2020).

Standards or regulations for personal data protection are regional so each country has its regulations. Among them is the European Union's General Data Protection Regulation or GDPR. The GDPR is now used as a guideline for personal data protection practices.

Regulations regarding personal data protection generally also regulate third parties who process data so that it is not only the owner, collector, and user of data (Dharmawan et al., 2019; Li et al., 2022).

Given the importance of implementing personal data protection for companies or organizations even though its application produces side effects, due to market needs where personal data security is now one of the factors for consumers in choosing products or services, companies or organizations need to implement personal data protection practices.

The company has to protect personal data utilized in its operations, such as consumer data, but it also must protect the personal data of its workers because both fall under the scope of personal data.

2.2. Indonesia Personal Data Protection Act

The regulation regarding Personal Data Protection is designed to fulfill the mandate of the Constitution of the Republic of Indonesia article 28 concerning human rights and adhere to the values of Pancasila (*Undang-Undang Perlindungan Data Pribadi*, 2022).

The Act contained in Personal Data Protection Act will provide security for the personal data of the Indonesian people and uphold state sovereignty and will remain in effect even outside the jurisdiction of the Indonesian Territorial Act in the event of a violation that influences the Indonesian people or has a legal impact in the jurisdiction of Indonesian Act (*Undang-Undang Perlindungan Data Pribadi*, 2022). Personal data according to the Personal Data Protection Act can be understood as "any data about a person either identified and/or identifiable separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems." (*Undang-Undang Perlindungan Data Pribadi*, 2022).

In addition, personal data is also categorized into two, namely general and specific personal data.

Full name, gender, nationality, religion, and/or other personal information that can be used to identify a person are examples of general personal data. Meanwhile, Health information and data, biometrics, genetics, political beliefs, life/sexual orientation, criminal history, child information, personal financial information, and/or other information in line with laws and regulations are an example of specific personal data. (*Undang-Undang Perlindungan Data Pribadi*, 2022)

In the Personal Data Protection Act, 12 points regulate the types of personal data; ownership rights over personal data; handling of personal data; obligations of the personal data controller and the personal data processor in the processing of personal data; transfer of personal data; administrative sanctions; prohibition in the use of personal data; establishment of a code of conduct for the personal data controller; dispute resolution and procedural Act; international cooperation; the role of government and society; and the last is the criminal provisions (*Undang-Undang Perlindungan Data Pribadi*, 2022)

The Personal Data Protection Act's existence shows the commitment of the Indonesian government in protecting the rights of its citizens to the security of their personal data. The government also hopes that the existence of the Personal Data Protection Act can be used as an opportunity for business actors whose activities intersect with the use of personal data to increase public trust and are not seen as a burden for compliance obligations and avoid mere violation sanctions.

With the enactment of the Personal Data Protection Act recorded in the State Gazette of the Republic of Indonesia as Act of the Republic of Indonesia Number 27 of 2022 in October 2022, organizations and companies whose activities intersect with the use of but not limited to customer personal data, in particular, will need to obey with this PDP Act which the government of the Republic of Indonesia is given relaxation of its effective enactment, which is two years after the passing of the PDP Act. Therefore, organizations and companies whose activities intersect with personal data protection are required to comply with the PDP Act no later than October 2024 and sanctions will be imposed as stipulated in the PDP Act for parties who violate its provisions.

The hope is that this Personal Data Protection Act can become a legal basis to harmonize several existing Acts related to personal data protection that are less comprehensive. So that the personal data of the Indonesian people can be protected from parties who try to take advantage without the permission of the data owner and the regulations of the PDP Act.

2.3. Personal Data Protection Framework

Challenges in modern times are increasing along with the development of technology, especially technology in the communication and information sector which has now been integrated with everyday human life (Diamantopoulou et al., 2020). Technological developments have also encouraged the issuance of new regulations, especially regarding personal data protection. Regulations related to personal data protection specifically regulate the gathering, handling, and use of personal data by an organization or company (Diamantopoulou et al., 2020)

Compliance with personal data protection regulations is a challenge for organizations and companies. This is because of the complexity of business operations, especially with a continuous flow of information (Diamantopoulou et al., 2020)

With its complexity to meet the standards regulated by personal data protection regulations, steps or frameworks are needed to make it easier for organizations or companies to be simpler in meeting the standards of personal data protection regulations.

The data framework plays a pivotal role in enhancing personal data protection systems and complying with the regulations. There have been several frameworks for personal data protection, however choosing the right one for a company and complying with the regulation is a challenge.

2.4. ASEAN Personal Data Protection Framework

In 2016 through the ASEAN Telecommunications Ministers meeting in Bandar Seri Begawan, Brunei Darussalam issued a framework for personal data protection known as the ASEAN Framework on

Personal Data Protection (ASEAN, 2016; Tampubolon & Ramadhan, 2020).

The ASEAN Framework on Personal Data Protection does not oblige ASEAN member states to adopt this framework, and this is to demonstrate the commitment of ASEAN member states to prioritizing personal data protection (ASEAN, 2016; Surtiwa et al., 2021; Tampubolon & Ramadhan, 2020)

This ASEAN framework has seven main principles to strengthen personal data protection, the seven principles are (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 (ASEAN, 2016).

2.5. ISO 27701:2019

ISO 27701 is a standard issued by the International Standardization Organization (ISO). Before ISO 27701 was issued, during the process of formulation this standard was also known as ISO 27752 and changed to ISO 27701 when it was ratified in 2019 (International Standard Organization, 2019).

The ISO 27701 standard is an extension of the ISO 27001 standard which focuses more on in-depth personal data protection. ISO 27001 itself is a standard for information security in general so ISO 27701 is an extension or development that is more specific to information security in the form of personal data (Fadhil, 2021; Fal', 2021).

ISO 27701 was developed to address global challenges regarding personal data protection. The passage of the EU GDPR and the Data Protection Act (DPA) by the United Kingdom requires all activities in the European Union and the United Kingdom that intersect with personal data to comply with these regulations. However, neither the GDPR nor DPA does not specify how to achieve compliance with these regulations, and this is the basis for developing the ISO 27701 extension from its parent ISO 27001.

ISO 27701 comprehensively discusses the Privacy Information Management System (PIMS). Starting from system design to system implementation and supervision are all contained in this ISO 27701(Grishaeva, 2021).

Specifically, ISO 27701 contains guidelines for designing and implementing PIMS. The points discussed include 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 relationships with suppliers; information security incident management; information security aspects on business continuity; Compliance (Fadhil, 2021; Fal', 2021).

In addition to the design and implementation points of PIMS, ISO 27701 also has specific guidelines for personal data managers and processors. And ISO 27701 is claimed to have good compatibility and integration with existing standards and regulations (International Standard Organization, 2019).

2.6. ENISA Personal Data Protection Guidelines

The European Union Agency for Network and Information Security or known as ENISA, is founded in 2004 and it is intended to raise the awareness and culture of information security and cybersecurity within the European Union's society (Markopoulou et al., 2019).

ENISA released guidelines for personal data protection to help with compliance with the EU's GDPR and reduce the risk of not complying with the regulation. The guideline consists of Data Protection by Design and by Default, Data Protection Impact Assessment, Data Protection Engineering, Privacy Enhancing Technologies, and Data Breach Notification.

Data Protection guideline covers system protection design, impact assessment, implementation of enhancing technologies, and data breach notification.

Privacy by design is the first principle of the ENISA guideline, its concept is to embed privacy data protection into the client's system and processes. Integrating privacy protection into every system and process ensures that all the systems and processes are privacy concerns therefore it could prevent

privacy breaches in the future. Other than preventing breaches it also makes every process privacy concern by default (European Network and Information Security Agency, 2014).

Data Protection Impact Assessment (DPIA) is the second principle and guideline that discusses the assessment of privacy-concerned risks on processes and systems. It is one of the requirements of the GDPR to have a privacy impact assessment and to identify any risks of privacy breaches in the client's systems and processes (European Network and Information Security Agency, 2019).

Data Protection Engineering is the third concept and still considered under the ENISA's Privacy by Design guideline. It merely discusses more on the strategies and techniques of data processing activities and its strategy to comply with the GDPR (European Network and Information Security Agency, 2022).

Privacy Enhancing Technologies is the guideline for implementing technology to empower the privacy protection of the client's systems and processes. The technologies discussed in the guidelines such as encrypting, anonymization, pseudonymization, and data minimization (European Network and Information Security Agency, 2017).

EU's GDPR also requires organizations to have a data breach notification to ensure that if there are any data breaches occur within the organization that they will notice and try to minimize the effects. ENISA has already released the data breach notification guideline. It discusses how to manage an incident, coordination with other parties, notification information content, and timeframe. The ENISA is mostly considered helpful in helping organizations comply with the EU's GDPR

3. Research Methodology

In this research, there are three major steps in the proposed decision-making model. These steps consist of determining the criteria used for the selection, the weighting of the criteria, ranks the alternatives by using. These steps are supplemented with 4 subprocesses which are criteria validation, Analytical Hierarchy Process (AHP) for criteria weighting and priority, and Technique for Order of Preferences by Similarity to Ideal Solution. A detailed illustration of the method of decision-making can be seen in Fig.1.

For determining the criteria used for the selection, first by reviewing literature references. There are also some criteria that the experts recommended to be included in the selection process. The experts that are involved consist of people with different backgrounds, mostly information security, cyber security, and risk management.

The criteria gathered through various literature reviews and expert opinions are yet to be validated in relevance to the context of the research. Since most of the literature is not specifically for personal data protection framework selection, therefore the validation of the criteria gathered is needed to be objective towards the research purposes.

To validate the criteria, a questionnaire using a Likert scale from 1 to 5 is used. In which 1 is the least important and 5 is the most important. The panel of experts will determine the importance of the criteria to be considered in choosing a framework for personal data protection.

The results of the questionnaire are then processed and calculated the geometric mean of the experts' answers to each criterion. A geometric mean is used instead of an arithmetic mean since Geomean reduces the influence of a high gap of values within the data set. Therefore, it lessens any miscalculation compared to the arithmetic mean. The criteria that are through from the validation process is the criteria that its geometric mean is above 4. Therefore, we only include criteria that based on the questionnaire are determined to be "important" and not less than important.

After the criteria that are used for the selection are concluded then the process as follows continues by calculating the weight of the criteria by using AHP. The purpose of weighing the criteria is to know which criteria are the most priority and the most to be considered (Alowaigl et al., 2021; Dachyar et al., 2023; Mohamed et al., 2019). AHP is considered the method to weigh and determine the criteria priority because it involves consistency checking to ensure the opinion from experts are valid. The pairwise comparison of each criterion and sub-criteria is measured with the help of the Expert Choice application.

The weight of the criteria and sub-criteria that have been obtained is used as input for the rank and choice of framework. And since the TOPSIS method requires the expert's opinion for each alternative regarding the criteria and sub-criteria. Therefore, a questionnaire is used to help gather the expert's opinions with a different questionnaire. The questionnaire uses a Likert scale from 1 to 5 with 1 being the worst and 5 being the best. Then, the results from the questionnaire will be the input for the TOPSIS calculation to determine the rank of the frameworks.

TOPSIS is used to determine which framework is the first choice based on the weight of the criteria and expert views on the alternatives regarding the criteria (Alowaigl et al., 2021; Giovanni et al., 2022; Mohamed et al., 2019). The reason behind the use of TOPSIS is that it requires the expert's opinion not based on pairwise comparison of each other alternatives. Therefore, it eliminates the relativeness of the score of each alternative not relative to other alternatives but merely to the alternative's performance and ability itself.

When the first choice has been obtained, a sensitivity analysis is conducted to investigate furthermore on the effects of the weight of each criterion towards the final classification. This analysis will provide a better view of the strengths and weaknesses of the frameworks based on the criteria. The sensitivity analysis is conducted with the Expert Choice application.

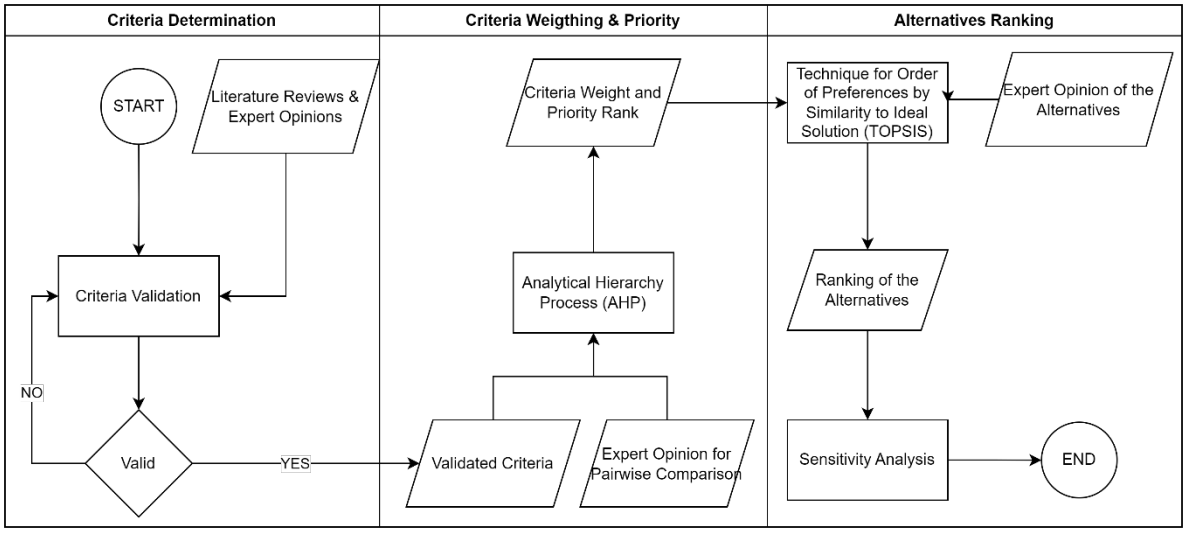

Fig.1: Overview of The Decision-Making Model

4. Results and Discussion

This research is intended to help decide and prioritize data framework alternatives for personal data protection with consideration of four main criteria which include sixteen sub-criteria for deciding the data framework intended to be used by companies in Indonesia.

The framework alternatives are selected based on how closely the frameworks adhere to the Indonesian Personal Data Protection Act. Since the Indonesian PDP Act is more likely similar to the European Union General Data Protection (GDPR) then the ENISA Personal Data Protection framework is involved because it is widely used for complying with EU's GDPR. The other alternatives are ISO 27701 and ASEAN Personal Data Protection Framework. ISO 27701 is a standard that International Standard Organization released, and it was aimed to be implemented widely without any regional or regulation restrictions. While ASEAN PDP Framework is chosen due to Indonesia is an ASEAN member and ratifies the framework in 2016.

The criteria and sub-criteria are acquired through a literature review and analysis of literature related to data protection in general. A total of four criteria with sixteen sub-criteria could be involved in this research. Other than literature analysis criteria are also included from the expert's opinion. The criteria

gathered can be seen in Table 1.

Table 1. Criteria and Sub-Criteria for Personal Data Protection Framework Selection Identification Results

Main Criteria for Selection	Sub-Criteria for Selection	Reference
Business and Economy	Adoption Costs	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Operating Costs	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Supporting Technology Costs	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Framework Reputation	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
Legal	Harmonization with Applicable General Law	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Harmonization with Applicable Sectoral Law	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
Technical	Framework Scope	(Bu et al., 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Complexity of Adoption	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Operational Complexity	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Compatibility	(ASEAN, 2016; Bu et al., 2020; Cavoukian, 2020; Olukoya, 2022)
	Flexibility	(ASEAN, 2016; Bu et al., 2020; Cavoukian, 2020; Olukoya, 2022)
	Availability of Supporting Technology	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
	Adoption Process Duration	(Carauta Ribeiro & Dias Canedo, 2020; Kilic et al., 2015; Malindzakova & Puskas, 2018)
Security	Incident Management	(ASEAN, 2016; Bu et al., 2020; Cavoukian, 2020; Olukoya, 2022)
	Control and Monitoring System	(ASEAN, 2016; Bu et al., 2020; Cavoukian, 2020; Olukoya, 2022)
	Efforts to Prevent Leakage and Misuse of Personal Data	(ASEAN, 2016; Bu et al., 2020; Cavoukian, 2020; Olukoya, 2022)

The criteria gathered from literature reviews and expert opinions are then yet to be validated. Validation is needed to ensure that those criteria are fit to be included in the selection process for the personal data protection framework.

Data from Table 2 explains that there are a total of four criteria and fifteen sub-criteria that are accepted and eligible for the framework selection assessment.

The expert's opinion and scoring of the appropriateness of the criteria to be involved in the personal data protection framework selection are gathered using a questionnaire with Likert scale measurement

from 1 to 5 and it is processed with geometric mean to obtain the average score from the panel of expert's opinion. The acceptance threshold is set at 4 therefore sub-criteria that are below 4.00 are rejected.

Of sixteen criteria there is only one criterion that is not accepted based on the expert's opinion which is framework reputation that is considered not an important matter to be involved in selecting a framework for personal data protection because the reputation of the framework exceeds outside of Indonesia and may differ in Indonesia.

Table 2. Acceptance of Criteria and Sub-Criteria for Personal Data Protection Framework Selection

Main Criteria for Selection	Sub-Criteria for Selection	Weighted Geomean	Acceptance
Business and Economy	Adoption Costs	4,18	Yes
	Operating Costs	4,12	Yes
	Supporting Technology Costs	4,31	Yes
	Framework Reputation	1,31	No
Legal	Harmonization with Applicable General Law	5,00	Yes
	Harmonization with Applicable Sectoral Law	5,00	Yes
Technical	Framework Scope	4,57	Yes
	Complexity of Adoption	4,37	Yes
	Operational Complexity	4,78	Yes
	Compatibility	4,12	Yes
	Flexibility	4,37	Yes
	Availability of Supporting Technology	5,00	Yes
	Adoption Process Duration	4,00	Yes
Security	Incident Management	4,57	Yes
	Control and Monitoring System	4,57	Yes
	Efforts to Prevent Leakage and Misuse of Personal Data	4,57	Yes

The results shown in Table 3 describe the weight and rank for each of the main criteria framework selection. While the data in Table 4 describes the weight and rank of the sub-criteria for framework selection.

Legal criteria are considered as the top priority criteria with 0.61 followed by Business & Economy with 0.19 and then Security with 0.15 and last Technical with 0.05.

Then on the sub-criteria, the top rank is Harmonization with Applicable General Law and the last is Flexibility. This shows that complying with the rules and regulations plays an integral part in deciding which framework will be chosen. Since if a company fails to comply with the Indonesian regulation there will be sanctions enacted such as administrative sanctions, fines, and criminal sanctions which may lead up to business permission revoked.

After Legal the next criteria are Business & Economy, Security and Technical. Based on the results, business & economy is above security. This can be caused by companies' need also to plan their financial expenses regarding the adoption, operation, and technology costs while the security will automatically enhance itself by complying with the requirements of the regulation. Therefore, the security factor is still considered important, however, it can be covered by legal factors. This can be seen by the relatively small aggregate between the business & economy weight scored 0.19 compared

to the security weight scored 0.15.

Technical is considered less important than the other three criteria since the purpose is to comply with the rules and regulations by improving personal data protection. The difficulties with the technical factors that the company may face will have to adapt. Since the purpose is to comply with the regulations and enhance the personal data protection system.

Table 3. Main Criteria Weight and Rank

Main Criteria for Selection	Criteria Weight	Rank
Legal	0.61	1
Business and Economy	0.19	2
Security	0.15	3
Technical	0.05	4

Table 4. Sub-Criteria Weight and Rank

Sub-Criteria	Sub-Criteria Local Weight	Global Weight	Rank
Harmonization with Applicable General Law	0,74	0,45	1
Harmonization with Applicable Sectoral Law	0,26	0,16	2
Adoption Costs	0,58	0,11	3
Incident Management	0,53	0,08	4
Supporting Technology Costs	0,29	0,06	5
Efforts to Prevent Leakage and Misuse of Personal Data	0,32	0,05	6
Operating Costs	0,13	0,03	7
Control and Monitoring System	0,15	0,02	8
Framework Scope	0,34	0,02	9
Complexity of Adoption	0,17	0,01	10
Compatibility	0,15	0,01	11
Operational Complexity	0,11	0,01	12
Availability of Supporting Technology	0,1	0,01	13
Adoption Process Duration	0,1	0,01	14
Flexibility	0,03	0,01	15

After the weight of the criteria has been calculated then the next step is to determine the first choice of the alternatives for the personal data protection framework. The results shown in Table 5 are the rank of the framework alternatives considered in this research.

The expert's opinion on the alternatives with the consideration of the criteria and sub-criteria weight is calculated with the TOPSIS approach.

The score indicates that ISO 27701:2019 is the first choice compared to ENISA and ASEAN. The ISO 27701:2019 is considered the most harmonized towards the Indonesian PDP Act and the easiest to integrate with the existing system since it is part of the ISO standard series and the extension of ISO 27001:2019 therefore, many companies in Indonesia which already familiar with the framework will find it easier to implement. While the ENISA is thought to be more complex to implement since it promotes Privacy by Design which needed to be embedded in every system and it is much harder to integrate into an existing system (European Network and Information Security Agency, 2014). Therefore, it is easier to implement in a new system. While the ASEAN is lacking specific details on the guidelines and how to implement them.

Table 5. Framework for Personal Data Protection Alternative Rank

Alternatives	Score	Rank
ENISA PDP Framework	0,65	2
ISO 27701: 2019	0,72	1
ASEAN PDP Framework	0,10	3

Although the most ideal framework has been obtained, not all companies or organizations are suitable for implementing it. Each has different characteristics and goals so there may be other options that are more suitable for a particular company. To examine the influence of variables, sensitivity analysis is conducted. By changing the weight of the criteria to see the effect of the weight of a particular criterion on the ranking of alternative frameworks. Sensitivity analysis is performed using the Expert Choice application.

Fig. 2 is the ranking result of the equalization of the weight of each criterion. By being equalized, the ranking results are not affected or have no change, so if all criteria have a balanced weight, ISO 27701: 2019 remains the first choice, followed by ENISA PDP in second position and ASEAN PDP in third position.

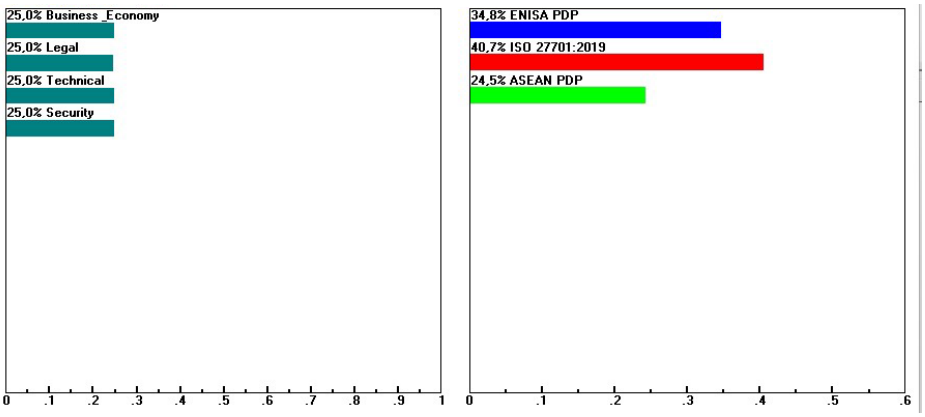

Fig. 2: Sensitivity Analysis Equal Weight for Each Criterion

Then in Fig 3 is the ranking result of the prioritization of business and economic weights. Increasing the weight of business and economic criteria to 0.94, ISO 27701: 2019 remains the first choice but in the second and third choices there is a change in position.

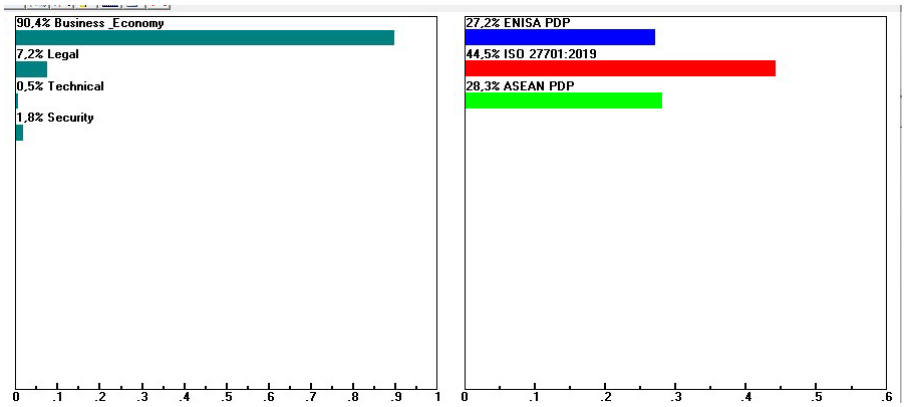

Fig.3: Sensitivity Analysis of Increasing the Business & Economy Criteria Weight

In Fig. 4, the technical criteria are prioritized to 0.95. This has no impact on the first rank still held by ISO 27701: 2019. However, it is the same with the increase in the weight of business and economic criteria where the second position is filled by ASEAN PDP and the third position by ENISA PDP.

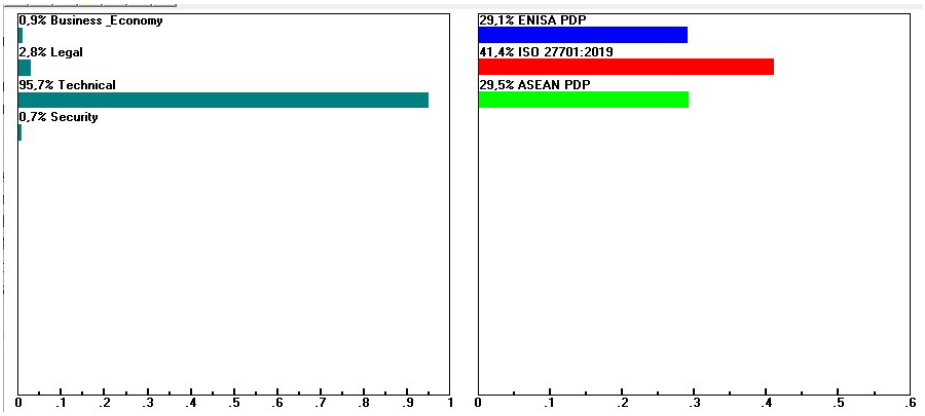

Fig. 4. Sensitivity Analysis of Increasing the Technical Criteria Weight

In Fig 5, the enhanced criteria are security criteria. With the weighting being 0.5 significant changes to the framework rating can be seen. The first choice became ENISA PDP then the second position became ISO 27701: 2019 and the third was ASEAN PDP.

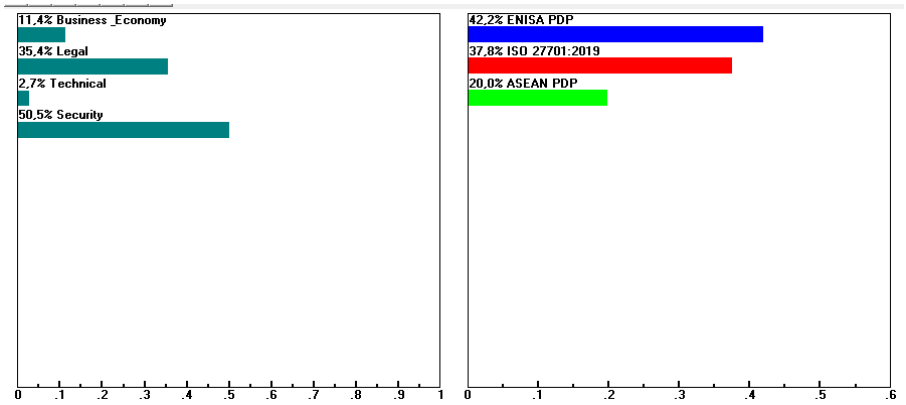

Fig. 5. Sensitivity Analysis of Increasing the Security Criteria Weight

The sensitivity analysis results indicate that the adjustment of the criteria weights affects the rank of the alternatives of the framework. With four scenarios of sensitivity analysis conducted, the results show that ISO 27701:2019 remains a strong candidate and is defeated by ENISA PDP Guideline only when the security criteria are increased to become the priority. It also gives another perspective for companies that have constraints on the criteria and may have different priorities than most companies. For example, if a company gives more attention to the security criteria, therefore, they will tend to choose ENISA PDP guideline over ISO 27701:2019.

Based on the findings above, ISO 27701:2019 remains the best framework to be implemented overall. However, in terms of security, it lacks compared to ENISA PDP. This would then explain that ENISA PDP has a strong point on security factors compared to ISO 27701:2019 and ASEAN PDP. The complexity and comprehensive guidelines of ENISA PDP play a vital role in their strength in the security factor.

The ASEAN PDP framework may be considered the weakest among the others. This can be caused by the simplicity of the framework itself and does not have a comprehensive on how to implement the framework. However, based on the sensitivity analysis above that when the factors of business & economy, and technical are increased it is considered better than ENISA PDP even though still lacks ISO 27701:2019. But this shows that it has a strong point compared to the ENISA PDP on the technical and business & economic factors. And ASEAN PDP is the only framework that is ratified and signed by all the ministers of telecommunication in ASEAN including Indonesia. Therefore, ASEAN PDP is

the only framework that the Indonesian minister of telecommunication approves. Even though it is ratified in 2016 and the Indonesian PDP Act is passed in 2022.

5. Conclusion

In this research, our primary objective was to identify the most suitable framework alternative for personal data protection, specifically tailored to companies in Indonesia. Based on our comprehensive findings, we conclude that ISO 27701:2019 emerges as the optimal first choice for businesses seeking to bolster their personal data protection measures and adhere to the requirements outlined in the Indonesian Personal Data Protection Act.

The evaluation of four key criteria, encompassing fifteen sub-criteria, guided our decision-making process. Among these, the Legal criteria emerged as the most crucial factor, emphasizing the paramount importance of compliance with rules and regulations. The Business & Economy criteria followed closely, highlighting the significance of considering the costs associated with framework adoption and operation. Moreover, the Security criteria ranked third, with the understanding that adhering to regulations inherently reinforces and strengthens data security. Lastly, the technical criteria were deemed less influential due to the necessity of adapting to technical challenges in line with compliance requirements.

The weight assigned to each criterion significantly impacted the rankings of the frameworks, providing a unique perspective on selecting the most suitable alternative. While ISO 27701:2019 excelled in Business & Economy, Legal, and technical criteria, the framework with a distinct advantage in the Security factor was ENISA PDP.

Ultimately, businesses in Indonesia stand to benefit from the adoption of ISO 27701:2019, leveraging its advantages in key criteria and ensuring robust personal data protection measures. However, organizations must also consider specific security needs and weigh the benefits of ENISA PDP in that regard.

We believe that the insights gained from this study contribute to the informed decision-making process for companies seeking to enhance their personal data protection efforts. The framework selection process is now fortified with valuable information to navigate the complex landscape of personal data protection, ensuring compliance with regulations, and safeguarding sensitive information effectively. As the digital landscape evolves, continuous evaluation and adaptation of data protection frameworks will remain essential for companies to uphold their commitment to data privacy and security.

This research could be further improved by also involving business stakeholders as the panel of experts in determining the criteria and opinions on each of the alternatives. Therefore, an insight from business stakeholders may provide a different perspective towards the results.

References

Alowaigl, A., A. Al-Shqeerat, K. H., & Hadwan, M. (2021). A multi-criteria assessment of decision support systems in educational environments. *Indonesian Journal of Electrical Engineering and Computer Science*, *22*(2), 985. https://doi.org/10.11591/ijeecs.v22.i2.pp985-996

Altarawneh, H., & Tarawneh, M. M. (2023). Business Intelligence and Information System Management: A Conceptual View. *Journal of System and Management Sciences*, *13*(2), 31–44. https://doi.org/10.33168/JSMS.2023.0203

ASEAN. (2016). *Framework on Personal Data Protection*. 1–6.

Badan Sandi dan Siber Negara, D. O. K. S. (2022). *Laporan Tahunan 2021 Monitoring Keamanan Siber*. Badan Sandi dan Siber Negara Republik Indonesia.

Bu, F., Wang, N., Jiang, B., & Liang, H. (2020). " Privacy by Design " implementation : Information

system engineers ' perspective. *International Journal of Information Management*, *53*(March), 102124. https://doi.org/10.1016/j.ijinfomgt.2020.102124

Carauta Ribeiro, R., & Dias Canedo, E. (2020). Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. *ACM International Conference Proceeding Series*, 175–184. https://doi.org/10.1145/3396956.3398252

Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. *IEEE Consumer Electronics Magazine*, *9*(2), 78–82. https://doi.org/10.1109/MCE.2019.2953739

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Cui, J., & Lim, C. K. (2022). The Privacy Concerns' Influences on Bike-Sharing Consumers' Behavior. *Journal of System and Management Sciences*, *12*(2), 258–272. https://doi.org/10.33168/JSMS.2022.0212

Dachyar, M., Salman, M., & Nurcahyo, R. (2023). *Strategies to Improve the Education and Research Scholarship Program at the Universities*. *12*(1), 389–395. https://doi.org/10.18421/TEM121

Dharmawan, N. K. S., Kasih, D. P. D., & Stiawan, D. (2019). Personal data protection and liability of internet service provider: A comparative approach. *International Journal of Electrical and Computer Engineering*, *9*(4), 3175–3184. https://doi.org/10.11591/ijece.v9i4.pp3175-3184

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO / IEC27001 : 2013 and ISO / IEC27002 : 2013 to GDPR compliance controls. *Information & Computer Security*. https://doi.org/10.1108/ICS-01-2020-0004

European Network and Information Security Agency. (2014). *Privacy and Data Protection by Design – from policy to engineering* (Issue December). https://doi.org/10.2824/38623

European Network and Information Security Agency. (2017). *A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment*. *December*.

European Network and Information Security Agency. (2019). *ONLINE PLATFORM FOR SECURITY OF PERSONAL* (Issue December). https://doi.org/10.2824/3000

European Network and Information Security Agency. (2022). *DATA PROTECTION ENGINEERING* (Issue January).

Fadhil, M. I. (2021). *Control Design of Information Security Related to Privacy in The Smart SIM Business Process*. 66–72.

Fal', O. M. (2021). Documentation in the ISO/IEC 27701 Standard. *Cybernetics and Systems Analysis*, *57*(5), 796–802. https://doi.org/10.1007/s10559-021-00404-3

Giovanni, G., Gita, R., Dachyar, M., & Pratama, N. R. (2022). *Ideal Location Selection for Global Excavator Manufacturing Facilities in North America*. *July 2021*, 310–319.

Grishaeva, S. A. (2021). *Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701 : 2019*. 2021–2023.

Guseva, O. Y., Kazarova, I. O., Dumanska, I. Y., Gorodetskyy, M. A., Melnichuk, L. V, & Saienko, V. H. (2022). Personal Data Protection Policy Impact on the Company Development. *WSEAS Transactions on Environment and Development*, *18*, 232–246. https://doi.org/10.37394/232015.2022.18.25

IBM Security. (2021). *Cost of a Data Breach Report*.

Undang-undang Perlindungan Data Pribadi, 1 (2022) (testimony of Indonesia).

International Standard Organization. (2019). *INTERNATIONAL STANDARD ISO / IEC Security techniques — Extension to* (Vol. 2019).

Kementerian Komunikasi dan Informatika (Kominfo). (2021). *Laporan Kinerja Kementerian Komunikasi dan Informatika 2021* (Issue 9).

Kilic, H. S., Zaim, S., & Delen, D. (2015). Selecting "the best" ERP system for SMEs using a combination of ANP and PROMETHEE methods. *Expert Systems with Applications*, *42*(5), 2343–2352. https://doi.org/10.1016/j.eswa.2014.10.034

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*(April 2021), 106868. https://doi.org/10.1016/j.infsof.2022.106868

Loishyn, A. A., Hohoniants, S., Tkach, M. Y., Tyshchenko, M. H., Tarasenko, N. M., & Kyvliuk, V. S. (2021). *Development of the Concept of Cybersecurity of the Organization*. *10*(3), 1447–1453. https://doi.org/10.18421/TEM103

Madyatmadja, E. D., Karsen, M., Yuri, A., Sijabat, D. P., Wiratama, G. R., Santika, R., & Pristinella, D. (2023). The Effectiveness of Security and Customer Convenience in the Use of E-Commerce. *Journal of System and Management Sciences*, *13*(3), 193–204. https://doi.org/10.33168/JSMS.2023.0313

Malindzakova, M., & Puskas, D. (2018). The AHP method implementation for ERP software selection with regard to the data protection criteria. *TEM Journal*, *7*(3), 607–611. https://doi.org/10.18421/TEM73-17

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, *35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Mohamed, E. M., Bouikhalene, B., Ouatik, F., & Safi, S. (2019). AHP and TOPSIS methods applied in the field of scientific research. *Indonesian Journal of Electrical Engineering and Computer Science*, *14*(3), 1382–1390. https://doi.org/10.11591/ijeecs.v14.i3.pp1382-1390

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a Global Data Breach Database and the Challenges Encountered. *Journal of Data and Information Quality*, *13*(1), 1–33. https://doi.org/10.1145/3439873

Noor, M. U. (2020). Indonesian millennial awareness to privacy and personal data protection on the internet. *DESIDOC Journal of Library and Information Technology*, *40*(2), 431–436. https://doi.org/10.14429/djlit.40.02.14969

Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers and Security*, *117*, 102697. https://doi.org/10.1016/j.cose.2022.102697

Petrov, P., Kuyumdzhiev, I., Malkawi, R., Dimitrov, G., & Jordanov, J. (2022). *Digitalization of Educational Services with Regard to Policy for Information Security*. *11*(3), 1093–1102. https://doi.org/10.18421/TEM113

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303. https://doi.org/10.3934/MBE.2020286

Shahim, A. (2021). Security of the digital transformation. *Computers and Security*, *108*, 102345. https://doi.org/10.1016/j.cose.2021.102345

Sudarwanto, A. S., & Kharisma, D. B. B. (2021). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-09-2021-0193

Surtiwa, S. S., Gultom, C. J., Law, F., Indonesia, U., & Barat, J. (2021). *Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer to Peer Lending ASEAN for Data Protection : 558*(Aprish 2019), 720–726.

Tampubolon, T., & Ramadhan, R. (2020). ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara. *Padjadjaran Journal of International Relations*, *1*(3), 270. https://doi.org/10.24198/padjir.v1i3.26197

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., & Gallego-Nicasio Crespo, B. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information and Computer Security*, *28*(4), 531–553. https://doi.org/10.1108/ICS-01-2020-0002