



Factors in Data Privacy: Assessing Awareness, Knowledge, Attitudes, and Practices in Selected State Universities in the Philippines

Karlo Jose E Nabablit ^{1*}, Neil P Balba ²

^{1,2} Graduate School, Colegio De San Juan De Letran Calamba, Philippines

¹ Cavite State University, Philippines

* Corresponding Author: **Karlo Jose E Nabablit**

Article Info

Impact Factor (RSIF): 8.29

Volume: 02

Issue: 04

Received: 23-04-2026

Accepted: 25-05-2026

Published: 27-06-2026

Page No: 12-18

Abstract

Data privacy has become a critical concern in higher education as institutions increasingly rely on digital technologies to manage academic and administrative information. While technological safeguards and regulatory frameworks are essential, the effectiveness of data privacy programs also depends on the awareness, knowledge, attitudes, and practices (AKAP) of individuals who process and access personal information. This study assessed the data privacy awareness, knowledge, attitude, and practices of students, faculty members, and staff in selected Philippine state universities. A cross-sectional quantitative descriptive research design was employed involving 396 respondents selected through stratified random sampling from five state university campuses in Cavite, Philippines. Data were collected using a validated researcher-developed AKAP questionnaire and analyzed using descriptive statistics, including frequency, percentage, and weighted mean. The findings revealed that respondents demonstrated a high level of data privacy awareness (94–95%), indicating that they were fully aware of their rights and responsibilities under the Data Privacy Act of 2012. Respondents also exhibited an excellent understanding of data privacy principles (90%) and consistently practiced appropriate data privacy measures (88–91%). However, attitudes toward data privacy, although generally positive (80–82%), were comparatively lower than the other dimensions, suggesting that awareness and knowledge do not always translate into consistently proactive privacy mindsets. Overall, the findings indicate that the participating state universities have cultivated a strong culture of data privacy through effective awareness initiatives and institutional policies. Nevertheless, continuous capacity-building programs, behavioral interventions, and periodic policy reinforcement are recommended to strengthen privacy attitudes and sustain responsible data handling practices among higher education stakeholders.

Keywords: Data Privacy, Awareness, Knowledge, Attitude, Practices, Higher Education, Philippine State Universities

1. Introduction

In the Philippines, the enactment of the Data Privacy Act of 2012 (Republic Act No. 10173) established the legal framework for protecting personal information and promoting responsible data processing across public and private organizations (Presbitero & Ching, 2018) ^[11]. The law requires institutions to implement appropriate organizational, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of personal data. While the Act provides a comprehensive legal framework, studies indicate that its implementation across higher education institutions remains inconsistent (Flores & Ching, 2018) ^[5].

This implementation gap is reflected in reports from the National Privacy Commission (NPC), which continue to document incidents of unauthorized disclosure, phishing attacks, ransomware, and other cybersecurity threats affecting educational institutions and government agencies (National Privacy Commission, 2024). These incidents suggest that legal compliance alone is insufficient without the active participation of individuals responsible for handling personal information.

Recent studies have emphasized that effective data privacy protection depends not only on technological safeguards and institutional policies but also on the awareness, knowledge, attitudes, and practices of individuals who process or access personal data (Dienlin, 2024; Meier & Kramer, 2022)^[3, 9]. Human behavior remains one of the most influential factors affecting information security, as privacy breaches frequently result from inadequate awareness, poor decision-making, weak security practices, or failure to comply with institutional policies. Consequently, fostering a strong culture of data privacy among students, faculty members, and administrative staff has become an essential component of institutional governance.

Previous studies have reported generally positive levels of data privacy awareness in higher education institutions; however, variations remain across different dimensions of privacy behavior. While individuals may demonstrate high awareness of privacy rights and legal requirements, this awareness does not always translate into appropriate attitudes or consistent protective practices. This phenomenon has been discussed in the literature as the "privacy paradox," wherein individuals express concern for privacy but fail to consistently adopt behaviors that adequately safeguard personal information (Jernejcic & El-Gayar, 2022; Meier & Kramer, 2022)^[6, 9]. Such findings suggest that assessing awareness alone provides an incomplete understanding of institutional readiness for data privacy.

Within Philippine higher education institutions, empirical studies examining the combined dimensions of awareness, knowledge, attitude, and practices (AKAP) remain limited, particularly in state universities (Doce & Ching, 2018; Ramos, 2020)^[4, 12]. Existing research often focuses on specific stakeholder groups or emphasizes legal compliance and technological controls rather than the human dimensions of data privacy (Martirez, 2023)^[8]. Moreover, there is limited evidence comparing these behavioral dimensions among students, faculty members, and non-teaching personnel within the same institutional setting. Understanding these dimensions is essential because each stakeholder group performs different roles in collecting, processing, accessing, and protecting personal information.

Assessing the awareness, knowledge, attitudes, and practices of university stakeholders provides valuable insights into the strengths and weaknesses of institutional data privacy culture. Such evidence may guide universities in designing targeted capacity-building initiatives, strengthening privacy education, improving institutional policies, and promoting responsible data handling practices. More importantly, understanding the behavioral aspects of data privacy complements organizational and technological safeguards, contributing to a more comprehensive approach to data protection within higher education institutions.

This study assessed the data privacy awareness, knowledge, attitude, and practices of students, faculty members, and staff

in selected Philippine state universities. Specifically, it sought to determine the level of awareness of respondents regarding data privacy principles and rights, evaluate their knowledge of data privacy concepts and legal requirements, examine their attitudes toward protecting personal information, and assess their actual privacy-related practices. The findings are intended to provide empirical evidence that may support the development of institutional initiatives aimed at strengthening data privacy culture and promoting responsible information handling within higher education institutions.

2 Methodology

2.1. Research Design

This study employed a cross-sectional quantitative descriptive research design to assess the data privacy awareness, knowledge, attitude, and practices (AKAP) of students, faculty members, and staff in selected Philippine state universities. A descriptive approach was deemed appropriate because it systematically describes the current status of a phenomenon without manipulating variables, enabling the researchers to examine stakeholders' perceptions and behaviors related to data privacy at a specific point in time (Creswell & Creswell, 2018)^[2].

2.2. Research Setting and Participants

The study was conducted in five selected state university campuses in Cavite, Philippines. These institutions were purposively selected based on the presence of designated Data Protection Officers (DPOs), active implementation of institutional data privacy initiatives, and compliance with the registration requirements of the National Privacy Commission (NPC).

The respondents consisted of students, faculty members, and non-teaching staff who regularly access or process institutional information systems and personal data as part of their academic or administrative responsibilities. A total of 396 respondents participated in the study.

2.3. Sampling Procedure

Purposive sampling was initially employed to identify the participating state university campuses based on institutional characteristics relevant to data privacy implementation. Within each campus, stratified random sampling was utilized to ensure proportional representation of the three respondent groups: students, faculty members, and non-teaching staff. The sample size was determined using a sample size estimation formula for proportions at a 95% confidence level and a 5% margin of error.

2.4. Research Instrument

Data were collected using a researcher-developed Awareness, Knowledge, Attitude, and Practices (AKAP) Questionnaire on data privacy. The instrument was designed to measure four dimensions of stakeholders' data privacy readiness:

- Awareness, which assessed respondents' familiarity with their rights and responsibilities under the Data Privacy Act of 2012;
- Knowledge, which measured respondents' understanding of fundamental data privacy concepts, principles, and institutional requirements;
- Attitude, which examined respondents' perceptions,

beliefs, and willingness to protect personal information; and

- Practices, which evaluated the extent to which respondents applied appropriate data privacy measures in their daily academic and administrative activities.

The questionnaire was developed based on a review of relevant literature, the Data Privacy Act of 2012 (Republic Act No. 10173), and the implementing guidelines of the National Privacy Commission. It underwent expert validation to establish its relevance, clarity, and content validity, and the recommended revisions were incorporated into the final instrument. A pilot test involving 40 respondents was conducted to assess reliability, yielding a Cronbach's alpha coefficient of 0.913, indicating excellent internal consistency for measuring the awareness, knowledge, attitudes, and practices (AKAP) of respondents regarding data privacy.

2.5. Data Collection Procedure

Approval to conduct the study was obtained from the concerned university authorities before data collection commenced. After securing institutional permission, the researchers coordinated with campus administrators to facilitate the administration of the questionnaire.

Participation was voluntary, and respondents were informed of the objectives of the study before completing the survey. Informed consent was obtained from all participants, and confidentiality of responses was maintained throughout the research process. The completed questionnaires were

retrieved, checked for completeness, and prepared for statistical analysis.

2.6. Data Analysis

Descriptive statistical techniques were employed to analyze the collected data. Frequency counts, percentages, and weighted means were computed to determine the respondents' levels of awareness, knowledge, attitude, and practices regarding data privacy.

2.7. Ethical Considerations

The study adhered to established ethical principles in conducting human participant research. Participation was voluntary, and respondents were informed of the purpose of the study, their right to withdraw at any time, and the confidentiality of the information they provided. No personally identifiable information was disclosed in the presentation of the findings. The collection, storage, and processing of research data complied with the provisions of the Data Privacy Act of 2012 (Republic Act No. 10173) to safeguard participants' privacy and confidentiality.

3. Results and Discussion

3.1. Data Privacy Awareness

To determine respondents' level of awareness regarding data privacy, students, faculty members, and staff were asked to assess their understanding of the principles and rights set forth in the Data Privacy Act of 2012. The summary of their responses is presented in Table 1.

Table 1: Respondents' Perceived Level of Awareness on Data Privacy Toward Data Privacy (in percentage %)

RESPONDENT (N = 396)	1	2	3	4	5	%	VERBAL INTERPRETATION
Student	0.23	0.92	6.88	22.01	69.97	95	Fully Aware
Faculty	0.00	0.52	5.34	16.72	77.41	94	Fully Aware
Staff	0.11	0.38	4.40	15.42	79.69	95	Fully Aware

Legend:

5 - Fully Aware: Fully aware of data privacy rights and practices.

4 - Generally Aware: Generally aware, with a solid understanding of data privacy.

3 - Somewhat Aware: Some awareness, but not fully confident in understanding data privacy rights.

2 - Minimally Aware: Limited awareness of data privacy rights and practices.

1 - Not Aware: No knowledge of data privacy principles and practices.

Table 1 presents the respondents' perceived level of awareness regarding data privacy. The findings indicate that students, faculty members, and staff demonstrated a high level of awareness, with overall awareness ratings ranging from 94% to 95%, interpreted as Fully Aware. These results suggest that respondents possess a strong understanding of their rights as data subjects and recognize the importance of protecting personal information within the university environment. This finding is consistent with Sola and Sambo (2025) ^[13], who reported that Philippine students across various disciplines exhibit high levels of awareness regarding the fundamental provisions of the Data Privacy Act of 2012. A closer examination of the indicators reveals that respondents demonstrated the highest levels of awareness concerning the fundamental rights guaranteed under the Data Privacy Act of 2012. Specifically, they were highly aware of their right to be informed about the collection and processing of personal data, the requirement for informed consent prior to data processing, and the obligation of institutions to implement appropriate safeguards to protect personal information. These findings suggest that institutional orientations, awareness campaigns, and policy dissemination initiatives have been effective in familiarizing university

stakeholders with the core principles of data privacy and personal data protection.

Despite the generally high level of awareness, comparatively lower ratings were observed for less frequently exercised rights, particularly the right to data portability and the right to object to the processing of personal data. Although these indicators were still interpreted as Fully Aware, their relatively lower scores indicate that respondents may be less familiar with procedural or technical aspects of the Data Privacy Act than with its more commonly encountered provisions. This observation is supported by Manlaran *et al.* (2026) ^[7], who found that while the general objectives and protective provisions of the Act are widely understood, specific data subject rights that are infrequently exercised tend to receive less attention among members of the academic community.

Overall, the findings reinforce previous studies demonstrating that awareness is generally stronger for data privacy rights that individuals regularly encounter during institutional transactions, such as consent and notification, than for rights that are exercised less frequently. This pattern highlights the need for higher education institutions to expand their data privacy education initiatives beyond the

basic principles of compliance and place greater emphasis on promoting a comprehensive understanding of all data subject rights prescribed under the Data Privacy Act of 2012. Such efforts can help ensure that students, faculty, and staff are not only aware of their fundamental privacy rights but are also empowered to exercise them effectively whenever necessary. The finding supports the view that sustained awareness programs, regular orientations, and effective communication

strategies contribute significantly to strengthening institutional data privacy culture.

3.2. Data Privacy Knowledge

The respondents' perceived level of knowledge on data privacy was assessed to determine their understanding of the principles and practices prescribed by the Data Privacy Act of 2012.

Table 2: Respondents' Perceived Level of Knowledge on Data Privacy Toward Data Privacy (in percentage %)

RESPONDENT (N = 396)	1	2	3	4	5	%	VERBAL INTERPRETATION
Student	0.13	0.76	8.62	31.74	58.72	90	Excellent
Faculty	0.00	2.07	7.59	29.31	61.03	90	Excellent
Staff	0.00	0.00	9.12	32.65	58.24	90	Excellent

Legend:

5 - Excellent Understanding - Excellent understanding of data privacy principles and practices.

4 - Good Understanding - Good understanding with minor gaps in knowledge.

3 - Basic Understanding - Basic understanding with some uncertainty on key concepts.

2 - Limited Understanding - Limited knowledge and understanding of data privacy principles.

1 - No Understanding: No knowledge of data privacy principles and practices.

Table 2 presents the respondents' level of knowledge regarding data privacy. The results reveal an overall rating of 90%, interpreted as Excellent Understanding, indicating that students, faculty members, and staff possess a solid grasp of fundamental data privacy concepts and the principles governing the protection of personal information. This finding suggests that respondents have developed an adequate understanding of both the legal framework and the practical responsibilities associated with handling personal data within the university setting. It also supports the assertion of Solas (2026)^[14] that privacy education enhances individuals' understanding of legal obligations while fostering responsible management of personal information. The respondents demonstrated the strongest knowledge in areas directly associated with routine data processing activities, particularly informed consent, access control, implementation of security safeguards, prevention of unauthorized disclosure, and the lawful collection and processing of personal information. These findings indicate that institutional policies, seminars, and awareness initiatives have effectively reinforced respondents' understanding of the essential principles that govern responsible data management. The consistently high ratings across these indicators further suggest that the university has established a strong foundation for promoting compliance with data privacy standards.

In contrast, comparatively lower levels of knowledge were observed in topics requiring greater familiarity with

operational and regulatory procedures, including data minimization, records retention, secure disposal of personal information, and specific provisions of the Data Privacy Act of 2012. Although these indicators were still interpreted as reflecting Excellent Understanding, their relatively lower ratings imply that respondents may be less acquainted with the procedural requirements that guide the entire data lifecycle. As emphasized by Manlaran *et al.* (2026)^[7], a comprehensive understanding of these operational aspects is necessary to ensure consistent compliance with legal and ethical standards in both academic and administrative functions.

Taken together, the findings indicate that respondents possess not only a strong theoretical understanding of data privacy but also a sound appreciation of the responsibilities involved in protecting personal information. Nevertheless, the identified knowledge gaps underscore the importance of sustained institutional capacity-building initiatives, such as periodic refresher programs, specialized workshops, and policy orientation sessions. Strengthening these areas will enable university stakeholders to move beyond basic compliance and develop a more comprehensive and practice-oriented understanding of data privacy principles.

3.3. Data Privacy Attitude

The perceived level of attitude toward data privacy among students, faculty members, and staff is presented in Table 3.

Table 3: Respondents' Perceived Level of Attitude on Data Privacy Toward Data Privacy (in percentage %)

RESPONDENT (N = 396)	1	2	3	4	5	%	VERBAL INTERPRETATION
Student	2.04	3.68	19.54	33.65	41.09	82	Highly Proactive
Faculty	2.41	2.93	22.41	38.79	33.45	80	Generally Mindful
Staff	1.76	3.53	18.24	36.76	39.71	82	Highly Proactive

Legend:

5 - Highly Proactive - Highly proactive and cautious about privacy concerns, considering risks carefully.

4 - Generally Mindful - Generally mindful of privacy risks, but may overlook certain aspects.

3 - Uncertain - Indifferent or uncertain about privacy risks and benefits.

2 - Disregards Risks - Tends to disregard privacy risks and shares data freely.

1 - Unconcerned - Completely unconcerned about privacy risks and has no hesitation in sharing data.

Table 3 presents the respondents' attitudes toward data privacy. The findings reveal that the respondents generally hold positive attitudes regarding the protection of personal information. Students and staff obtained an overall attitude

rating of 82%, interpreted as Highly Proactive, while faculty members achieved an overall rating of 80%, interpreted as Generally Mindful. These results indicate that respondents value data privacy and demonstrate a willingness to support

responsible data protection practices within the university environment.

The response distribution further reinforces this positive outlook. The largest proportion of students (41.09%), faculty members (33.45%), and staff (39.71%) selected the highest attitude rating (5 – Highly Proactive), while a considerable number also selected rating 4 – Generally Mindful. In contrast, only a small percentage of respondents chose the lower attitude categories (ratings 1 and 2). This pattern suggests that positive perceptions toward safeguarding personal information are widely shared across the university community and that most respondents recognize the importance of exercising caution when handling personal data.

Despite these encouraging results, differences were observed among the respondent groups. Students and staff were classified as Highly Proactive, reflecting a stronger inclination to adopt privacy-conscious behaviors and support data protection initiatives. Faculty members, on the other hand, were categorized as Generally Mindful, indicating that although they appreciate the importance of privacy and exercise reasonable caution, their attitudes may not consistently translate into the same level of proactive engagement demonstrated by the other groups. Nevertheless, the overall findings indicate that all respondent groups maintain favorable attitudes toward data privacy.

When compared with the respondents' awareness and knowledge scores, attitude obtained relatively lower ratings. This suggests that possessing knowledge of data privacy regulations and principles does not necessarily lead to the

development of a consistently proactive privacy mindset. Positive attitudes toward privacy are influenced not only by knowledge but also by personal beliefs, perceived responsibilities, organizational culture, and everyday experiences in handling personal information. Consequently, institutional efforts should extend beyond awareness campaigns and knowledge dissemination by fostering a culture in which privacy-conscious values are consistently reinforced through policies, leadership support, and regular privacy-related activities.

The findings are consistent with the Privacy Calculus Theory, which explains that individuals evaluate the perceived benefits and potential risks before deciding whether to disclose personal information (Dienlin, 2024) ^[3]. Likewise, the results align with studies on the privacy paradox, which suggest that individuals often express favorable attitudes toward privacy even though these attitudes may not always result in the highest level of privacy-conscious behavior (Jernejcic & El-Gayar, 2022) ^[6]. This relationship highlights that cognitive understanding alone is insufficient to establish a proactive privacy culture, as factors such as convenience, institutional trust, and situational considerations may influence privacy-related decisions despite awareness of potential risks (Bringula *et al.*, 2024) ^[1].

3.4. Data Privacy Practices

To determine the respondents' data privacy practices, they were asked to assess the extent to which they implement data privacy measures in their daily activities. The results are presented in Table 4.

Table 4: Respondents' Perceived Level of Practice on Data Privacy Toward Data Privacy (in percentage %)

RESPONDENT (N = 396)	1	2	3	4	5	%	VERBAL INTERPRETATION
Student	0.23	0.95	10.07	31.15	<u>57.60</u>	89	Consistently Practicing
Faculty	0.00	0.52	9.48	37.93	<u>52.07</u>	88	Consistently Practicing
Staff	0.00	0.59	5.88	32.35	<u>61.18</u>	91	Consistently Practicing

Legend:

5 - Consistently Practicing - Consistently follows best practices for protecting personal data and ensuring security.

4 - Generally Practicing - Generally, follows data privacy practices, though there may be occasional lapses.

3 - Sometimes Practicing - Some adherence to data privacy practices, but could improve.

2 - Rarely Practicing - Rarely follows best practices for data privacy or may unintentionally expose personal data.

1 - Not Practicing - Does not follow any data privacy practices and regularly risks exposing personal data.

Table 4 presents the respondents' data privacy practices. The findings reveal that students, faculty members, and non-teaching staff consistently implement data privacy measures in their respective academic and administrative responsibilities. Students obtained an average rating of 89%, faculty members 88%, and non-teaching staff 91%, all verbally interpreted as Consistently Practicing. These results indicate that respondents have effectively translated their awareness, knowledge, and positive attitudes toward data privacy into routine privacy-protective behaviors.

The highest-rated practices were associated with fundamental data protection measures, including the use of strong passwords, restricting access to confidential information, verifying the necessity of providing personal information before disclosure, complying with institutional policies, and exercising caution when handling sensitive data. These behaviors reflect respondents' commitment to safeguarding personal information and suggest that institutional policies, awareness programs, and training initiatives have been effective in promoting responsible data handling across the university community.

Although the overall practice ratings remained consistently high, relatively lower scores were observed for routine cybersecurity behaviors, particularly the regular updating of passwords and login credentials. While these practices were still interpreted as Consistently Practicing, the findings suggest that repetitive security measures are less consistently performed than other privacy-related activities. This observation reflects a common challenge in maintaining good cyber hygiene, where routine security tasks may gradually receive less attention despite individuals' awareness of their importance (Sola & Sambo, 2025) ^[13].

The results imply that respondents have established positive data privacy practices in their daily activities. However, sustaining these practices requires continuous institutional support through periodic awareness campaigns, refresher training, cybersecurity simulation exercises, and policy reinforcement. Strengthening routine cyber hygiene behaviors will help ensure that privacy protection remains a consistent organizational practice rather than a compliance-driven obligation, thereby enhancing the university's overall culture of data privacy and information security.

3.5. Overall Assessment of Awareness, Knowledge, Attitude, and Practices

Figure 1 illustrates the respondents' overall assessment of

awareness, knowledge, attitude, and practices on data privacy.

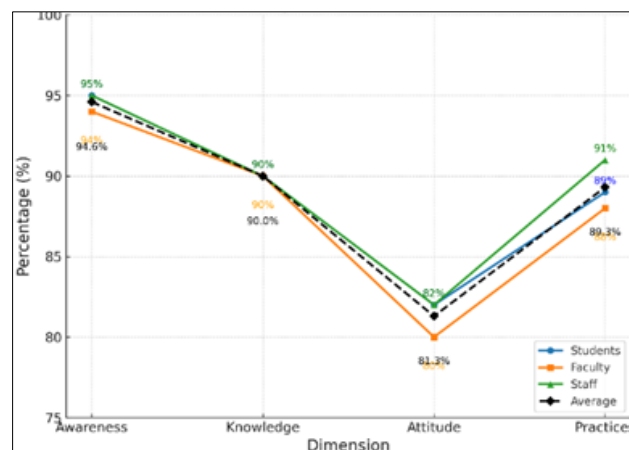


Fig 1: Level of Awareness, Knowledge, Attitude, and Practices of Data Privacy Among Respondents

The comparative assessment of the four dimensions reveals a consistent pattern across respondent groups. Awareness obtained the highest ratings (94–95%), followed by knowledge (90%) and practices (88–91%), while attitude recorded comparatively lower scores (80–82%).

Collectively, the participating state universities have successfully established a strong foundation of data privacy awareness and knowledge among students, faculty members, and staff. More importantly, these competencies are reflected in respondents' day-to-day privacy practices, indicating that institutional policies and educational initiatives have positively influenced responsible data handling behaviors.

However, the relatively lower attitude scores indicate that cognitive understanding alone does not necessarily foster consistently proactive privacy mindsets. This gap reflects the complex nature of human decision-making in privacy-related situations, where convenience, institutional trust, and perceived benefits may influence individuals' willingness to disclose personal information despite recognizing potential risks.

Taken all together, the results demonstrate that the participating universities have cultivated a positive data privacy culture characterized by high levels of awareness, sound knowledge, and responsible practices. Nevertheless, sustaining this culture requires continuous education, regular policy reinforcement, and behavioural interventions that strengthen privacy attitudes alongside technical and organizational safeguards. Such initiatives will further enhance institutional readiness to protect personal information and promote responsible data governance within higher education. Sustaining a positive data privacy culture requires continuous education and behavioral interventions that strengthen privacy attitudes alongside technical safeguards (ICEED, 2024; Solas, 2026) ^[14].

4. Research Implication

4.1. Conclusion

The study concludes that students, faculty members, and staff in the selected Philippine state universities demonstrate a high level of awareness, excellent knowledge, positive attitudes, and consistent data privacy practices. The findings indicate that the participating universities have successfully established a strong culture of data privacy through effective

institutional policies, awareness initiatives, and educational programs that promote responsible handling of personal information.

Among the four dimensions assessed, awareness obtained the highest ratings, followed by knowledge and practices, while attitude recorded comparatively lower scores. Although respondents generally exhibited favorable attitudes toward data privacy, the findings suggest that a strong understanding of data privacy principles does not always result in a consistently proactive privacy mindset. This emphasizes the importance of continuously reinforcing positive privacy attitudes through sustained education, awareness campaigns, and practical learning experiences.

The evidence demonstrates that the participating state universities are fostering an environment that supports responsible data privacy practices. Nevertheless, continuous improvement through regular training, policy reinforcement, and institutional initiatives remains essential to sustain and further strengthen data privacy awareness, attitudes, knowledge, and practices among university stakeholders

4.2. Recommendation

1. State universities should sustain and strengthen their data privacy awareness programs by conducting regular orientations, seminars, and information campaigns for students, faculty members, and staff to reinforce their understanding of the Data Privacy Act of 2012 and their responsibilities in protecting personal information.
2. Universities could implement continuous capacity-building activities that focus not only on increasing knowledge but also on cultivating positive privacy attitudes through scenario-based training, practical workshops, and simulations that encourage responsible decision-making in handling personal data.
3. Institutional policies and data privacy practices should be regularly reviewed, monitored, and reinforced to ensure consistent compliance with data privacy regulations and promote responsible handling of personal information across academic and administrative functions.
4. Future researchers are encouraged to investigate other factors that may influence data privacy attitudes and practices, such as organizational culture, digital literacy,

perceived privacy risks, and technological readiness. Similar studies may also be conducted in other higher education institutions or employ inferential or mixed-method research designs to provide a broader understanding of data privacy behavior in the Philippine higher education sector.

References

1. Bringula RP, Lansigan RR, Racelis MC, Lansigan PLG, Lansigan PLG. Data privacy paradox: The role of higher education institutions towards building data privacy awareness in the digital age. In: 2024 IEEE 13th International Conference on Engineering Education (ICEED). IEEE; 2024. p. 1-6. doi:10.1109/ICEED62316.2024.10923801.
2. Creswell JW, Creswell JD. *Research design: Qualitative, quantitative, and mixed methods approaches*. 5th ed. Thousand Oaks (CA): SAGE Publications; 2018.
3. Dienlin T. Privacy calculus: Theory, studies, and new perspectives [Preprint]. OSF Preprints; 2024. doi:10.31235/osf.io/z3gw8.
4. Doce LJ, Ching MRD. RA 10173 and its challenges to Philippine state universities and colleges' compliance performance: The case of Mindanao State University-General Santos City. In: Proceedings of the 2nd International Conference on Education and E-Learning; 2018. p. 100-104. doi:10.1145/3234781.3234789.
5. Flores RTG, Ching MRD. Philippine SUCs compliance performance on RA 10173: A case study on Bukidnon State University. In: Proceedings of the 2nd International Conference on Education and E-Learning; 2018. p. 95-99. doi:10.1145/3234781.3234790.
6. Jernejcic T, El-Gayar OF. The role of the privacy calculus and the privacy paradox in the acceptance of wearables for health and wellbeing. *AIS Trans Hum Comput Interact*. 2022;14(4):518-545. doi:10.17705/1thci.00177.
7. Manlaran MS, Miranda KPB, Pescante CPF. An empirical study on data privacy awareness and practices among Misamis University students [Internet]. Zenodo; 2026 [cited 2026 Jul 23]. Available from: <https://doi.org/10.5281/zenodo.18373093>
8. Martinez KC. Compliance on Data Privacy Act of private higher educational institutions (HEIs) in the province of Albay: Basis for institutional policy. *Int J Econ Bus Entrep Res*. 2023;3:100-115.
9. Meier Y, Krämer NC. The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Commun Res*. 2022;49(8):1083-1108. doi:10.1177/00936502221102101.
10. National Privacy Commission. Data Breach Management System (DBNMS) Live Stats [Internet]. 2024 [cited 2026 Jul 23]. Available from: <https://privacy.gov.ph/dbnmslivestats>
11. Presbitero JV, Ching MRD. Assessing compliance of Philippine state universities to the Data Privacy Act of 2012: The case of Caraga State University. In: Proceedings of the 2nd International Conference on Education and E-Learning; 2018. p. 110-114. doi:10.1145/3234781.3234800.
12. Ramos DP. Perceptions of students, faculty and administrative staff on the Data Privacy Act: An exploratory study [Internet]. 2020 [cited 2026 Jul 23]. Available from: <https://www.academia.edu/43085532>
13. Sola E, Sambo RJ. Level of knowledge of criminology students on Data Privacy Act of 2012. *Int J Multidiscip Res*. 2025;7(5). doi:10.36948/ijfmr.2025.v07i05.53478.
14. Solas J. Data privacy awareness and compliance of students in online learning platforms. *Globus J Prog Educ*. 2026.

How to Cite This Article

Nabablit KJE, Balba NP. Human factors in data privacy: Assessing awareness, knowledge, attitudes, and practices in selected state universities in the Philippines. *Int J Humanit Sustain Innov*. 2026;2(4):12-18.

Creative Commons (CC) License

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution NonCommercial-ShareAlike 4.0 International (CC BYNC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.