

## Awareness of Personal Data Protection Law in concern to literacy

Annisa Fajriyati Sadeli<sup>1\*</sup>, Indira Irawati<sup>2</sup>

<sup>1,2</sup>Departement of Library and Information Sciences, Universitas Indonesia  
Jl. Margonda Raya, Pondok Cina, Beji, Depok, Jawa Barat 16424  
)\*Corresponding Author, Email: annisa.fajriyati@ui.ac.id

Received: June 2023; Accepted: December 2023; Published: December 2023

### Abstract

Understanding privacy literacy can help everyone treat their personal data shared on online platforms. Data protection starts from the idea that individuals have the right to information about themselves. There must be efforts to prevent misuse; hence, it makes digital literacy important. This research aimed to measure students' understanding of the importance of protecting personal data in the PDP Law based on the categories of knowledge, attitudes, and behavior. The research used quantitative methods with an analytical survey approach. Data analysis techniques used the Analytical Hierarchy Process (AHP). The population was 75 undergraduate and postgraduate students in West Java. The final score showed the number 81. Research results showed that the knowledge dimension scored 82, or a good level. It explained that most respondents understood data privacy protection laws. The attitude dimension had a score of 83, classified as good. Respondents were expected to stay informed about information protection and data privacy. The behavioral dimension was lower than the other dimensions, namely 77 or classified as an average level. In conclusion, the awareness level of the Data Privacy Protection Law based on the areas and dimensions that have been taken into account is at a good level, although it still needs improvement in terms of habits or behavior.

Keywords: Digital literacy; Personal Data Protection Law; Privacy data

### *Kesadaran terhadap Undang-Undang Perlindungan Data Pribadi dalam fokus literasi*

#### Abstrak

Pentingnya pemahaman terkait literasi privasi dapat membantu setiap orang dalam memperlakukan data pribadi mereka yang dibagikan di berbagai platform online. Perlindungan data dimulai dari gagasan bahwa individu memiliki hak atas informasi tentang diri mereka, dan harus ada upaya pencegahan terjadinya penyalahgunaan, hal inilah yang menyebabkan literasi digital menjadi penting. Penelitian ini bertujuan untuk mengukur pemahaman mahasiswa tentang pentingnya perlindungan data pribadi dalam UU PDP berdasarkan kategori pengetahuan, sikap dan perilaku melalui survei. Penelitian menggunakan metode kuantitatif dengan pendekatan survei analitik dan teknik analisis data menggunakan Analytical Hierarchy Process (AHP). Populasi yang digunakan adalah 75 mahasiswa sarjana dan pascasarjana di Jawa Barat. Skor akhir menunjukkan angka 81. Hasil penelitian menunjukkan dimensi pengetahuan mendapat skor 82 atau tingkat Baik. Ini menjelaskan bahwa sebagian besar responden memahami hukum perlindungan privasi data. Sedangkan pada dimensi sikap memiliki nilai 83 atau tergolong baik. Responden diharapkan untuk tetap mengetahui semua yang mereka pikirkan tentang informasi dan perlindungan privasi data. Sedangkan dimensi perilaku lebih rendah dari dimensi lainnya yaitu 77 atau tergolong tingkat rata-rata. Kesimpulannya, tingkat kesadaran UU Perlindungan Privasi Data berdasarkan area dan dimensi yang telah diperhitungkan tersebut berada pada tingkat yang baik meskipun masih perlu ada peningkatan di bagian pembiasaan atau perilaku.

Kata Kunci: Data pribadi; Literasi digital; Undang-Undang Perlindungan Data Pribadi

## INTRODUCTION

Understanding privacy literacy crosses with digital literacy because both are often combined and seen as equal. Regardless, current definitions of privacy literacy and digital literacy establish their differences. In digital literacy, to actively use new technologies as they emerge, each person must develop the necessary skills (Reddy, Sharma, & Chaudhary, 2020). Meanwhile, privacy literacy is a mental process or cognitive experience that arises when information is shared (Wissinger, 2017). The definition of privacy literacy focuses on how a person understands the responsibilities and risks that arise from sharing information online.

In contrast, digital literacy focuses on how a person uses task-based information in a digital environment. Based on this definition, privacy literacy is more aligned with critical thinking. Therefore, understanding privacy literacy can assist everyone in treating their personal data shared on various online platforms.

A serious threat may occur if there is still a lack of understanding of privacy literacy in Indonesia. For example, as much as 26 million customer data was allegedly leaked and traded on BreachForums by Bjorka in August 2022. Then, as many as 1.3 billion SIM cards or SIM card registration data were also allegedly leaked and sold last September 2022, and Bjorka admitted to having obtained 87GB of data from the Ministry of Communication and Information, where the leaked data was in the form of NIK, telephone number, provider name, and registration date (CNN Indonesia, 2022). These are some of the many cases that have occurred in Indonesia, which, of course, must be avoided due to the dissemination of personal data in the

online environment. It shows the importance of public awareness that personal data is important to protect.

In the financial industry, Soemitra and Hasan (2022) claimed that two factors contribute to personal data leaks: 1) consumer factors and 2) financial service business actors. Due to consumer behavior in completing online loan transactions and disclosing personal information such as identity numbers, cellphone numbers, and credit and debit card numbers, there is a factor of consumer data leakage. In this case, the human resource factor that can be prioritized in society is each person's literacy ability. It is crucial to improve the fundamental digital capabilities and the abilities required to comprehend and utilize internet content (Peng & Yu, 2022).

On the other hand, the issue of personal data currently has official government regulations through Law Number 27 of 2022 concerning the Protection of Personal Data, also known as the Personal Data Protection (PDP) Law. Because of this, the public needs to understand how to control all information in digital form, especially to control the circulation of personal data when using social media or e-commerce and protect their data. Data protection laws are a critical component of a legal compliance framework whose primary goal is to strike the right balance between privacy and freedom of information (Oppenheim, Muir, & Korn, 2020). The General Data Protection Regulation (GDPR) is the first regulation concerning data protection in the European Union (EU) that aims to restore public confidence in the ethical use of their data to advance the digital economy inside the member of EU (Voigt & von dem Bussche, 2017). So, the GDPR can be a reference in comparing or even

adopting the essential points needed in the PDP Law implemented in Indonesia.

Many developing countries still need to gain more awareness of data protection. In Southeast Asia, the recorded countries already have laws related to data protection including Thailand, Singapore, Malaysia, and the Philippines. However, Indonesia is a country that seems late in having and enforcing this law compared to other countries. Several regulations regarding personal data protection in Indonesia are spread across certain sectors, such as banking, health, and population.

According to PDP Law, privacy data is data about individuals who are identified or can be identified separately or combined with other information, either directly or indirectly, through electronic or non-electronic systems. Meanwhile, protecting data privacy is the overall effort to protect privacy data in a series of privacy data processing to guarantee the constitutional rights of privacy data subjects (Presiden Republik Indonesia, 2022). According to GDPR, personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (European Parliament, 2016). The definitions of data privacy are similar, especially considering the critical fact that data privacy may allow for identifying a person through information gathered in this manner.

Law number 27 of 2022 on Personal Data Protection (PDP Law) concerning the

protection of privacy data has approximately five main objectives: first, protecting and guaranteeing the fundamental rights of citizens to the protection of privacy data and second, raising public awareness of the importance of protecting privacy data. Third, encourage the growth of the digital economy and industry information and communication technology. Fourth, support the competitiveness of the domestic industry; fifth, ensuring that the public obtains services from corporations, public bodies, international organizations, governments, and other public organizations.

In terms of the scope of the PDP Law, this applies to many parties, namely individuals, corporations, public bodies, and international organizations both within the jurisdiction of the Republic of Indonesia and those outside the jurisdiction which have legal consequences or affect the interests of the state. However, the PDP Law does not apply to the processing of privacy data carried out by individuals in privacy or household activities, for example, husbands and wives who store or process each other's data in a family; this is wholly the responsibility of everyone.

According to Almasyhari, Sari, and Sukesti (2022), various privacy data can be about a person's health or medical records, genetic data, biometric data, sexual life, a person's political views, crime, child data, privacy financial data or historical loans and other data by statutory regulations. In addition, data such as employees and addresses are examples of privacy data that we often share with third parties. Of course, this is very risky if the third party who processes our data is not responsible and if this data can be misused.

Almasyhari et al. (2022) conducted a study entitled "Information Security Awareness of Students on Academic Information Systems Using Google Approach." The dimensions tested are related to knowledge, behavior, and attitude. In addition, it uses the CIA concept, namely Confidentiality, Integrity, and Availability of classified information. The results of the study show that the level of awareness in each of these dimensions is at 75%, which means that the level of awareness of students regarding information security awareness is at a moderate level.

Batmetan, Kariso, Moningkey, and Tumembow (2018) conducted another study on the same topic, which discussed the level of privacy awareness on information security issues. This survey was conducted on PTIK students from Unima. The conclusion is that most students know how vital privacy security is in public services and its risks. However, many students still feel they do not care about their privacy security even though they are aware of the risks that will occur. Students are one of the most important communities to have a good level of digital literacy. Göldağ (2021) states that students' awareness of digital data security and their digital literacy levels are positively and significantly correlated. Students are becoming more mindful of digital data security as their levels of digital literacy rise (Göldağ, 2021). For this reason, there is a need for broader socialization and the introduction of information security and privacy policies among students and the public.

Priliasari (2019) researched aims to examine the legal protection of privacy data from borrowers of online loan application services. The conclusion is that

the Indonesian state has provided consumer protection as stipulated in the law, but more is needed to protect consumers. It is hoped that the government will immediately provide privacy data protection to the public so that it is not misused. This research is the basis that the wider community must use their privacy data wisely. Besides that, to feel more protected by law, this privacy data protection law will be enacted in 2022. Once enacted, awareness is needed to implement these regulations. In Merriam-Webster's dictionary, awareness is the quality or state of being aware: knowledge and understanding that something is happening or exists. According to the Cambridge Dictionary, one is aware now that something exists or has knowledge or experience of a particular thing. From the definition itself, we can see why awareness can affect the implementation of a regulation because it will have an impact on what someone does after they understand what to do.

In the study of information science and libraries, we can see this point from two perspectives. The first is as a subject of privacy data, where members of the public must be able to prevent adverse outcomes associated with privacy data leaks communicated to third parties. This results in a subject of privacy data capacity to be more than just understanding but also conceptualizations of the fundamentally political nature of the larger data assemblage or, more succinctly, personal data literacy. Personal data literacy should work to increase students' understanding of the social, political, economic, and cultural consequences of data and their ability to critically reflect on these processes on the internet (Pangrazio & Selwyn, 2019).

Second, from the point of view of a library institution, which in this case can be called a controller of privacy data, librarians must also be aware that we must also protect users' privacy data. Generally, the user's privacy data includes names, addresses, affiliates, telephone numbers, dates of birth, and other data usually used to register new library members. These all relate to the area of information policy in the field of library and information science. According to Oppenheim et al. (2020), ensuring legal compliance and accountability is the primary goal of information policy, and current processes need to reflect this.

Academically, it is expected that this research will contribute to a deeper understanding of a reference for developing sub-fields of information policy studies and literacy studies related to security awareness, information privacy, and privacy literacy. However, in this study, the limitations are only related to the point of view of privacy data subjects so that we can be aware of the types and how we manage privacy data.

Previous research discusses company information security awareness and related company information, so the research subjects are employees. Then related legal research usually uses a normative legal approach and is seen from the point of view of the content quality of the law itself so that legal experts generally carry out research. Meanwhile, this study combines the two: measuring awareness of the PDP Law through an information security theory approach. Previous research discusses company information security awareness and related company information, so the research subjects are employees. Then, related legal research usually uses a normative legal approach

and is seen from the point of view of the content quality of the law itself so that legal experts generally carry out research.

Meanwhile, this study combined the two: measuring awareness of the PDP Law through an information security theory approach, with the respondents being West Java students. Based on this explanation, the research question is the extent to which students understand the contents of the PDP Law based on the categories of knowledge, attitudes, and behavior. Through a survey, this research aimed to measure students' understanding of the importance of protecting personal data in the PDP Law based on the categories of knowledge, attitudes, and behavior.

## RESEARCH METHODS

The study used the quantitative method with an analytic survey approach, namely collecting data from all or part of the population to assess the relative occurrence, distribution, and interrelationships of variables that occurred naturally. We choose this approach since the goal of the study was to characterize the traits of the population under research, calculate the population's proportion, and generate precise forecasts, particularly with student knowledge of private data protection.

The operational variables in this study consisted of three dimensions derived from Krueger's capital. Krueger's approach is a measurement model based on psychological theory (Kruger & Kearney, 2006). According to Kruger and Kearney (2006), a person's tendency to do something profitable for him will depend on three measurable components: first is knowledge, namely everything that someone knows about the security of privacy information;

second is attitude, namely everything that someone thinks about the security of privacy information, and the third is behavior, namely what is done by someone related to the security of privacy information (Nurbojatmiko, Firmansyah, Aini, Saehudin, & Amsariah, 2020). This model is identical to the information security awareness model, which is often used to measure information security awareness in a company toward its employees. However, in this study, the Kruger model would also be used to measure how aware people were regarding protecting their privacy data, so a slight adaptation was made by linking questions to the questionnaire with the contents of the privacy data protection law. The first derivative of this variable was knowledge, attitude, and behavior. Meanwhile, for each of these dimensions, several essential areas of UU-PDP would be measured, namely Types of Privacy Data, Rights of Privacy Data Subjects, Processing of Privacy Data, and Principles of Privacy Data Protection.

The population was undergraduate and postgraduate students in Indonesia. The sampling technique was non-probability sampling, especially accidental sampling, or convenience sampling. In using accidental sampling techniques, the researcher only selected existing cases until

the sample reached the desired size and was determined. The researcher selected anyone who happened to be found as a research sample and willing to answer the survey questionnaire. The researcher created the research instrument consisting of 30 questions using Indonesian for each variable and distributed them via Google Forms to make it easier for respondents to answer the questions. The survey was conducted for one month, from April 1, 2023, to April 30, 2023. Within the target population of the students, 75 individuals met the inclusion criteria, and they all consented to participate in the study.

Data analysis consisted of several stages. We calculated each respondent's score based on the instrument's answer. We give 10 for "True" answers, 5 for "Don't know" answers, and 0 for "False" answers. Then, we weighed dimensions and focus areas using the Analytical Hierarchy Process (AHP). This component provides a subjective assessment of the elements based on the professional judgment and opinion of management through comparisons of pairs. Each dimension will have its weight, which is used in the calculation of awareness or awareness later. The distribution of weights for dimensions and questions for focus areas are described in Table 1.

Table 1  
Dimension of Weights

Dimension	Percentage
Knowledge	30%
Attitude	20%
Behavior	50%

Source: Kruger and Kearney, 2006

Table 2 displays four focus areas: Types of privacy data, Rights of privacy data subjects, processing of privacy data, and principles of privacy data protection.

These four focus areas were taken based on the urgency of the main points, which were the most important things for knowing the contents of the PDP Law.

Table 2  
Focus Area

Focus Area	No. Question
Type of Personal Data	1
Rights of Personal Data Subjects	2,3,4,5
Processing of Personal Data	6
Principles of Personal Data Protection	7,8,9,10

Source: Researcher, 2023

The level of awareness is explained by the following awareness scale, which is

defined in Table 3 based on management's perception of awareness performance.

Table 3  
Scales

Awareness	Measurement (%)
Good	80-100
Average	60-79
Poor	59 and less

Source: Kruger and Kearney, 2006

## RESULTS AND DISCUSSION

Table 4 shows an overview of the respondent profiles. Respondents consisted of twenty-seven males and forty-eight females. Most respondents are postgraduate students, 60 percent. Meanwhile, graduate students are 40

percent. This was because the convenience sampling was carried out in an environment close to the researchers, where many were postgraduate students. The most age is in the range of 17-25 years, namely as much as 52 percent.

Table 4  
Respondent Data

Profile Respondents	Freq	%	
Gender	Male	27	36%
	Female	48	64%
Age	17-25	39	52%
	26-35	28	37.30%
	36-45	8	10.70%
Occupation	PNS	19	25.30%
	Karyawan Swasta	10	13.30%
	Wiraswasta	0	0%
	Mahasiswa	45	60%
Education (Ongoing)	Other	1	1.30%
	Sarjana	30	40%
	Pascasarjana	45	60%

Source: Data processing result, 2023

Next is the calculation of student awareness scores, which are shown in Table 5. The question with the lowest score is number 30; in the behavior dimension

related to a legal contract or document ownership as evidence of privacy data processing documentation, the value obtained is 6.6. Meanwhile, the question

with the highest score is number 7; on the knowledge dimension related to the principle of processing privacy data, there must be valid consent from the subject of privacy data, and the value obtained is 9.3. So, the average student already knows

how an agreement between a privacy data subject and a privacy data processor should be carried out, but still needs to document a valid contract or agreement with a third party that processes privacy data.

Table 5  
The Measurement Result

Dimension	Question	Answer	Avg
Knowledge	1. Types of Personal Data according to the PDP Law consist of Specific and General Personal Data	True, False,	7.7
	2. The subject of Personal Data has the right to receive information regarding the purposes for which Personal Data is used	Do not know	9.2
	3. The subject of Personal Data has the right to gain access to and obtain a copy of Personal Data about themselves by statutory provisions		8.3
	4. The subject of Personal Data has the right to withdraw consent to processing Personal Data about them that has been given to the Personal Data Controller		8.4
	5. The subject of Personal Data has the right to delay or limit the processing of Personal Data for Personal Data processing		8.6
	6. Processing of personal data includes activities of collection, processing, storage, updating, dissemination/display, and destruction		7.8
	7. In connection with the principles of processing personal data by other parties, there must be valid consent from the Personal Data Subject.		9.3
	8. Processing of Personal Data is carried out by protecting the security of Personal Data		9
	9. Processing of Personal Data is carried out by notifying the purposes and processing activities, as well as failures to protect Personal Data		8.3
	10. Processing of Personal Data is carried out responsibly and can be clearly proven		8.8
Attitude	1. I am aware that the types of personal data, according to the PDP Law, are divided into Specific Data and General Data.	True, False,	7.7
	2. I am aware that the types of personal data, according to the PDP Law, are divided into Specific Data and General Data.	Do not Know	9.1
	3. I am aware that as the owner of personal data, I have the right to access and obtain a copy of Personal Data about me		8.8
	4. I am aware that I can withdraw consent to the processing of Personal Data about me that has been given to the Personal Data Controller		7.8
	5. I am aware that I can delay or limit the processing of Personal Data in proportion to the purposes of processing the Personal Data.		8.6

	6. I know that personal data processing includes collection, processing, storage, updating, dissemination/display, and destruction		8.2
	7. I know that I must legally consent to the Personal Data I share with other parties		9.2
	8. I am aware that when collecting personal data, I must know its security so that data leaks do not occur		9.2
	9. I am aware that I must know the purposes and activities of Personal Data processing and be notified if there is a failure to protect Personal Data		9
	10. I am aware that some contracts or documents must be held as proof of documentation of the processing of Personal Data		8.4
Behavior	1. I can easily distinguish which types of personal data are specific and which are general	True, False	8.4
	2. I know information about the purposes for which the personal data I collect on a platform is used		7.7
	3. I gain access to and obtain a copy of Personal Data about myself from the platforms where I collect personal data		8
	4. I withdraw the consent to the processing of Personal Data about him that has been given to the Personal Data Controller if there is any incompatibility in collecting personal data		7.3
	5. I limit the processing of personal data proportionally according to the purposes for which it is processed		6.9
	6. I understand that the processing of personal data includes collection, processing, storage, updating, dissemination/display, and destruction		7.2
	7. I legally consent to the Personal Data that I share with other parties		9.2
	8. I ensure the security of the personal data I provide so that data leaks do not occur		7.7
	9. I am aware of the purposes and activities of processing Personal Data and am notified if there is a failure to protect Personal Data		8.8
	10. I have a valid contract or document as proof of Documentation of Personal Data processing		6.6

Source: Researcher, 2023

Table 5 shows the score for each dimension, with the AHP calculation as a reference for determining the score. The final calculation yielded a result of 81. The score is between 60 and 79, which is considered an excellent level according to Kruger and Kearney's recommendations.

For the dimension, knowledge scores 82 or a good level. It explains that most respondents understand the law of protecting data privacy even though they

did not read the contents of the PDP Law. Prior research by Trepte et al. (2015) shows that the need for knowledge about individual online privacy control strategies, legal and technical aspects, as well as institutional practices provides explanations for why user behavior on the Internet appears contradictory. Internet users must acquire the skills necessary to effectively manage their personal privacy or secure their personal

data. Someone who knows the security of his data privacy will be more confident in overcoming the problems that befall him regarding the leakage of his data privacy. In the knowledge dimension, students' understanding is more about matters related to the principles of processing personal data, which require the personal data subject's consent in its management. It is demonstrated by question number 7, namely "In connection with the principles of processing personal data by other parties, there must be valid consent from the Personal Data Subject" with a score of 9.3.

Meanwhile, the dimension attitude is 83 or a good level. The respondents are expected to be aware of everything they think of personal data information and protection. The highest score is found in questions number 7 and 8, namely about the principles of processing and security of personal data, with a score of 9.2. Based on the answers to the questionnaire, findings showed that an individual's perceptions and evaluations of privacy and personal data were generally positive. It indicated that the respondents' actions were consistent with the PDP Law's provisions. According to Steininger and Rückel (2013), legal awareness is positively correlated with a lawful attitude, as attentive Internet users are more likely to identify legally critical situations, thereby reducing the likelihood of users being drawn to the Internet by false convenience and anonymity and there is a lawful mindset and engaging in lawful activity has a big benefit. One of

the differences between previous research and current research is that previous research defined the results of attitudes and behavior based on a legal compliance perspective, which then impacts the desired behavior. The research presents that aspects of behavior are measured directly using the contents of applicable laws to find facts about actual behavior, not expected behavior.

The dimension behavior is lower than the other dimension; it is 77 percent or an Average level. The highest score for this dimension is in question number 7, with a score of 9.2, namely regarding the data subject's legal consent to the data shared with third parties. It means that students not only know but have also implemented one of the principles of personal data processing by consenting to the data they share in an online environment. This dimension relates to how a person has good behavioral habits towards specific references, in this case, the PDP Law. Students already have acceptable behavior in managing information security and law of privacy data protection, but it still needs upgrading to make it a habit. Masur (2020) believes that knowledge alone is not enough to change someone's behavior unless someone can reflect and express this knowledge so that it becomes a culture in society. For example, when someone knows that Facebook collects data from its users for advertising purposes, then this knowledge is only helpful with the ability to relate this knowledge to their behavior coupled with an awareness of the risks that will occur.

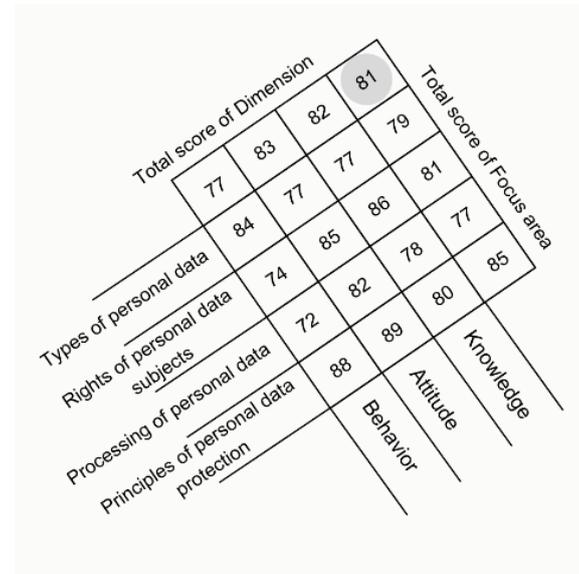


Figure 1. Awareness Map  
Source: Researcher, 2023

One claim that is difficult to refute is that information liability is a fundamental component of data protection. Policymakers have discovered in the information provided to data subjects that the tool 1) makes people aware of the relevant aspects of processing and 2) puts them in a condition to act upon that knowledge (Helberger, Borgesius, & Reyna, 2017). This method is justified because it puts the weak party—the data subject—on an even with all other participants by minimizing information asymmetry through required disclosures (Ducato, 2020).

The principle of processing privacy data in Article 16 of the PDP Law states that the processing of privacy data is carried out responsibly and can be proven clearly. The article also intends to regulate the prohibition of financial service business actors from providing data and information about consumers to third parties. So, when there is a leak of privacy data and a person's awareness is good enough about the PDP Law, he can make legal demands or consult with the authorities. To operate in accordance with

the law, students must read, comprehend, and analyze legal materials. This is a critical component in shaping an individual's perspective on lawful activity. Then, students can influence other people to spread awareness about how important the contents of the PDP Law are to be known and implemented in everyday life in society.

From the perspective of information institutions such as libraries, archives, and museums as personal data processors, we must pay attention to treating user privacy data security. For example, health libraries or libraries in institutions where medical research is carried out may process several types of unique category user data, including health, race, ethnic origin, genetics, sex life, or sexual orientation (Oppenheim et al., 2020). Avoid actions that could inadvertently cause data to be leaked to third parties, as this could be detrimental to the institution. That is why it is essential for library and information science students who will become staff at information institutions to be highly aware of this PDP Law.

From the perspective of us as subject privacy data in Indonesia, through surveys with a small scope, such as the student environment here, it is known that the level of awareness is at a 'good level.' However, they are only sometimes ready to comply with the regulations contained in the PDP Law. Besides regulation and awareness, Cybercrime is another aspect closely related to protecting personal data. Widi, Qahar, and Aswari (2021) stated the need for everyone to be aware of the risks of engaging in online crime, since a rise in cases of careless people engaging in online crime has been caused by lenders' unlawful use of personal data. When we have a high enough awareness of the PDP Law, we will be more careful in sharing our private data with other parties, and we will especially be more aware of verifying and validating whether the third party is safe or not in managing our privacy data.

Online privacy protection calls for a range of strategies, an understanding of intricate encryption systems, familiarity with the different privacy settings available on different platforms or electronic devices, the ability to read and understand a variety of privacy policies, and a knack for understanding intricate information systems (Stepanović, 2019). Therefore, online privacy literacy skills are necessary to understand how online systems work and how to protect personal data uploaded to online platforms responsibly. There would be fewer instances of careless individuals exposing personal data due to the growing literacy component of using personal data on digital platforms. The public will have a better understanding of how the flow of personal data and information is managed on digital sites and will have a better understanding of what provisions should

be in accordance with applicable law. As a form of fostering good digital literacy, a socialization process can be carried out with the public so that they are more aware of the existence of the PDP Law.

## CONCLUSION

Overall, the awareness level of Data Privacy Protection Law based on the focus area and dimension is at a good level. According to the findings, each dimension plays a broadly similar, albeit marginally different and insignificant, role. However, in each dimension, several parameters need to be improved to increase student awareness of the existence of the contents of the PDP Law. In the dimension of knowledge, one of the primary causes of data leakage crimes is internet access. For this reason, it is also necessary to increase student knowledge about the entire contents of the PDP Law, not just the central part. Regarding the attitude dimension, the experimental parameters of students with data privacy are suitable. What the respondents have done is quite in accordance with what is stated in the PDP Law. Meanwhile, in the behavioral dimension, the habitual parameters in making agreement documentation with personal data processors are still relatively low compared to other parameters. This causes the behavioral dimension to become a habitual aspect that needs improvement. Even though it is challenging to do practically, it will make an impression if it is done repeatedly. The findings of this study should be helpful as a guide when discussing how crucial it is for students to comprehend the PDP Law, especially in increasing the level of digital literacy. Students are agents who are expected to be influential to the larger community in general. This research is

limited to a PDP Law awareness survey among students, so future research should be able to measure awareness of the broader community as well as socialize the importance of the UUPDP in regulating regulations between personal data subjects, personal data processors, and the government as the control center. Further studies are needed to investigate some modifications to make this measurement model more accurate, in particular, creating more detailed research questions with other approaches to ensure that each assessment is as accurate as possible, employing a Likert scale for more varied response options or ensuring more diverse respondents so that research can more accurate.

## REFERENCES

- Almasyhari, A. K., Sari, Y. P., & Sukesti, F. (2022). Edukasi literasi digital: Peningkatan kesadaran masyarakat dalam perlindungan data pribadi dan kaitannya terhadap financial technology. *Jurnal Abdimas PHB: Jurnal Pengabdian Masyarakat Progresif Humanis Brainstorming*, 5(3), 449-453. <https://doi.org/10.30591/japhb.v5i3.3849>
- Batmetan, J. R., Kariso, B., Moningkey, M., & Tumembow, A. (2018). *Tingkat kesadaran privasi atas masalah keamanan informasi (Lack of security awareness)*. [https://doi.org/10.31219/osf.io/cah\\_zr](https://doi.org/10.31219/osf.io/cah_zr)
- CNN Indonesia. (2022). 10 kasus kebocoran data 2022: Bjorka dominan, ramai-ramai bantah. Retrieved from [cnnindonesia.com](https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah)
- Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, 37, 1-16. <https://doi.org/10.1016/j.clsr.2020.105412>
- European Parliament. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.*, (2016). <https://www.legislation.gov.uk/eur/2016/679/contents>.
- Göldağ, B. (2021). Investigation of the relationship between digital literacy levels and digital data security awareness levels of university students. *E-International Journal of Educational Research*, 12(3), 82-100. <https://doi.org/10.19160/e-ijer.950635>
- Helberger, N., Borgesius, F. Z., & Reyna, A. (2017). The perfect match? A closer look at the relationship between EU Consumer Law and Data Protection Law. *Common Market Law Review*, 54(5), 1-28. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3048844](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048844)
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of

- information. *Media and Communication*, 8(2), 258–269. <https://doi.org/10.17645/mac.v8i2.2855>
- Nurbojatmiko, Firmansyah, A. F., Aini, Q., Saehudin, A., & Amsariah, S. (2020). Information security awareness of students on academic information system using Kruger approach. *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 1–7. IEEE. <https://doi.org/10.1109/CITSM50537.2020.9268795>
- Oppenheim, C., Muir, A., & Korn, N. (2020). *Information Law: Compliance for librarians, information professionals and knowledge managers*. London: Facet Publishing.
- Pangrazio, L., & Selwyn, N. (2019). ‘Personal data literacies’: A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, 21(2), 419–437. <https://doi.org/10.1177/1461444818799523>
- Peng, D., & Yu, Z. (2022). A literature review of digital literacy over two decades. *Education Research International*, 2022, 1–8. <https://doi.org/10.1155/2022/2533413>
- Presiden Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. , Pub. L. No. 17 Oktober 2022. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Jakarta (2022). <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>.
- Priliasari, E. (2019). Pentingnya perlindungan data pribadi dalam transaksi pinjaman online. *Majalah Hukum Nasional*, 49(2), 1–27. <https://doi.org/10.33331/mhn.v49i2.44>
- Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy. *International Journal of Technoethics*, 11(2), 65–94. <https://doi.org/10.4018/IJT.20200701.oa1>
- Soemitra, A., & Hasan, A. (2022). Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di Indonesia. *Juripol: Jurnal Institusi Politeknik Ganesha*, 5(1), 288–303. Retrieved from <https://jurnal.polgan.ac.id/index.php/juripol/article/view/11538>
- Steininger, K., & Rückel, D. (2013). Legal literacy and users’ awareness of privacy, data protection and copyright legislation in the web 2.0 era. *Wirtschaftsinformatik Proceedings*, 103. Leipzig: Association for Information Systems (AIS) eLibrary. Retrieved from <https://aisel.aisnet.org/wi2013/103/>
- Stepanović, I. (2019). Privacy and digital literacy: Who is responsible for the protection of personal data in Serbia? *Zbornik Instituta Za Kriminološka i Sociološka Istraživanja*, 38(3), 45–56. Retrieved from [https://www.iksi.ac.rs/zbornik\\_arhiva/zbornik\\_iksi\\_3\\_2019/zbornik\\_iksi\\_3\\_2019\\_ivana\\_stepanovic.pdf](https://www.iksi.ac.rs/zbornik_arhiva/zbornik_iksi_3_2019/zbornik_iksi_3_2019_ivana_stepanovic.pdf)
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). *Reforming European Data Protection Law* (S. Gutwirth, R. Leenes, & P. de Hert, Eds.). Dordrecht: Springer Netherlands. <https://doi.org/10.1007/978-94-017-9385-8>
- Voigt, P., & von dem Bussche, A. (2017).

- The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>
- Widi, F., Qahar, A., & Aswari, A. (2021). Legal protection against personal data in online loan transactions. *Golden Ratio of Law and Social Policy Review*, 1(1), 17–25. <https://doi.org/10.52970/grlspr.v1i1.152>
- Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, 11(2), 378–389. <https://doi.org/10.15760/comminfolit.2017.11.2.9>

