

**Implementation of RA 10173 (Data Privacy Act of 2012)  
among SSS offices in Panay Island**

**Cherrey Rose P. Malco\***

Capiz State University - Pontevedra Campus  
Pontevedra, Capiz, Philippines  
Email: cherreyrose@gmail.com

**Honey Lee E. Casa, DPA**

Capiz State University - Pontevedra Campus  
Pontevedra, Capiz, Philippines

**ABSTRACT**

This study was conducted to determine the awareness and implementation of the Data Privacy Act in the SSS Offices in Panay Island. These included Antique branch, Iloilo Central Branch, Kalibo Branch, Roxas Branch, Molo-Iloilo Branch, Visayas West 2 Division, Legal Department, Medical Department, Employer Delinquency and Monitoring Department and the Iloilo Processing Center. Employing descriptive research design, this study utilized a questionnaire developed based on the provisions of the Data Privacy Act All employees of the different branches and departments of SSS in Panay Island were included in the study. Descriptive statistics were used to analyze the results of the study. The findings revealed that SSS employees in the various branches and departments of Panay Island were aware of the Data Privacy Act and confirmed its implementation in their offices. Older age, higher educational attainment, longer length of service, and higher employment status resulted to higher awareness and perceived implementation. Barriers to implementation include time and resources constraints as well as emerging technologies. Recommendations centered on the conduct of mandatory DPA orientation seminars and examinations for new employees, the holding of DPA seminars regularly for all employees and the annual assessment, evaluation and audit on data privacy practices and implementation in SSS branches and departments not only in Panay Island but also nationwide.

**Keywords:** Data privacy, awareness, implementation, challenges.

Date Submitted: February 2, 2026

Date Accepted: February 11, 2026

Date Published: March 2, 2026

**INTRODUCTION**

The security with which one's data is properly handled is called Data Privacy. This involves the protection of one's data, how it is shared and how it is collected and stored. With

---

\*Corresponding author

DOI: <http://doi.org/10.69651/PIJHSS0501869>

Recommended citation:

Malco, C. R. P., & Casa, H. L. E. (2025). Status of implementation of R.A. 10173 (Data privacy act of 2012) among SSS offices in Panay Island. Pantao (The International Journal of the Humanities and Social Sciences) 5 (1), 9783-9795. <http://doi.org/10.69651/PIJHSS0501869>

the advent of the digital information revolution, data has become one of the most important resources of any organization. As noted by Chandrasekeran et al. (2023), the rapidly changing landscape of digital information necessitates the proper management, storage, and retrieval of crucial records of employees and clients. In the Philippines, mechanisms to ensure data security were established through Republic Act No. 10173, also known as the Data Privacy Act of 2012, which mandates public and private organizations, agencies, and institutions to protect and safeguard sensitive and confidential data of their members. The National Privacy Commission defines this law as the policy of the State to protect the fundamental human right of privacy of communication while ensuring the free flow of information to promote innovation and growth (Republic Act No. 10173, Ch. 1, Sec. 2).

Consistent with this mandate, the Social Security System (SSS), like other government agencies, upholds data privacy rights and ensures that all personal data collected are processed in accordance with the principles of transparency, legitimate purpose, and proportionality. The agency maintains confidential records and reports submitted by employers and members as required under Republic Act No. 1161, known as the Social Security Law. Furthermore, SSS ensures that all personal data processing adheres to Republic Act No. 10173, its Implementing Rules and Regulations, and other relevant policies issued by the National Privacy Commission. Despite the enactment of the Data Privacy Act in 2012 and the conduct of implementation studies in various agencies, there remains a need to examine its implementation specifically within SSS offices in Panay Island. Understanding the extent of implementation can support improvements in efficiency and effectiveness, thereby strengthening data privacy practices within the agency.

This study is anchored on the Information Uses and Gratification Theory of Blumler and Katz (1974), as cited in Sichach (2023), which emphasizes that user behavior is driven by goals and motivations rather than solely by privacy sensitivity. Disclosure of information is influenced by higher level motivations and associated privacy concerns that affect technology use, and inconsistencies may arise when individuals express concern for privacy but exhibit behaviors that do not reflect such concern. Complementing this perspective, Smith et al. (2011) introduced the Antecedents Privacy Concerns Outcomes Model, which explains how privacy concerns are shaped by antecedents such as personal traits, contextual factors, regulatory forces, and technological attributes, and how these concerns lead to outcomes such as reduced disclosure or limited technology use. Xu et al. (2012) further emphasized that these antecedents can either increase or decrease privacy concerns depending on varying conditions.

Policy implementation is a critical stage in the policy making process, involving the execution of laws through coordinated actions of stakeholders, organizations, and procedures to achieve policy goals (Stewart et al., 2018). It can be understood as a process, an output, and an outcome involving multiple actors and control mechanisms. In this study, the concept of implementation is applied to the awareness and execution of the Data Privacy Act of 2012 within the Social Security System. The study is also grounded in the top down model of policy implementation proposed by Meter and Horn (1975), as cited in Khan (2016), which identifies six variables influencing policy performance, namely policy standards and objectives, resources, intergovernmental communication and enforcement activities, characteristics of agencies, economic, social, and political conditions, and the disposition of implementers. These variables provide a framework for examining how SSS branches in Panay Island comply with and implement the provisions of the Data Privacy Act.

The findings of this study are expected to benefit several stakeholders. SSS employees will gain insights into the extent of implementation of the Data Privacy Act in their respective offices and how it protects both their personal data and that of members. SSS members will be assured that their personal information is processed in accordance with the principles and provisions of the law, thereby enhancing their awareness of their rights. Department heads can

utilize the results to evaluate employee compliance and implementation practices within their units. SSS management may use the findings to assess adherence to the Data Privacy Manual and identify areas for improvement across branches in Panay Island. Future researchers may also use the results as a reference for similar studies on data privacy implementation.

This study focuses on determining the awareness and implementation of the Data Privacy Act among SSS employees in Panay Island. It covers selected SSS branches and departments including Antique Branch, Iloilo Central Branch, Kalibo Branch, Roxas Branch, Molo Iloilo Branch, Visayas West 2 Division, Legal Department, Medical Department, Employer Delinquency and Monitoring Department, and the Iloilo Processing Center. A questionnaire based on the provisions of the Data Privacy Act was utilized as the primary research instrument, and descriptive statistical tools such as frequency counts, percentages, mean, and standard deviation were employed for data analysis.

For clarity, key terms are defined conceptually and operationally. The Data Privacy Act refers to Republic Act No. 10173, which establishes a framework for processing personal data in the Philippines (NPC, 2012). Implementation pertains to the execution or practice of a plan or policy (Lutkevich, 2024), and in this study refers specifically to the execution of the Data Privacy Act. Organizational safety measures refer to procedures and practices ensuring a safe environment (OSHA, 2020), and in this context relate to measures adopted by SSS to protect personal data. Personal data collection, use, and access involve the processes of gathering, utilizing, and controlling access to personal information (Bhandari, 2020). Personal data purpose and transparency refer to clearly stating the purpose of data collection and ensuring transparency in processing (Wigmore, 2022). Physical safety measures involve protecting both paper and electronic data through secure storage and disaster recovery systems (Fennelly, 2022). The Social Security System is a government agency providing social protection to private sector workers (Bugante, 2016). Technical safety measures refer to tools and processes that ensure the confidentiality, integrity, and availability of information systems (Collins Dictionary, 2019).

Existing literature indicates that data privacy awareness varies across demographic profiles. Age influences awareness, with younger individuals demonstrating greater engagement with privacy rights, while older individuals may be more cautious but less proactive (Petrosyan, 2023). Differences in perception across age groups were also noted by Kaiser (2021) and Waitman (2023), while Pender (2025) identified a gap in awareness and action between younger and older adults. Gender differences in privacy behavior have been explored by Mailok et al. (2023) and Tifferet (2018), although overall concern for privacy does not significantly differ between men and women. Civil status does not significantly affect awareness, although employment status may influence it, with permanent employees showing higher awareness (Agup, 2024). Educational attainment is associated with greater understanding of data privacy concepts (Park and Vance, 2023), while length of service may influence familiarity with data management practices (Miano, 2025).

Similarly, implementation of data privacy practices is influenced by various factors. Age may affect decision making and implementation strategies (Alley et al., 2018), while younger and older employees differ in their motivations and behavioral influences (Morris et al., 2015). Gender does not significantly affect implementation practices, although slight differences in perceived control over personal data exist (Savić and Veinović, 2018). Civil status does not significantly influence implementation, but employment status again shows differences, with permanent employees demonstrating better implementation (Agup, 2024). Higher education levels contribute to better implementation of data privacy concepts (Park and Vance, 2023), while longer tenure may enhance awareness of compliance and consequences of data breaches (Miano, 2025).

Data privacy is a key component of data protection, which involves safeguarding sensitive information to meet regulatory requirements and ensure confidentiality and integrity (APEC, 2015). Cavoukian (2016) identifies data protection as encompassing traditional protection methods, data security, and data privacy. According to ICRC (2015), data protection also includes processes for restoring data and ensuring authorized access. Data privacy mechanisms protect individuals from threats in the digital age (Foronda et al., 2023), ensuring that personal information is not accessed by unauthorized parties (Alafaa, 2022). Global frameworks such as the General Data Protection Regulation provide guidelines for managing sensitive data and have influenced the development of similar laws worldwide (Machado et al., 2023; Savić and Veinović, 2018).

The General Data Protection Regulation outlines key principles including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles guide organizations in ensuring responsible data processing and compliance with regulatory requirements. In the Philippines, the Data Privacy Act of 2012 serves as a comprehensive legal framework governing personal data protection. Enacted on 15 August 2012 and supported by implementing rules issued by the National Privacy Commission in 2016, the law addresses the need for standardized data protection practices in response to increasing global data exchange (Gaba, 2024). It applies broadly to individuals and entities processing personal data, including those operating beyond national boundaries when Philippine data is involved (Wall, 2024). The law emphasizes transparency, legitimate purpose, and proportionality, and requires informed consent prior to data collection, with specific exceptions under contractual, legal, or emergency conditions.

Empirical studies reveal varying levels of implementation of data privacy laws. The OECD (2023) identified gaps in national privacy strategies and challenges related to regulation, enforcement, and emerging technologies. Aguilar (2024) found that data protection policies were highly implemented but challenges such as lack of awareness, limited resources, and complex regulations persisted. Pitogo (2019) reported partial compliance in a frontline agency, citing challenges such as lack of awareness and resource constraints. Foronda et al. (2023) highlighted the influence of age and location on perceptions of data privacy implementation, while Castor (2021) found moderate implementation levels in higher education institutions. Tanate Lazo (2021) observed that while stakeholders demonstrated strong knowledge and compliance, gaps in specific provisions remained.

Overall, the literature indicates that while the Data Privacy Act has been widely implemented across various organizations in the Philippines, the level of implementation varies from moderate to high, with persistent challenges affecting its effectiveness. These findings underscore the need for further investigation into specific institutional contexts, such as the Social Security System in Panay Island, to better understand and enhance the implementation of data privacy policies.

### Statement of the problem

This study explored the level of awareness and the status of implementation of the Data Privacy Act among SSS Offices in Panay Island. Specifically, this study sought to answer the following questions:

1. What is the profile of the SSS employees in terms of age, gender, civil status, educational attainment, length of service in SSS, status of employment, and branch or department?
2. What is the level of awareness of the Data Privacy Act among SSS employees in Panay Island?

3. What is the extent of implementation of the Data Privacy Act among SSS Offices in Panay Island?
4. What is the level of awareness of the Data Privacy Act among the respondents when grouped according to their profile?
5. What is the extent of implementation of the Data Privacy Act among the respondents when grouped according to their profile?
6. What is the distribution of the respondents according to their awareness and implementation of the Data Privacy Act?
7. What challenges are encountered in the implementation of the Data Privacy Act among SSS Offices in Panay Island?

## METHODOLOGY

The study employed a descriptive quantitative research design to examine the awareness and implementation of the Data Privacy Act as perceived by employees of the Social Security System in Panay Island. Quantitative research involves the systematic collection and analysis of numerical data and is utilized to identify patterns and averages, make predictions, test causal relationships, and generalize findings to broader populations (Bhandari, 2022). In this investigation, the design was appropriate in evaluating the levels of awareness and implementation across different branches and departments of the Social Security System within the specified locale.

The study was conducted among employees of various branches and departments of the Social Security System located in Panay Island. These included Antique Branch, Iloilo Central Branch, Kalibo Branch, Roxas Branch, Molo Iloilo Branch, Visayas West 2 Division, Legal Department, Medical Department, Employer Delinquency and Monitoring Department, and the Iloilo Processing Center. All employees from these branches and departments were included in the study through complete enumeration, and no sampling technique was applied, ensuring that the entire population of interest was represented in the data collection process.

The respondents of the study consisted of employees from the aforementioned branches and departments of the Social Security System in Panay Island. A researcher made questionnaire based on the provisions of the Data Privacy Act served as the primary data gathering instrument. The instrument was composed of four parts. The first part elicited information regarding the personal profile of the respondents, specifically age, gender, civil status, educational attainment, length of service, status of employment, and branch or department. The second part measured the level of awareness of the Data Privacy Act among employees and consisted of 50 provisions of the law, assessed using a five point scale. The responses were scored as 5 Fully Aware, 4 Aware, 3 Moderately Aware, 2 Slightly Aware, and 1 Not Aware. The third part determined the level of implementation of the Data Privacy Act using another set of 50 provisions, also rated on a five point scale with corresponding scores of 5 Fully Implemented, 4 Implemented, 3 Moderately Implemented, 2 Slightly Implemented, and 1 Not Implemented. The fourth part identified barriers to implementation and included items reflecting challenges encountered by employees, as well as an open ended portion where respondents could share their personal experiences regarding these challenges.

The research instrument was based directly on the provisions of the Data Privacy Act; therefore, formal validity and reliability testing was not conducted. Instead, the instrument underwent face validation by a panel of experts composed of the advisory committee and other research professionals to ensure its appropriateness and clarity.

The study considered three main variables. The first variable was the profile of respondents, categorized according to age, gender, civil status, educational attainment, length

of service, status of employment, and branch or department. Age was grouped into 30 and below, 31 to 40, 41 to 50, and 51 and above. Gender was categorized as male or female, while civil status included single, married, widow or widower, and separated or annulled. Educational attainment was classified into Bachelor's Degree, Bachelor's Degree with Master's Unit, Master's Degree, Master's Degree with Doctorate Units, and Doctorate Degree. Length of service was grouped into 10 and below, 11 to 20, and above 20. Status of employment included job order or casual, rank and file, supervisory, and managerial employees. Branches and departments were identified as Antique Branch, Iloilo Central Branch, Kalibo Branch, Roxas Branch, Molo Iloilo Branch, Visayas West 2 Division, Legal Department, Medical Department, Employer Delinquency and Monitoring Department, and the Iloilo Processing Center.

The second variable, level of awareness of the Data Privacy Act, was categorized into fully aware, aware, moderately aware, slightly aware, and not aware. The interpretation of mean scores for awareness was defined as follows: 4.21 to 5.00 Fully Aware, 3.41 to 4.20 Aware, 2.61 to 3.40 Moderately Aware, 1.81 to 2.60 Slightly Aware, and 1.00 to 1.80 Not Aware. The third variable, level of implementation, was categorized into fully implemented, implemented, moderately implemented, slightly implemented, and not implemented. The interpretation of mean scores for implementation was defined as follows: 4.21 to 5.00 Fully Implemented, 3.41 to 4.20 Implemented, 2.61 to 3.40 Moderately Implemented, 1.81 to 2.60 Slightly Implemented, and 1.00 to 1.80 Not Implemented.

Prior to data collection, the researcher sought permission from the heads of each branch and department where the study was conducted. Upon approval, the questionnaire was converted into a Google Forms format and distributed to the respondents. The purpose of the study was clearly explained, and participation was voluntary. Respondents were given the option to participate or decline and were provided sufficient time to complete the questionnaire upon giving consent. After data collection, the responses were compiled and processed for statistical analysis.

The study utilized descriptive statistical tools to analyze the collected data. Frequency counts were employed to determine the number of respondents according to their personal profile as well as their levels of awareness and implementation. Percentages were used to present the proportion of respondents within each category when grouped according to profile, level of awareness, and level of implementation. The mean was computed to determine the level of awareness and perceived implementation of the Data Privacy Act based on the scores obtained from the questionnaire responses. Standard deviation was used to measure the variability of the data, where a low standard deviation indicates that data points are closely clustered around the mean, while a high standard deviation signifies a wider dispersion of values.

## RESULTS AND DISCUSSION

This study involved 168 employees from various Social Security System branches and departments in Panay Island and employed a descriptive quantitative research design using complete enumeration as the sampling approach. Data were gathered through a researcher-made questionnaire anchored on the provisions of the Data Privacy Act, and the responses were analyzed using descriptive statistical tools including frequency counts, percentages, mean, and standard deviation. The discussion that follows is grounded on the data collected and interpreted directly in relation to the objectives of determining the profile of respondents, their level of awareness and extent of implementation of the Data Privacy Act, variations across profile variables, the relationship between awareness and implementation, and the challenges encountered in its implementation.

The profile of respondents revealed that out of 168 employees, 41.7% were aged 31 to 40 years, 26.8% were 41 to 50 years, 17.5% were 51 years and above, and 14.3% were 30 years and below, indicating that the workforce was predominantly composed of adults. In terms of gender, 67.3% were female and 32.7% were male, while civil status showed that 56.5% were married, 40.5% were single, 1.8% were widowed, and 1.2% were separated or annulled. Educational attainment indicated that 41.1% held bachelor's degrees, 40.5% had master's degrees, 14.3% had bachelor's degrees with master's units, 3.0% had doctorate degrees, and 1.2% had master's degrees with doctorate units. With respect to length of service, 50.6% had served 10 years and below, 29.2% had served 11 to 20 years, and 20.2% had served above 20 years. Regarding employment status, 73.8% were rank and file employees, 15.5% were supervisory, 6.0% were job order or casual, and 4.8% were managerial. Distribution across branches showed that the Iloilo Processing Center had 37 employees (22.0%), Iloilo Central Branch had 36 (21.4%), Kalibo Branch and Visayas West 2 Division had 19 each (11.3%), Roxas Branch had 17 (10.1%), Antique Branch had 16 (9.5%), Molo Iloilo Branch had 15 (8.9%), and the Legal, Medical, and Employer Delinquency and Monitoring Departments had 3 each (1.8%). These findings indicate a workforce largely composed of experienced and educated employees, consistent with the assertion of Park and Vance (2023) that higher educational attainment is associated with greater awareness of data privacy concepts.

The level of awareness of the Data Privacy Act among SSS employees was generally high, with an overall mean of  $\bar{x} = 4.09$  and  $\sigma = 0.55$ , interpreted as Aware. Among the 50 provisions examined, the highest awareness was observed in "The data subject is provided specific information regarding the purpose and extent of processing" with  $\bar{x} = 4.54$  and  $\sigma = 0.66$ , followed by "The collection of personal data is only for a declared, specified and legitimate purpose" with  $\bar{x} = 4.41$  and  $\sigma = 0.69$ , "Only personal data that is necessary and compatible with declared, specified, and legitimate purpose is collected" with  $\bar{x} = 4.39$  and  $\sigma = 0.67$ , and "Consent of the data subject is always obtained prior to processing of sensitive personal information" with  $\bar{x} = 4.38$  and  $\sigma = 0.67$ . Additional high awareness was recorded in "The sensitive personal information is not transferred to third parties" and "Processing upholds the rights of the data subject, to refuse, withdraw consent or object," both with  $\bar{x} = 4.27$  and  $\sigma = 0.82$  and  $\sigma = 0.71$ , respectively. These findings align with Wall (2024), who emphasized that personal data processing must adhere to transparency, legitimate purpose, and proportionality. However, lower awareness was observed in provisions such as "Personal data which are incomplete, outdated, false, or unlawfully obtained could be erased or blocked by the data subject" with  $\bar{x} = 3.83$  and  $\sigma = 0.62$ , "Personal data is erased or blocked when the data subject withdraws consent" with  $\bar{x} = 3.84$  and  $\sigma = 0.84$ , "Regular vulnerability assessment shall be conducted" with  $\bar{x} = 3.85$  and  $\sigma = 0.76$ , "The data subject shall be indemnified for any damage" with  $\bar{x} = 3.88$  and  $\sigma = 0.69$ , and "The data subject shall have the right to suspend, withdraw or order the blocking" with  $\bar{x} = 3.90$  and  $\sigma = 0.71$ . Only 13 out of 50 provisions or 26% were rated as Fully Aware, indicating that awareness remains uneven across provisions.

The extent of implementation of the Data Privacy Act was interpreted as Implemented with an overall mean of  $\bar{x} = 4.10$  and  $\sigma = 0.60$ . The highest implementation was observed in "Consent is required prior to the collection and processing of personal data" with  $\bar{x} = 4.47$  and  $\sigma = 0.66$ , followed by "The data subject is provided specific information regarding the purpose and extent of processing" with  $\bar{x} = 4.33$  and  $\sigma = 0.66$ , "Consent of the data subject is always obtained prior to processing of sensitive personal information" with  $\bar{x} = 4.30$  and  $\sigma = 0.65$ , and both "Only personal data that is necessary and compatible with declared, specified, and legitimate purpose is collected" and "The collection of personal data is only for a declared, specified and legitimate purpose" with  $\bar{x} = 4.26$  and  $\sigma = 0.66$  and  $\sigma = 0.67$ , respectively. These findings support Wall (2024), emphasizing the importance of informed consent in data

processing. Conversely, the lowest implementation scores were observed in “Date when personal data were last accessed and modified are made accessible” with  $\bar{x} = 3.92$  and  $\sigma = 0.80$ , “Personal data is erased or blocked when consent is withdrawn” with  $\bar{x} = 3.95$  and  $\sigma = 0.84$ , “Regular vulnerability assessment shall be conducted” with  $\bar{x} = 3.97$  and  $\sigma = 0.82$ , “Personal data which are incomplete, outdated, false, or unlawfully obtained could be erased or blocked” with  $\bar{x} = 3.97$  and  $\sigma = 0.84$ , and “The data subject shall have the right to suspend, withdraw or order the blocking” with  $\bar{x} = 3.97$  and  $\sigma = 0.80$ . Only 18% of the provisions were fully implemented, indicating gaps between awareness and actual practice.

When grouped according to profile, the level of awareness showed variation across categories. The overall awareness remained at  $\bar{x} = 4.09$  and  $\sigma = 0.55$ . Employees aged 41 to 50 years were Fully Aware with  $\bar{x} = 4.27$  and  $\sigma = 0.51$ , while other age groups were Aware, including those 30 and below with  $\bar{x} = 4.06$  and  $\sigma = 0.75$ , those 31 to 40 with  $\bar{x} = 4.02$  and  $\sigma = 0.51$ , and those 51 and above with  $\bar{x} = 4.02$  and  $\sigma = 0.45$ . Both female and male respondents were Aware with  $\bar{x} = 4.10$  and  $\sigma = 0.50$ , and  $\bar{x} = 4.08$  and  $\sigma = 0.64$ , respectively. Civil status showed that separated or annulled respondents were Fully Aware with  $\bar{x} = 4.44$  and  $\sigma = 0.37$ , while others were Aware. Higher awareness was also observed among those with doctorate degrees with  $\bar{x} = 4.29$  and  $\sigma = 0.45$  and those with longer service above 20 years with  $\bar{x} = 4.24$  and  $\sigma = 0.47$ . Managerial and supervisory employees were Fully Aware with  $\bar{x} = 4.38$  and  $\sigma = 0.48$  and  $\bar{x} = 4.22$  and  $\sigma = 0.55$ , respectively, while rank and file and casual employees were Aware. The Medical Department recorded the highest awareness with  $\bar{x} = 4.47$  and  $\sigma = 0.46$ , while the Legal Department had the lowest with  $\bar{x} = 3.87$  and  $\sigma = 0.21$ . These findings partially support Mailok et al. (2023) and Agup (2024) regarding gender similarities, and strongly support Park and Vance (2023) and Miano (2025) regarding the influence of education and experience.

Similarly, the extent of implementation varied across profile variables with an overall mean of  $\bar{x} = 4.10$  and  $\sigma = 0.55$  interpreted as Implemented. Employees aged 41 to 50 years perceived implementation as Fully Implemented with  $\bar{x} = 4.28$  and  $\sigma = 0.58$ , while other age groups perceived it as Implemented. Both female and male respondents perceived implementation as Implemented with  $\bar{x} = 4.11$  and  $\sigma = 0.58$  and  $\bar{x} = 4.09$  and  $\sigma = 0.64$ . Separated or annulled respondents perceived it as Fully Implemented with  $\bar{x} = 4.60$  and  $\sigma = 0.45$ . Those with doctorate degrees and bachelor's degrees with master's units perceived it as Fully Implemented with  $\bar{x} = 4.39$  and  $\sigma = 0.60$  and  $\bar{x} = 4.23$  and  $\sigma = 0.54$ , respectively. Employees with more than 20 years of service also perceived higher implementation with  $\bar{x} = 4.26$  and  $\sigma = 0.56$ . Managerial and supervisory employees perceived implementation as Fully Implemented with  $\bar{x} = 4.42$  and  $\sigma = 0.54$  and  $\bar{x} = 4.27$  and  $\sigma = 0.66$ . Roxas Branch had the highest implementation with  $\bar{x} = 4.50$  and  $\sigma = 0.47$ , followed by the Medical Department with  $\bar{x} = 4.47$  and  $\sigma = 0.63$ , while the Legal Department had the lowest with  $\bar{x} = 3.84$  and  $\sigma = 0.33$ . These findings align with Alley et al. (2018), Morris et al. (2015), and Miano (2025), highlighting the influence of experience and organizational role on implementation.

The distribution of respondents according to awareness and implementation revealed that among those fully aware, 58 perceived full implementation, 9 perceived implementation, and 1 perceived moderate implementation. Among those aware, 67 perceived implementation, 12 perceived full implementation, and 6 perceived slight implementation. All 13 respondents who were moderately aware perceived moderate implementation, while among the two slightly aware respondents, one perceived moderate implementation and one perceived slight implementation. These results demonstrate a direct pattern where higher awareness corresponds to higher perceived implementation, supporting findings of Pitogo (2019), Aguilar (2024), and Tanate Lazo (2021).

The challenges encountered by employees further contextualize these findings. Time and resource constraints were identified by 96 respondents or 57%, followed by emerging

technologies with 91 or 54%, lack of training with 81 or 48%, lack of awareness with 76 or 45%, understaffing with 66 or 39%, organizational issues with 48 or 29%, complicated regulatory landscape with 31 or 18%, and wait and see attitude with 29 or 17%. These barriers are consistent with prior studies by Pitogo (2019), Foronda et al. (2023), and Aguilar (2024), indicating that despite moderate to high awareness and implementation, structural and resource limitations continue to hinder full compliance.

In synthesis, the findings of this study demonstrate that SSS employees in Panay Island exhibit an overall level of awareness of the Data Privacy Act at  $\bar{x}$  = 4.09 and  $\sigma$  = 0.55 and perceive its implementation at  $\bar{x}$  = 4.10 and  $\sigma$  = 0.60, both interpreted as generally adequate but not fully achieved. Variations across profile variables indicate that higher education, longer tenure, and higher organizational position are associated with greater awareness and stronger perceived implementation. The observed alignment between awareness and implementation underscores the importance of knowledge in promoting compliance. However, the presence of persistent challenges such as time and resource constraints, technological changes, and limited training highlights the need for targeted interventions. These results address the objectives of the study by providing a comprehensive understanding of awareness, implementation, and barriers, and contribute to the field by offering empirical evidence that can inform policy enhancement and organizational strategies, thereby setting the stage for recommendations and further inquiry in subsequent sections of the manuscript.

## CONCLUSION

This study examined the awareness and perceived implementation of the Data Privacy Act among 168 employees across various Social Security System branches and departments in Panay Island using a descriptive quantitative research design and complete enumeration. Data were collected through a researcher-made questionnaire anchored on the provisions of the Data Privacy Act and analyzed using descriptive statistical tools. The findings revealed that the respondents largely represented the workforce of the Social Security System in the study area, characterized by employees who were predominantly 31 to 40 years old, female, married, holding bachelor's and master's degrees, with 10 years or less in service, and occupying rank and file positions. This demographic composition suggests a workforce that is both relatively experienced and academically prepared, with many employees demonstrating a tendency to pursue further education, which may indicate aspirations for career advancement within the organization.

The study established that, as a whole, SSS employees were aware of the Data Privacy Act, particularly its general principles related to the collection, processing, and retention of personal data. Employees demonstrated high awareness of provisions requiring that data subjects be informed of the purpose and extent of data processing. However, gaps in awareness were evident in provisions concerning the rights of data subjects, especially the right to have incomplete, outdated, false, or unlawfully obtained data erased or blocked. This indicates that while foundational knowledge of the Data Privacy Act is present, there remains a need to strengthen awareness of specific rights and protective mechanisms embedded in the law. Correspondingly, the findings showed that the Data Privacy Act was perceived to be implemented in the SSS offices in Panay Island, particularly in areas related to consent, data collection, processing, and data sharing. Nonetheless, implementation was not uniform across all provisions, with lower levels observed in areas related to security measures for the protection of personal data, including the accessibility of data access logs and the conduct of vulnerability assessments, suggesting the need for improvements in technical and organizational safeguards.

Variations in awareness and implementation were observed across respondent profiles. Employees who were 41 to 50 years old, separated or annulled, holding doctorate degrees, with more than 20 years of service, occupying supervisory and managerial positions, and working in the Medical Department exhibited higher levels of awareness of the Data Privacy Act. Similarly, higher levels of perceived implementation were reported by respondents with similar characteristics, including those in the Kalibo and Roxas Branches and the Medical Department. These findings imply that seniority in age and length of service, higher educational attainment, and organizational roles involving oversight and decision making contribute to greater awareness and stronger perceptions of implementation. Such employees are likely more directly involved in ensuring compliance with data privacy regulations and are therefore more exposed to policies, procedures, and training related to data protection.

Furthermore, the study found that SSS employees, by virtue of their roles in collecting and processing personal data, tend to have a heightened awareness of data privacy principles and practices. The nature of their work necessitates familiarity with legal and organizational requirements, reinforcing the importance of data privacy within the institution. Data privacy is therefore both a legal obligation and an ethical responsibility for the Social Security System, which handles sensitive personal information. Maintaining strong data privacy practices is essential not only for compliance with Republic Act No. 10173 but also for sustaining public trust and ensuring the integrity of social security services.

Despite the generally positive levels of awareness and implementation, the study identified several key challenges that hinder full compliance with the Data Privacy Act. Time and resource constraints emerged as the most significant barrier, identified by more than half of the respondents, followed closely by challenges posed by emerging technologies. Additional concerns included lack of training, insufficient awareness of specific provisions, understaffing, organizational issues, complex regulatory requirements, and a wait-and-see attitude among some employees. These challenges highlight structural and operational limitations that affect the ability of the organization to fully implement data privacy policies, particularly in adapting to evolving technological environments and ensuring adequate training and resource allocation.

In light of these findings, it is evident that while the Social Security System in Panay Island demonstrates a generally satisfactory level of awareness and implementation of the Data Privacy Act, there remains a need for continuous improvement in both knowledge dissemination and operational execution. Strengthening awareness of data subject rights, enhancing security measures, and addressing organizational constraints are essential to achieving full compliance. Accordingly, it is recommended that mandatory data privacy orientation seminars and examinations be implemented for newly hired employees to establish foundational knowledge at the onset of employment. Regular training initiatives, such as quarterly or semiannual webinars lasting one to two hours, should be conducted to reinforce and update employees' understanding of the law. Additionally, systematic assessment, evaluation, and audit of data privacy practices should be undertaken annually across all branches and departments, not only within Panay Island but nationwide, to ensure consistent and effective implementation. Future research may further expand this inquiry by examining data privacy awareness and implementation in other government agencies within Panay Island to validate and compare findings.

Overall, this study contributes to the growing body of knowledge on data privacy implementation in government institutions by providing empirical evidence on the levels of awareness, extent of implementation, and challenges encountered within the Social Security System in Panay Island. The findings underscore the importance of continuous education, resource allocation, and organizational commitment in strengthening data privacy practices. By addressing identified gaps and implementing the recommended measures, the Social Security System can enhance its compliance with the Data Privacy Act and further uphold its

responsibility to protect sensitive personal information, thereby reinforcing institutional integrity and public trust.

## REFERENCES

Aguilar, J. J. D. (2024). Beyond compliance: Analysis of data privacy implementation. *Journal of Management, Economics, and Industrial Organization*, 8(2), 78–93. <https://doi.org/10.31039/jomeino.2024.8.1.4>

Agup, R. M. (2024). Data privacy act: Awareness, compliance, and challenges of nurses of government hospitals in Northern Philippines. *South Eastern European Journal of Public Health*.

Alafaa, P. (2022). Data privacy and data protection: The rights of users and the responsibility of companies in the digital world. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4005750>

Alley, S. J., Schoeppe, S., Rebar, A. L., Hayman, M., & Vandelanotte, C. (2018). Age differences in physical activity intentions and implementation intention preferences. *Journal of Behavioral Medicine*, 41(3), 406–415. <https://doi.org/10.1007/s10865-017-9899-y>

Asia-Pacific Economic Cooperation. (2015). APEC privacy framework. <https://www.apec.org/publications/2005/12/apec-privacy-framework>

Bhandari, P. (2020). Data collection: Definition, methods, and examples. <https://www.scribbr.com/methodology/data-collection/>

Bhandari, P. (2022). What is quantitative research? Definition, uses, and methods. <https://www.scribbr.com/methodology/quantitative-research/>

Bugante, S. (2016, August 30). 59 years of faithful service to the nation. *BusinessMirror*.

Castro, C. K. C. (2021). The implementation of the data privacy act among higher educational institutions in the Province of Pangasinan. *Asian Journal of Multidisciplinary Studies*, 4(2).

Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. <https://www.onetrust.com/blog/principles-of-privacy-by-design/>

Chandrasekaran, A., Oliva, R., & Salvador, F. (2023). Intervention-based research in operations management. *Foundations and Trends in Technology, Information and Operations Management*, 17(1), 1–81.

Collins Dictionary. (2019). Technical safety. <https://www.collinsdictionary.com/dictionary/english/safety-measure>

Fennelly, L. (2022). Effective physical security. <https://library.fiveable.me/key-terms/ap-gov/physical-safety>

Foronda, S. M., Javier, N., Vigonte, F., & Abante, M. V. (2023). Implementation of Republic Act 10173 or the Data Privacy Act of 2012 in Albay Electric Cooperative (ALECO). SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4621933>

Gaba, J. P. (2024). Keeping watch on data privacy: Philippines. *Asia Business Law Journal*. <https://law.asia/philippines-data-privacy-laws/>

Gonzales, E. C., & Ching, M. R. D. (2018). Performance compliance of Philippine national government agency on the data privacy act of 2012: A qualitative case study. *Library Philosophy and Practice*. <https://digitalcommons.unl.edu/libphilprac/5020>

Hirsh, J. H. (2019). The peril and potential of the GDPR. <https://gdpr.eu/what-is-gdpr/>

International Committee of the Red Cross. (2015). ICRC code of conduct on data protection. <https://www.icrc.org/en/icrc-and-data-protection>

Kaiser, A. F. (2021). Privacy and security perceptions between different age groups while searching online. [https://essay.utwente.nl/70190/1/Kaiser\\_BA\\_BMS.pdf](https://essay.utwente.nl/70190/1/Kaiser_BA_BMS.pdf)

Khan, A. R. (2016). Policy implementation: Some aspects and issues. *Journal of Community Positive Practices*, 16(3), 3–12. <https://jppc.ro/en/index.php/jppc/article/view/316>

Lutkevich, B. (2024). What is implementation? <https://www.techtarget.com/searchcustomerexperience/definition/implementation>

Machado, P., Vilela, J., Peixoto, M., & Silva, C. (2023). A systematic study on the impact of GDPR compliance on organizations. In *Proceedings of the XIX Brazilian Symposium on Information Systems* (pp. 435–442). <https://doi.org/10.1145/3592813.3592935>

Mailok, R., Hassan, H., Said, C. S., & Hashim, M. (2023). Assessing the levels of knowledge of personal data protection among students. *International Journal on Social and Education Sciences*, 5(4), 879–892. <https://doi.org/10.46328/ijonses.610>

Meter, D. S. V., & Horn, C. E. V. (1975). The policy implementation process: A conceptual framework. *Administration and Society*, 6, 445–488.

Miano, L. C. (2025). Awareness on data privacy vis-à-vis data management practices at a state university in Quezon province: Input towards data-driven policy manual for good governance. *Edelweiss Applied Science and Technology*. <https://doi.org/10.55214/25768484.v9i1.4130>

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2015). Gender and age differences in employee decisions about implementing new technology: An extension to the theory of planned behavior. *IEEE Transactions on Engineering Management*, 52(1), 69–84. <https://doi.org/10.1109/TEM.2004.839967>

National Privacy Commission. (2012). The data privacy act of 2012. <https://privacy.gov.ph>

Occupational Safety and Health Administration. (2020). Work hazard prevention and control. <https://www.osha.gov/safety-management/hazard-prevention>

Organisation for Economic Co-operation and Development. (2023). Report on the implementation of the OECD privacy guidelines. OECD Digital Economy Papers, 361. <https://doi.org/10.1787/cf87ae8f-en>

Park, J., & Vance, A. (2023). Data privacy in education. <https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education>

Petrosyan, A. (2023). Share of global internet users familiar with privacy rights 2021, by age group. <https://www.statista.com/statistics/1302075/privacy-rights-awareness-worldwide-by-age-group>

Pitogo, V. (2019). National government agency's compliance on Data Privacy Act of 2012: A case study. *Journal of Physics: Conference Series*, 1201, 012021. <https://doi.org/10.1088/1742-6596/1201/1/012021>

Savić, D., & Veinović, M. (2018). Challenges of general data protection regulation (GDPR). In *Proceedings of Sinteza 2018* (pp. 23–30). <https://doi.org/10.15308/Sinteza-2018-23-30>

Sichach, M. (2023). Information uses and gratifications theory: Background, history and limitations. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4729248>

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016.

Stewart, J. J., Hedge, D. M., & Lester, J. P. (2008). *Public policy: An evolutionary approach* (3rd ed.). Thomson Wadsworth.

Tanate-Lazo, R. J. C., & Cabonero, D. A. (2021). Philippine data privacy law: Is it implemented in a private university library, or not? *Library Philosophy and Practice*.

Tifferet, S. (2018). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*. <https://doi.org/10.1016/j.chb.2018.11.046>

Waitman, R. (2023). Study: Younger consumers are more active on privacy. <https://iapp.org/news/a/study-younger-consumers-are-more-active-on-privacy>

Wall, A. (2024). Philippines data privacy act and implementing regulations. <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations>

Wigmore, I. (2022). What is data purpose and transparency? <https://www.techtarget.com/whatis/definition/transparency>

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23(4).