

The Level of Awareness on Data Privacy Act Among the Selected Employees in Metro Manila

Joffer Brezuela Jumaquio

*Master of Science in Criminology, PHINMA St. Jude College, Quezon City Inc.,
Murphy, Quezon City, Philippines*

Publication history: Received: March 27, 2026; Revised: April 20, 2026; Accepted: April 25, 2026

Email of Corresponding Author: jumaquiojoffer@gmail.com

Abstract

This study aimed to assess the level of awareness of selected government and private employees in Metro Manila regarding the Data Privacy Act of 2012 (Republic Act No. 10173). Anchored on Organizational Compliance Theory (Weaver, Treviño, & Cochran, 1999) and the legal framework of the Data Privacy Act, the study examined how awareness, organizational practices, and compliance mechanisms influence data privacy implementation. A quantitative research design was employed using a structured and validated survey questionnaire administered to 110 respondents selected through stratified random sampling from one government and one private institution. Data were analyzed using frequency, percentage, and weighted mean. Findings revealed that respondents, despite having high educational attainment and extensive years of service, demonstrated only a slight level of awareness of the Data Privacy Act, with a grand mean of 2.44. While they were highly aware of the importance of protecting personal and sensitive information, they showed low awareness regarding mandatory training and penalties for non-compliance. The study also identified significant issues and challenges, particularly inadequate training, low awareness of key provisions, limited resources, and insufficient technological capability, which contributed to compliance difficulties (AWM = 3.12). In response, the proposed solutions—rated as highly recommended (AWM = 3.39)—emphasized regular training programs, improved cybersecurity systems, integration of data privacy education into organizational processes, and capacity-building initiatives. The study concluded that enhancing employee awareness through continuous training and strengthening institutional capabilities are critical for improving compliance with data privacy regulations. The findings align with SDG 16 (Peace, Justice, and Strong Institutions) by promoting accountability, data protection, and institutional integrity, and SDG 4 (Quality Education) through the emphasis on continuous learning and capacity-building. In terms of sustainability impact, the study contributes to strengthening organizational governance, improving data protection practices, and fostering a culture of accountability and security within institutions, thereby supporting long-term institutional resilience and public trust.

Keywords: Awareness, Compliance, Data Privacy Act of 2012, Data Protection, Government Employees, Metro Manila, Organizational Compliance, Private Employees

1. Introduction

Data privacy refers to individuals' ability to control how their personal information is collected, managed, and shared (Buxton, 2024b; Algolia, 2024). Personal information includes any data that can directly or indirectly identify an individual (Section 3[g], R.A. No. 10173). The increasing reliance on digital platforms has led to widespread collection of personal data across institutions such as government agencies, hospitals, and private organizations. In the Philippines, data breaches reached approximately 0.14 million in the fourth quarter of 2023, driven by rapid digitalization, evolving cyber threats, and insufficient cybersecurity measures (Technologies, 2024). The enactment of the Data Privacy Act of 2012 aimed to protect the fundamental right to privacy while supporting innovation and information flow (Doce and Ching, 2018). However, cybercrimes such as identity theft and online fraud continue to pose risks, emphasizing the need for increased awareness and preventive strategies. Cybersecurity threats—including ransomware, phishing, and denial-of-service attacks—highlight the importance of adopting holistic approaches such as systems thinking to manage risks (Leveson, 2014). Despite regulatory frameworks, developing countries like the Philippines continue to face challenges in addressing cybercrime and ensuring adequate protection of personal data.

Literature emphasizes that data privacy is both a legal and ethical concern in modern society. Organizations increasingly rely on personal data for decision-making and operational efficiency, making data protection essential (Diyoke & Tochukwu, 2020). Privacy is recognized as a fundamental human right, though it must be balanced with societal interests such as security and transparency (Supeno et al., 2025; Santana and Ansari, 2023). Employee awareness is a key determinant of effective data privacy implementation. Studies show that informed employees are more likely to follow proper data handling procedures and uphold accountability (Miano, 2025). Ethical responsibility and continuous training

further strengthen compliance (Inquiro, 2024). However, reports indicate that many data breaches result from human error rather than technological failure, underscoring the importance of awareness programs (NPC, 2021). Challenges in data privacy awareness include limited training, insufficient institutional support, and competing organizational priorities (Abubakar et al., 2024; Foronda et al., 2023). Structural constraints such as inadequate resources and fragmented systems also hinder effective implementation (IAPP, 2017; Data Guidance, 2017). To address these issues, literature recommends integrating privacy into organizational governance, adopting evidence-based policies, and strengthening collaboration among institutions (Lacity and Khan, 2021; Li et al., 2025; Claveria et al., 2025). Training programs and capacity-building initiatives are consistently identified as effective strategies for improving awareness and compliance.

Globally, the rise of digital technologies has intensified concerns over data protection, leading to the development of regulatory frameworks such as the GDPR in Europe. In the Philippines, the Data Privacy Act of 2012 established the National Privacy Commission to enforce compliance and promote data protection practices (NPC, 2016). Despite these efforts, challenges remain at the national and local levels. Philippine institutions often experience partial compliance due to financial limitations, lack of technical expertise, and competing priorities (Ching and Celis, 2018). Furthermore, employee awareness gaps persist, particularly in understanding key provisions such as consent and data subject rights (Barlaan, 2023). Metro Manila, as a hub of government and private sector activity, represents a critical setting for examining data privacy awareness due to its high concentration of data-driven operations and digital transactions.

This study is grounded in Organizational Compliance Theory, which posits that compliance behavior is influenced by both structural mechanisms and organizational culture (Weaver, Treviño, & Cochran, 1999). Effective compliance depends on the integration of policies, monitoring systems, and ethical leadership within organizational practices. The study is also anchored on the Data Privacy Act of 2012 (RA 10173), which mandates organizations to implement security measures such as appointing Data Protection Officers, conducting Privacy Impact Assessments, and developing privacy management programs (NPC, 2016). Additionally, the Input-Process-Output (IPO) model guides the conceptual framework, linking employee profiles and awareness levels (input), data collection methods (process), and compliance outcomes (output). These frameworks collectively support the assessment of employee awareness and its impact on data privacy compliance.

Existing literature highlights the importance of data privacy governance and employee awareness but reveals gaps in empirical research focusing on organizational settings in Metro Manila. While studies indicate the presence of compliance mechanisms, they also show that awareness and training remain insufficient (Foronda et al., 2023; Pitogo, 2019). There is limited evidence examining the actual level of employee awareness, the specific challenges affecting compliance, and the effectiveness of proposed interventions. This study addresses these gaps by assessing awareness levels, identifying barriers, and proposing strategies to enhance data privacy practices among employees in both government and private sectors.

This study aligns with several Sustainable Development Goals (SDGs):

SDG 9 – Industry, Innovation and Infrastructure: Promotes secure digital infrastructure and responsible data management.

SDG 16 – Peace, Justice, and Strong Institutions: Supports transparency, accountability, and protection of individual rights through data privacy laws.

SDG 8 – Decent Work and Economic Growth: Enhances workforce competence and ethical practices in handling data.

By strengthening data privacy awareness and compliance, the study contributes to building resilient institutions and secure digital environments.

This study contributes to multiple dimensions of sustainability:

Technological sustainability: Enhances cybersecurity practices and responsible data use.

Institutional sustainability: Strengthens governance, compliance systems, and organizational accountability.

Socio-economic sustainability: Builds trust in digital systems, supporting economic growth and public confidence.

Educational sustainability: Promotes continuous learning and capacity-building among employees. By addressing awareness gaps and proposing practical solutions, the study supports long-term improvements in data protection, organizational resilience, and sustainable digital transformation.

2. Material and methods

2.1 Research Design

This study employed a quantitative research design to measure the level of awareness of selected employees from government and private agencies in Metro Manila regarding the Data Privacy Act of 2012 (Republic Act No. 10173). The quantitative approach enabled the collection of numerical data and statistical analysis of employee perceptions. It provided an accurate profile of relevant phenomena and allowed the researcher to analyze awareness levels across a wide population (Saunders et al., 2009; Miller, 1991). The design aimed to generate objective and measurable data to determine how employee awareness contributes to data privacy compliance.

2.2 Locale of the Study

The study was conducted in Metro Manila (National Capital Region, NCR), Philippines. The area consists of 16 cities and 1 municipality and serves as a major center for government agencies, local government units, government-owned corporations, and private enterprises. Due to its dense population and extensive use of data-intensive systems, Metro Manila was considered a strategic and representative setting for examining awareness of the Data Privacy Act of 2012 in both public and private sectors.

2.3 Respondents of the Study

The respondents consisted of selected employees from one government agency and one private company in Metro Manila. These employees were engaged in services requiring the collection and processing of personal data. The total population included 151 employees, composed of both government and private sector personnel.

2.4 Sample and Sampling Procedure

The study utilized a stratified random sampling technique to ensure representation across different employee groups. The population was divided into two groups: government employees and private employees. From the total population of 151, a sample size of 110 respondents was determined using Slovin's formula with a 5% margin of error. The distribution of respondents included 46 government employees and 64 private employees. This method minimized selection bias and enhanced the reliability and generalizability of the findings within the study setting.

2.5 Research Instrument

Data were collected using a structured survey questionnaire developed and validated by academic and field experts. The instrument consisted of four parts: demographic profile, level of awareness of the Data Privacy Act of 2012, issues and challenges affecting awareness, and proposed solutions to enhance awareness. Responses were measured using a four-point Likert scale to assess levels of awareness, agreement, and recommendation. This structure allowed systematic evaluation of employee perceptions and experiences related to data privacy.

2.6 Data Gathering Procedure

The data collection process involved several steps to ensure accuracy and ethical compliance. The questionnaire was pre-tested among fifteen personnel to validate clarity and reliability, and revisions were made based on feedback. Formal permission and endorsement were obtained from relevant authorities before data collection. Survey questionnaires were distributed to selected respondents through digital platforms, particularly Google Forms. The purpose of the study, voluntary participation, and confidentiality of responses were clearly explained. Respondents were given sufficient time to complete the survey, after which the researcher collected and organized the data. Coordination with participating institutions ensured smooth administration of the survey, and assistance from a statistician was sought for data analysis.

2.7 Data Analysis Techniques

The study employed descriptive statistical tools to analyze the collected data. Frequency and percentage were used to describe the distribution of respondents according to demographic characteristics. Weighted mean was applied to determine the level of awareness and evaluate responses to survey indicators. The Likert scale was used to interpret responses, ranging from "Highly Aware" to "Not Aware," and from "Strongly Agree" to "Strongly Disagree" (Segrei, 2004). These techniques enabled systematic interpretation of quantitative data and supported the study's objective of assessing employee awareness.

2.8 Ethical Considerations

Ethical principles were strictly observed throughout the study. Participation was voluntary, ensuring that respondents were not subjected to pressure or coercion. The researcher-maintained fairness, transparency, and respect for participants, and ensured the confidentiality of all collected information. Ethical standards guided all stages of the research process, from data collection to analysis.

3. Results and Discussion

3.1 Profile of Respondents

3.1.1 Age Distribution

The results show that most respondents belonged to the 31–40 age group, accounting for the largest proportion, followed by those aged 41–50 and 20–30, while the least number came from those aged 51 and above. Both government and private employees reflected a similar age distribution, with the majority concentrated in the middle-age working group. This indicates that the respondents are primarily in their most active and productive working years, which suggests a workforce capable of understanding and adapting to data privacy requirements. Their age profile supports their potential to engage in organizational compliance and learning processes related to data privacy.

3.1.2 Gender Distribution

The findings reveal that female respondents slightly outnumbered male respondents overall. In government agencies, males were slightly more represented, while in private organizations, females comprised the majority. This distribution suggests a balanced representation of gender in the study, allowing for a broader perspective on awareness levels. Gender diversity may contribute to varied perceptions and practices related to data privacy within organizations.

3.1.3 Educational Attainment

Most respondents were college-level graduates, followed by those with master's units and master's degrees, while only a few had doctoral units or postgraduate qualifications. This indicates that the respondents generally possess a high level of educational attainment, which implies a strong capacity to understand legal frameworks such as the Data Privacy Act. Their educational background supports the reliability of their responses and suggests that awareness gaps are not due to lack of formal education.

3.1.4 Years in Service

The majority of respondents had 26–36 years of service, followed by those with 16–25 years and 46 years and above, while the least were in the 1–15 years category. This suggests that most respondents are experienced employees with long-term exposure to organizational processes. Despite this, awareness levels may still vary, indicating that experience alone does not guarantee knowledge of data privacy regulations.

3.2 Level of Awareness on the Data Privacy Act of 2012

3.2.1 Overall Awareness Level

The findings indicate that both government and private employees were generally “Slightly Aware” of the Data Privacy Act of 2012, with an overall mean score of 2.44. The highest awareness was observed in recognizing the importance of protecting personal and sensitive information, while the lowest awareness was found in the requirement to attend training and understanding penalties for non-compliance. Both groups showed nearly identical levels of awareness. This suggests that while employees recognize the importance of data protection, they lack deeper knowledge of specific legal provisions and compliance requirements. The results highlight the need for structured training and awareness programs to improve understanding of the law and its practical application.

3.2.2 Awareness of Key Provisions and Responsibilities

The results show that respondents were aware of identifying actions that may lead to data privacy violations and had moderate awareness of key provisions of the law. However, awareness was low regarding training requirements and penalties for violations. This indicates that employees possess basic conceptual awareness but lack comprehensive understanding of procedural and legal aspects. The findings imply that awareness is more intuitive than formal, reinforcing the importance of systematic training and policy orientation.

3.3 Issues and Challenges Affecting Awareness

3.3.1 Training and Knowledge Gaps

The results reveal that respondents strongly agreed that inadequate training is a major issue affecting awareness, along with a general low level of understanding of specific provisions such as consent, data subject rights, and accountability. The overall assessment of issues and challenges was at the level of agreement. This indicates that insufficient training programs significantly contribute to low awareness levels. The findings support the idea that employee understanding of data privacy depends largely on continuous education and institutional support, as emphasized in existing studies on organizational compliance.

3.3.2 Organizational and Behavioral Factors

The findings show that employees agreed that behavioral control, attitudes, and subjective norms influence their compliance with the Data Privacy Act. They also acknowledged challenges in complying with the law. This suggests that awareness is not only influenced by knowledge but also by psychological and organizational factors. Employees' willingness and ability to comply are shaped by workplace culture and perceived control, aligning with theories that emphasize behavioral influences on compliance.

3.3.3 Resource and Structural Constraints

The results indicate that respondents agreed that limited financial and human resources, particularly in smaller organizations, hinder compliance with data privacy requirements. This implies that structural limitations affect the implementation of privacy measures. Organizations may struggle to invest in secure systems and qualified personnel, highlighting the need for institutional support and resource allocation to improve compliance.

3.4 Proposed Solutions to Enhance Awareness

3.4.1 Training and Capacity Building

The findings show that respondents highly recommended organizing regular training sessions as the most effective solution to enhance awareness, followed by integrating data privacy into existing training programs and using practical engagement methods. This suggests that training is viewed as the primary strategy for improving awareness and compliance. The emphasis on continuous learning aligns with the need for capacity-building initiatives to strengthen employee competence in data privacy practices (Koontz & O'Donnell, 1976; Republic Act No. 10173, 2012).

3.4.2 Organizational and System Improvements

The results indicate that improving cybersecurity systems and providing training on Privacy Impact Assessments were also highly recommended solutions. This implies that awareness enhancement must be supported by strong organizational systems and technological infrastructure. Effective data protection requires both human competence and institutional capability to ensure compliance.

3.4.3 Monitoring and Evaluation Strategies

The findings show that respondents recommended using surveys and interviews to assess employee understanding and identify areas for improvement, although this was rated slightly lower than other solutions. This suggests that monitoring mechanisms are necessary but may not be prioritized compared to direct training interventions. However, evaluation remains essential for identifying gaps and improving awareness programs. Overall, the findings confirm that while employees demonstrate basic awareness of data privacy, significant gaps remain in their understanding of legal requirements, training obligations, and compliance mechanisms. The results emphasize the importance of continuous training, organizational support, and structured implementation strategies to enhance awareness and ensure effective compliance with the Data Privacy Act of 2012.

4. Conclusion & Recommendations

The study revealed that the respondents, who are mostly in their productive age with relatively high educational attainment and extensive years of service, possess the capacity to understand data privacy principles; however, both government and private employees in Metro Manila were only slightly aware of the provisions of the Data Privacy Act of 2012 due to insufficient training and limited understanding of its specific requirements. The findings further showed that respondents acknowledged significant issues and challenges in compliance, particularly the lack of training, low awareness of key provisions, and limited technological capability to address cyber threats, which contribute to misunderstandings and compliance difficulties. Moreover, the study identified that enhancing awareness through structured and continuous training programs is essential in improving employees' knowledge and ensuring compliance with the law.

Based on the findings, it is recommended that government and private institutions implement comprehensive and continuous training programs to enhance employees' awareness and understanding of the Data Privacy Act of 2012, particularly focusing on its provisions, responsibilities, and compliance requirements. Institutions should also strengthen their technological capabilities, organizational structures, and workforce capacity to effectively prevent and respond to cyber threats and data privacy risks. Furthermore, there is a need to improve information systems, promote proactive data protection practices, and support capacity-building initiatives that reinforce employees' ability to safeguard personal information. Finally, future researchers are encouraged to expand the scope of similar studies, explore additional methodologies, and assess the effectiveness of training programs and institutional readiness to further strengthen data privacy awareness and compliance.

Compliance with ethical standards

The authors declare no conflict of interest. This study complied with recognized ethical standards for human-participant research by ensuring voluntary participation with informed consent, the right to withdraw without penalty, and strict confidentiality through anonymous, secure, and aggregated data handling. Given the focus on psychological well-being, procedures were non-invasive, and safeguards were observed to minimize discomfort, with guidance to appropriate support services when needed, and required institutional permissions were secured for instrument use and access to academic records.

REFERENCES

- Abubakar, M., Umar, A., & Abubakar, M. (2024). Personal data and privacy protection: State of literature. ResearchGate.
- Agup, R. M. (2024). Data privacy act: Awareness, compliance, and challenges of nurses of government hospitals in Northern Philippines. *SEEJPH*, XXV, 2215–2224.
- Ayuyang, D. M. (2024). Extent of implementation and level of awareness of employees on the data privacy and cybersecurity acts of Cagayan State University. *Frontiers in Health Informatics*, 13(7).
- Bamberger, K. A., & Mulligan, D. K. (2019). *Privacy on the ground: Driving corporate behavior in the United States and Europe*. MIT Press.
- Barlaan, J. V. (2023). Exploring local government employees' awareness of data privacy act: Insights and recommendations in the lenses of the Theory of Planned Behavior.
- Bennett, C. J., & Raab, C. D. (2018). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
- Castro, C. K. (2021). The implementation of the Data Privacy Act among higher educational institutions in the Province of Pangasinan. *Asian Journal of Multidisciplinary Studies*, 4(2), 103–111.
- Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

- Ching, M. R. D., & Celis, N. J. (2018). Data privacy act of 2012: Compliance performance of CHED and COMELEC. De La Salle University Repository.
- Claveria, P. S., Abante, M. V., & Vigonte, F. (2025). Understanding the Data Privacy Act of 2012: Safeguarding the Filipino's digital rights. SSRN. <https://doi.org/10.2139/ssrn.5274285>
- Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *Digital Health*, 11. <https://doi.org/10.1177/20552076251343959>
- DataGuidance. (2017). GDPR v. Data Privacy Act and IRRs Philippines.
- Diyoke, M. C., & Tochukwu, S. (2020). An analysis of data protection and compliance in Nigeria. *ResearchGate*, 4, 377–382.
- DLA Piper. (2025). Data protection in the Philippines: Country overview. *DLA Piper Data Protection Handbook*.
- European Union. (2016). General Data Protection Regulation (GDPR). *Official Journal of the European Union*.
- Foronda, S. M. (2023). Implementation of Republic Act 10173: A systematic literature review. *SSRN Electronic Journal*.
- Foronda, S. M., Ching, M. R. D., & Pitogo, V. A. (2023). Understanding institutional determinants of data privacy compliance. *Philippine Journal of Public Administration*, 67(2), 145–168.
- Foronda, S. M., Javier, N., Vigonte, F., & Abante, M. V. (2023). Implementation of RA 10173 in ALECO. *SSRN Electronic Journal*.
- Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics. *Research and Practice in Technology Enhanced Learning*, 13(1).
- International Association of Privacy Professionals (IAPP). (2017). GDPR matchup: Philippines' Data Privacy Act. *Privacy Tracker*.
- Lacity, M., & Khan, S. (2021). Data privacy and governance frameworks in digital organizations. *Journal of Information Systems Management*, 38(3), 203–218.
- Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). Mapping GDPR effectiveness: A systematic review. *Computer Law & Security Review*, 57, 106129.
- Meyer, J. W., & Rowan, B. (1991). Institutionalized organizations: Formal structure as myth and ceremony. In *The new institutionalism in organizational analysis*. University of Chicago Press.
- Miano, L. C. (2025). Awareness on data privacy vis-à-vis data management practices. *Edelweiss Applied Science and Technology*, 9(1).
- National Privacy Commission (NPC). (2016). Implementing Rules and Regulations of RA 10173.
- National Privacy Commission (NPC). (2020). NPC advisory guidelines on Data Protection Officer functions.
- National Privacy Commission (NPC). (2021). Annual report on enforcement and compliance monitoring.
- Parker, C., & Nielsen, V. L. (2017). *Explaining compliance: Business responses to regulation*. Edward Elgar.
- Pesito, P. M. F., et al. (2020). Efficiency of compliance to Data Privacy Act of 2012. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5), 7669–7675.
- Pitogo, V. A. (2019). National government agency's compliance on Data Privacy Act of 2012. De La Salle University Repository.
- Republic of the Philippines. (2012). Republic Act No. 10173: Data Privacy Act of 2012. *Official Gazette of the Republic of the Philippines*.
- Santana, P. C., & Ansari, F. A. (2023). Data protection and privacy as a fundamental right. *Journal of Liberty and International Affairs*, 9(3), 555–576.
- Suchman, M. C. (1995). Managing legitimacy. *Academy of Management Review*, 20(3), 571–610.
- Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal data protection in legal theory. *Journal of Law and Legal Reform*, 6(3), 1349–1376.
- Westin, A. (1967). *Privacy and freedom*. Atheneum Press.